3GPP TSG-T (Terminals) Meeting #5
Kyongju, Korea, October 7 - 8, 1999

Document ***TSGT#5(99)186***

3G TS 31.102 V1.0.0 (1999-10)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM Application (3G TS 31.102 version 1.0.0)

Reference
DTS/TSGT-0331102U

Keywords
USIM, UICC

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

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. In particular, 3G TS 31.101 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 3GPP 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 terminal.

This is to ensure interoperability between a USIM and a terminal 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 terminal 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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

Editor's note: The following list is partly taken from GSM 11.11 version 7.1.0, and should be modified according to contents of the present document.

[1] GSM 01.02: "Digital cellular telecommunications system (Phase 2+); General description of a GSM Public Land Mobile Network (PLMN)".

[2] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[3] GSM 02.07: "Digital cellular telecommunications system (Phase 2+); Mobile Stations (MS) features".

[4] GSM 02.09: "Digital cellular telecommunications system (Phase 2+); Security aspects".

[5] GSM 02.11: "Digital cellular telecommunications system (Phase 2+); Service accessibility".

[6] GSM 02.17: "Digital cellular telecommunications system (Phase 2+); Subscriber Identity Modules (SIM) Functional characteristics".

[7] GSM 02.24: "Digital cellular telecommunications system (Phase 2+); Description of Charge Advice Information (CAI)".

[8] GSM 02.30: "Digital cellular telecommunications system (Phase 2+); Man-Machine Interface (MMI) of the Mobile Station (MS)".

[9] GSM 02.86: "Digital cellular telecommunications system (Phase 2+); Advice of charge (AoC) Supplementary Services - Stage 1".

[10] GSM 03.03: "Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification".

[11] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[12] GSM 03.38: "Digital cellular telecommunications system (Phase 2+); Alphabets and language-specific information".

[13] GSM 03.40: "Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP)".

[14] GSM 03.41: "Digital cellular telecommunications system (Phase 2+); Technical realization of Short Message Service Cell Broadcast (SMSCB)".

[15] GSM 04.08: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification".

[16] GSM 04.11: "Digital cellular telecommunications system (Phase 2+); Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[17] GSM 09.91: "Digital cellular telecommunications system (Phase 2+); Interworking aspects of the Subscriber Identity Module - Mobile Equipment (SIM - terminal) interface between Phase 1 and Phase 2".

[18] CCITT Recommendation E.118: "The international telecommunication charge card".

[19] CCITT Recommendation E.164: "Numbering plan for the ISDN era".

[20] CCITT Recommendation T.50: "International Alphabet No. 5". (ISO 646: 1983, "Information processing - ISO 7-bits coded characters set for information interchange".)

[21] ISO/IEC 7810 (1995): "Identification cards - Physical characteristics".

[22] ISO/IEC 7811-1 (1995): "Identification cards - Recording technique - Part 1: Embossing".

[23] ISO/IEC 7811-3 (1995): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards".

[24] ISO 7816-1 (1987): "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics".

[25] ISO 7816-2 (1988): "Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and locations of the contacts".

[26] ISO/IEC 7816-3 (1989): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[27] GSM 11.14: "Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - terminal) interface".

[28] GSM 11.12: "Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - terminal) interface".

[29] GSM 02.22: "Digital cellular telecommunications system (Phase 2+); Personalization of GSM Mobile Equipment (terminal) Mobile functionality specification".

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

[31] ISO/IEC 10646-1 (1993): "Information technology -- Universal Multiple-Octet Coded Character Set (UCS) -- Part 1: Architecture and Basic Multilingual Plane"

[32] GSM 03.60 : "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2"

[33] GSM 03.73: "Digital cellular telecommunications system (Phase 2+); Support of Localised Service Area (SoLSA); Service description; Stage 2"

[34] 3G TS 21.111: "USIM and IC Card Requirements".

[35] 3G TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[36] 3G TS 33.102: "3G Security Architecture"

[37] 3G TS 33.103: "3G Security; Integration Guidelines".

3 Abbreviations

3.1 Abbreviations

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

3GPP	3rd Generation Partnership Project
AC	Access Condition
ADF	Application Dedicated File
ADM	Access condition to an EF which is under the control of the authority which creates this file
AID	Application IDentifier
AK	Anonymity key
ALW	ALWays
AMF	Authentication Management Field
AuC	Authentication Centre
AUTN	Authentication token
CK	Cipher key
DF	Dedicated File
DO	Data Object
EF	Elementary File
EMUI	Encrypted Mobile User Identity
FCI	File Control Information
GK	User group key
GSM	Global System for Mobile communications
ICC	Integrated Circuit Card
ID	IDentifier
IK	Integrity key
IMUI	International Mobile User Identity
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
MF	Master File
MMI	Man Machine Interface
MSB	Most Significant Bit
NEV	NEVer
NPI	Numbering Plan Identifier
PIN	Personal Identification Number
RAND	Random challenge
RES	User response
RFU	Reserved for Future Use
RST	Reset
SE	Security Environment
SFI	Short EF Identifier
SQN	Sequence number

SW	Status Word
TLV	Tag Length Value
UICC	Universal Integrated Circuit Card
USIM	Universal Services Identity Module
XRES	Expected user response

4 Contents of the Elementary Files (EF)

This clause specifies the EFs for the UMTS 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 a EF_{ADN} record.

EFs or data items having an unassigned value, or, which during the UMTS session, are cleared by the terminal, 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 UMTS session by the allocation of a value specified in another GSM 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' (GSM 04.08 [15] refers).

Editor's note: The sentence above should be further considered if it is modified for USIM application.

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 CCITT Recommendation T.50 [20], bit 8 of every byte shall be set to 0.

For an overview containing all files see figure 9.

4.1 Contents of the EFs at the MF level

There are three EFs at the MF level.

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 must not contain a path object for application selection.
It is recommended that the application label does not contain more than 32 bytes.

Coding:
according to 3G TS 31.101 [35]

4.1.2 EF_{ICCID} (ICC Identity)

This EF provides a unique identification number for the ICC.

Contents:
according to 3G TS 31.101 [35]

Coding:
according to 3G TS 31.101 [35]

4.1.3 EF_{PL} (Preferred Language)

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 [xx]

Coding:
according to 3G TS 31.101 [xx]

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

The EFs in the 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 terminal for MMI purposes and for short message handling (e.g. screening of preferred languages in SMS-CB).

Identifier: '6F 05'	Structure: transparent	Mandatory
File size: 2n bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	ADM

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

Coding:
each language code is a pair of alpha-numeric characters, defined in ISO 639 [30]. Each alpha-numeric character shall be coded on one byte using the SMS default 7-bit coded alphabet as defined in GSM 03.38 [12] with bit 8 set to 0.

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

Editor's Note (CH): Should this EF be optional?

4.2.2 EF_{IMUI} (IMUI)

This EF contains the International Mobile User Identity (IMUI).

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

Access Conditions:

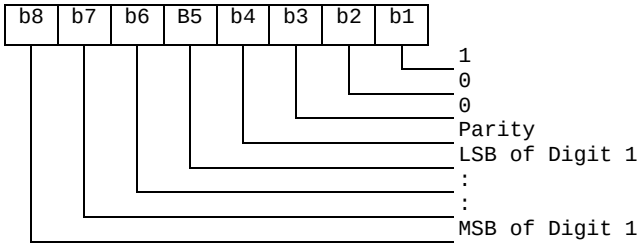
READ	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	PIN1

Bytes	Description	M/O	Length
1	Length of IMUI	M	1 byte
2 - 9	IMUI	M	8 bytes

- length of IMUI
  Contents:
  The length indicator refers to the number of significant bytes, not including this length byte, required for the IMUI.
  Coding: according to GSM 04.08 [15].

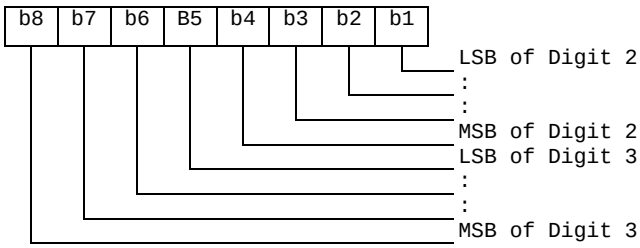
- IMUI
  Contents:
  International Mobile User Identity.
  Coding:
  This information element is of variable length. If a network operator chooses an IMUI of less than 15 digits, unused nibbles shall be set to 'F'.

  Byte 2:



  For the parity bit, see GSM 04.08 [15].

  Byte 3:



  etc.

4.2.3 EF_{CK} (Ciphering key CK)

Editor's note: This EF needs to be modified to store one or more CK and to meet all S3 requirements. Seq. No. ?.

This EF contains the ciphering key CK and the ciphering key sequence number n.

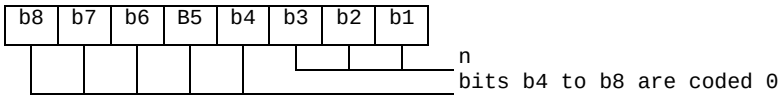
Identifier: '6F20'	Structure: transparent	Mandatory
File size: 17 bytes	Update activity: high	

Access Conditions:

READ	PIN1
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 – 8	Ciphering key CK	M	16 bytes
9	Ciphering key sequence number n	M	1 byte

- Ciphering key CK
  Coding:
  The least significant bit of CK is the least significant bit of the 16th byte. The most significant bit of CK is the most significant bit of the first byte.
- Ciphering key sequence number n
  Coding:



NOTE: GSM 04.08 [15] defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administrative phase.

4.2.4 $EF_{PLMNsel}$ (PLMN selector)

Editor's note: This EF may need to be modified based on 3G requirements.

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	PIN1
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 – 3	1st PLMN (highest priority)	M	3 bytes
22 – 24	8th PLMN	M	3 bytes
25 – 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 GSM 04.08 [15].
  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.

4.2.5 EF_{HPLMN} (HPLMN search period)

This EF contains the interval of time between searches for the HPLMN (see GSM 02.11 [5]).

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

Access Conditions:

READ	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	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 terminal as a default period.

For specification of the integer timer interval n, the maximum value and the default period refer to GSM 02.11 [5].

4.2.6 EF_{ACMmax} (ACM maximum value)

Editor's note: This EF may need to be modified based on the 3G service requirements.

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	PIN1
UPDATE	PIN1/PIN2 (fixed during administrative management)
INVALIDATE	ADM
REHABILITATE	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 25+24.

All ACM data is stored in the SIM and transmitted over the SIM/terminal interface as binary.

ACMmax is not valid, as defined in GSM 02.24 [7], if it is coded '000000'.

NOTE: If a GSM application is present on the UICC that shall co-operate with this specific USIM application this file is shared between the two applications.

4.2.7 EF_{UST} (USIM service table)

Editor's note: This EF needs to be modified according to the 3G service requirements and to the implementation of services, e.g. the FDN, BDN. .
It is not clear if the first and second bytes should be mandatory when the GSM phase 1 compatibility is not assumed.

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

Identifier: '6Fxx'	Structure: transparent	Mandatory
File size: X bytes, X >= 2	Update activity: low	

Access Conditions:

READ	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

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

-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:	VGCS Group Identifier List (EFVGCS and EFVGCSS)
	Service n°23:	VBS Group Identifier List (EFVBS and EFVBSS)
	Service n°24:	Enhanced Multi-Level Precedence and Pre-emption Service
	Service n°25:	Automatic Answer for Emlpp
	Service n°26:	Image (IMG)
	Service n°27:	SoLSA (Support of Local Service Area)
	Service n°28:	
	Service n°29:	
	Service n°30:	
	Service n°31:	
	Service n°32:	

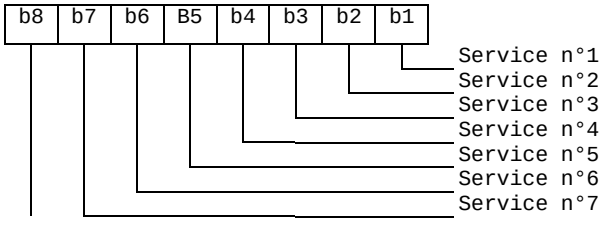
The EF shall contain at least two bytes. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the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

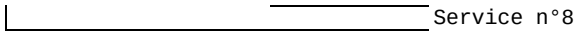
Coding:

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

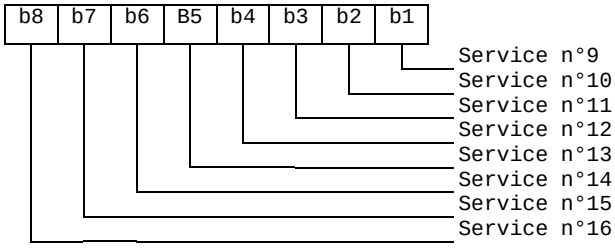
Service available means that the the USIM has the capability to support the service and that the service is available for the user of the USIM.
Service not available means that the service is cannot be used by the USIM user, nevertheless the USIM may have the capability to support the service.

First byte:





Second byte:



etc.

If the USIM supports the FDN feature (FDN allocated and activated) a special mechanism shall exist in the USIM which invalidates both EF_{IMSI} and EF_{LOCI} once during each UMTS session. This mechanism shall be invoked by the USIM automatically if FDN is enabled. This invalidation shall occur at least before the next command following selection of either EF. FDN is enabled when the ADN is invalidated or not activated.

If the USIM supports the BDN feature (BDN allocated and activated) a special mechanism shall exist in the USIM which invalidates both EF_{IMSI} and EF_{LOCI} once during each UMTS session and which forbids the REHABILITATE command to rehabilitate both EF_{IMSI} and EF_{LOCI} until the PROFILE DOWNLOAD procedure is performed indicating that the terminal supports the "Call control by USIM" facility. This mechanism shall be invoked by the USIM automatically if BDN is enabled. The invalidation of EF_{IMSI} and EF_{LOCI} shall occur at least before the next command following selection of either EF. BDN is enabled when the EF_{BDN} is not invalidated.

Editor's note: The mechanisms of FDN and BDN (?) are for further study. The description and service indication may need to be modified accordingly.

4.2.8 EF_{ACM} (Accumulated call meter)

Editor's note: This EF may need to be modified according to the 3G service requirements.

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 GSM 02.86 [9]).

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

Access Conditions:

READ	PIN1
UPDATE	PIN1/PIN2 (fixed during administrative management)
INCREASE	PIN1
INVALIDATE	ADM
REHABILITATE	ADM

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

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

NOTE: If a GSM application is present on the UICC that shall co-operate with this specific USIM application this file is shared between the two applications.

4.2.9 EF_{GID1} (Group Identifier Level 1)

Editor's note: This EF may need to be modified according to the 3G service requirements.

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

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

Access Conditions:

READ	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

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

4.2.10 EF_{GID2} (Group Identifier Level 2)

Editor's note: This EF may need to be modified according to the 3G service requirements.

This EF contains identifiers for particular USIM-terminal 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	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

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

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

4.2.11 EF_{SPN} (Service Provider Name)

Editor's note: If the service provider name is placed in the DIR file the EF could be removed. Further consideration is necessary.

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

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

Access Conditions:

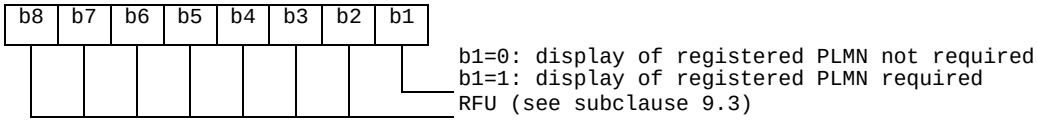
READ	ALWAYS
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

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 [3]).

Coding: see below

Byte 1:



- 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 GSM 03.38 [12] 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 [35].

4.2.12 EF_{PUCT} (Price per unit and currency table)

Editor's note: This EF may need to be modified according to the 3G service requirements.
Is this feature used in Phase 1 ?

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 terminal in conjunction with EF_{ACM} to compute the cost of calls in the currency chosen by the subscriber, as specified in GSM 02.24 [7]. This EF shall always be allocated if EF_{ACM} is allocated.

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

Access Conditions:

READ	PIN1
UPDATE	PIN1/PIN2 (fixed during administrative management)
INVALIDATE	ADM
REHABILITATE	ADM

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

- Currency code

  Contents:

  the alpha-identifier of the currency code.

  Coding:

  bytes 1, 2 and 3 are the respective first, second and third character of the alpha identifier. This alpha-tagging shall use the SMS default 7-bit coded alphabet as defined in GSM 03.38 [12] with bit 8 set to 0.

- Price per unit

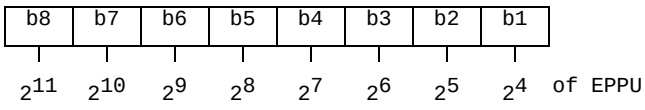
  Contents:

  price per unit expressed in the currency coded by bytes 1-3.

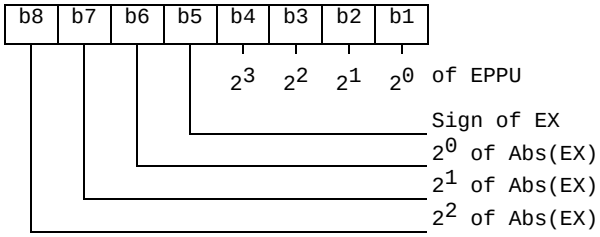
  Coding:

  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 terminal in compliance with GSM 02.24 [7] by the following formula:

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

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

NOTE: If a GSM application is present on the UICC that shall co-operate with this specific USIM application this file is shared between the two applications.

4.2.13 EF_{CBMI} (Cell broadcast message identifier selection)

Editor's note: This EF may need to be modified according to the 3G service requirements.

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

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

Identifier: '6F45'	Structure: transparent	Optional
File size: 2 n bytes	Update activity: low	

Access Conditions:

READ	PIN1
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	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 GSM 03.41, "Message Format on BTS-MS Interface - Message Identifier".
  Values listed show the types of message which shall be accepted by the MS.
  Unused entries shall be set to 'FF FF'.

4.2.15 EF_{ACC} (Access control class)

Editor's note: This EF needs to be modified according to the 3G requirements.
Investigation on requirements necessary (CN?!).

This EF contains the assigned access control class(es). GSM 02.11 [5] refers. The access control class is a parameter to control the RACH utilization. 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 GSM 02.11 [5].

Identifier: '6F78'	Structure: transparent	Mandatory
File size: 2 bytes	Update activity: low	

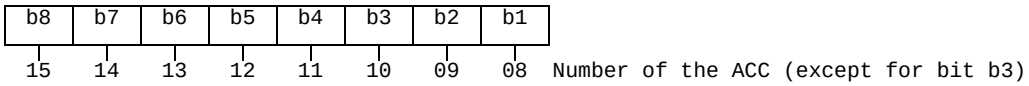
Access Conditions:

READ	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

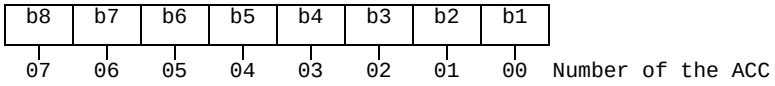
Bytes	Description	M/O	Length
1 - 2	Access control classes	M	2 bytes

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

  Byte 1:



  Byte 2:



4.2.16 EF_{FPLMN} (Forbidden PLMNs)

Editor's note: What about the (unwanted) interoperation of GSM and 3G of the same network operator?

This EF contains the coding for four Forbidden PLMNs (FPLMN). It is read by the terminal as part of the SIM initialization procedure and indicates PLMNs which the MS 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 terminal shall manage the list as follows.

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

When less than four 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 four FPLMNs exist in the EF, for 'FFFFFF' to occur in any position. The terminal 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	PIN1
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	ADM

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

- PLMN

  Contents:

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

  Coding:

  according to GSM 04.08 [15].

  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 4 PLMNs is required, the unused bytes shall be set to 'FF'.

NOTE: If a GSM application is present on the UICC that shall co-operate with this specific USIM application this file is shared between the two applications.
The four records of the GSM application are mapped to the first four records in this EF.

4.2.17 EF_{LOCI} (Location information)

Editor's note: This EF may need to be modified according to the 3G requirements.
S3 spec required on TMSI usage.
Mobility Management: LAI

This EF contains the following Location Information:

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

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

Access Conditions:

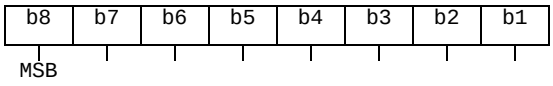
READ	PIN1
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	PIN1

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

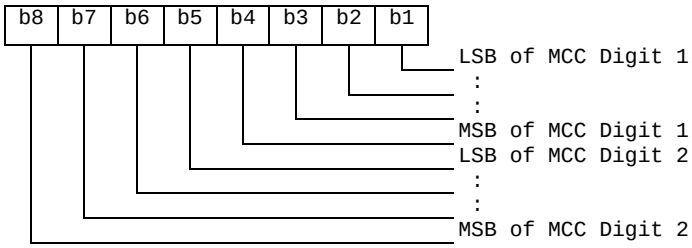
- TMSI

  Contents: Temporary Mobile Subscriber Identity

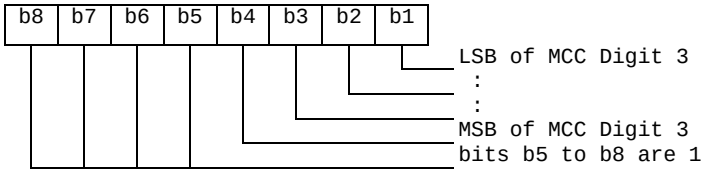
  Coding: according to GSM 04.08 [15].



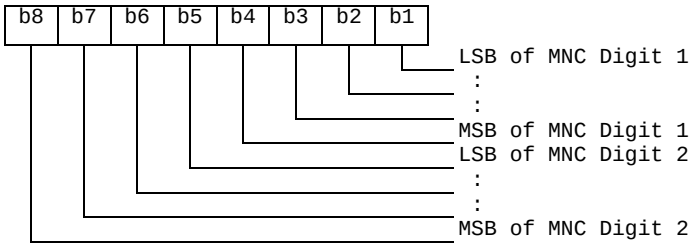
- LAI
  Contents: Location Area Information
  Coding: according to GSM 04.08 [15].



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 GSM 04.08 [15].
  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 subclause 9.3).

4.2.18 EF_{AD} (Administrative data)

Editor's note: This EF may need to be modified according to the 3G requirements.
T1: Used modes.

Editor's note: Should this be moved to 31.101?
It might be unlikely to be seen that a USIM for normal operation will be installed on a UICC that had another application for type approval.

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 terminal 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 terminal manufacturer to perform specific proprietary auto-test in its terminal during e.g. maintenance phases).

It also provides an indication of whether some terminal features should be activated during normal operation.

Identifier: '6FAD'	Structure: transparent	Mandatory
File size: 3+X bytes	Update activity: low	

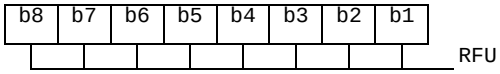
Access Conditions:

READ	ALW
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

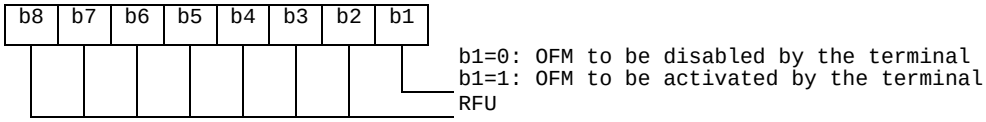
Bytes	Description	M/O	Length
1	MS operation mode	M	1 byte
2 - 3	Additional information	M	2 bytes
4 - 3+X	RFU	O	X bytes

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

- Additional information
  Coding:
  - specific facilities (if b1=1 in byte 1);
  Byte 2 (first byte of additional information):



  Byte 3:



  - terminal 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
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 – 2	USIM Release	M	2 bytes
3	USIM Version	M	1 byte
4	Operator Indication	M	1 byte
5-X	RFU	O	X-4 bytes

Coding:

'00' : The USIM based on the version of the present document approved by TSG-T in December 1999.

All other codings are reserved for specification by 3GPP.

- USIM Release

Contents:
Indicates the TSG-T approved release of the 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', [xx]

- 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)

Editor's note: This EF may need to be modified according to the 3G requirements.

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	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	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 GSM 03.41 [14]. Values listed show the identifiers of messages which shall be accepted by the MS to be passed to the USIM.

  Unused entries shall be set to 'FF FF'.

4.2.21 EF_{ECC} (Emergency Call Codes)

Editor's note: Should this EF be moved to DF Telecom?
Change Update condition to PIN1 ?

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:

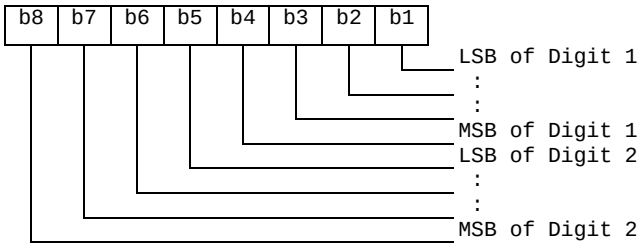
READ	ALW
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

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

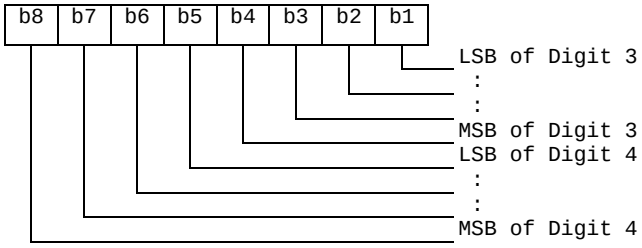
- Emergency Call Code
  Contents:
  Emergency Call Code

  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 that 6 digits is chosen, then the unused nibbles shall be set to 'F'.

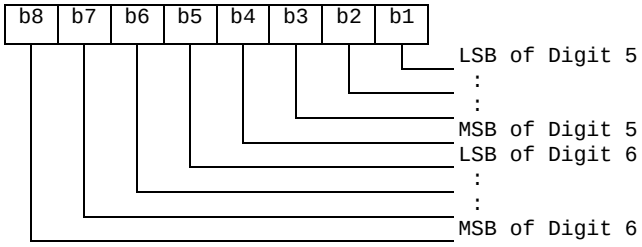
  Byte 1:



Byte 2:



Byte 3:



4.2.22 EF_{CBMIR} (Cell broadcast message identifier range selection)

Editor's note: This EF may need to be modified according to the 3G service requirements.

This EF contains ranges of cell broadcast message identifiers that the subscriber wishes the MS 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	PIN1
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	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 GSM 03.41 [14] "Message Format on BTS-MS Interface - Message Identifier". Values listed show the ranges of messages which shall be accepted by the MS.
  Unused entries shall be set to 'FF FF FF FF'.

.

4.2.24 $EF_{LOCIGPRS}$ (GPRS location information)

Editor's note: This EF may need to be modified according to the 3G requirements. It is necessary to confirm if the EF (and GPRS) is mandatory for the 3GPP system.

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	Mandatory
File size: 14 bytes	Update activity: high	

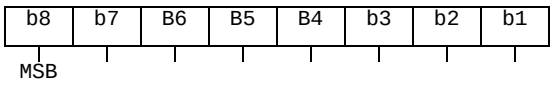
Access Conditions:

READ	PIN1
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 – 4	P-TMSI	M	4 bytes
5 – 7	P-TMSI signature value	M	3 bytes
8 – 13	RAI	M	6 bytes
14	Routing Area update status	M	1 byte

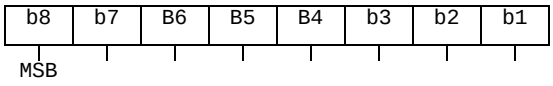
- P-TMSI
  Contents: Packet Temporary Mobile Subscriber Identity
  Coding: according to GSM 04.08 [15].

  Byte 1: first byte of P-TMSI



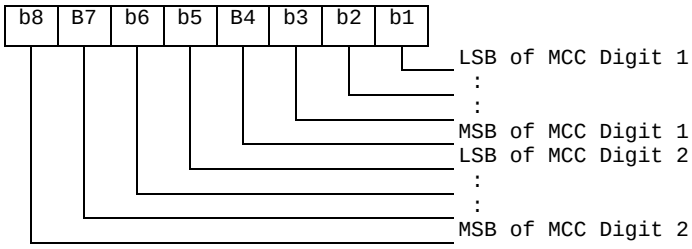
- P-TMSI signature value
  Contents: Packet Temporary Mobile Subscriber Identity signature value
  Coding: according to GSM 04.08 [15].

  Byte 5: first byte of P-TMSI signature value

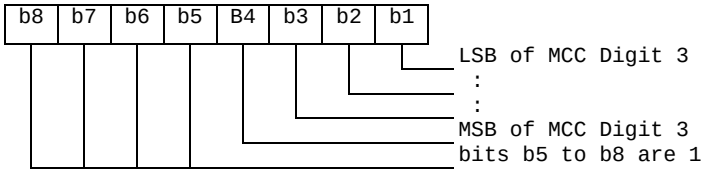


- RAI
  Contents: Routing Area Information
  Coding: according to GSM 04.08 [15].

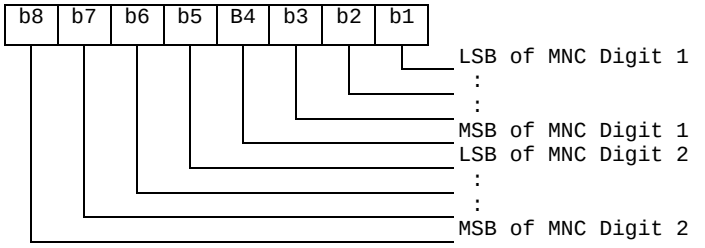
  Byte 8: first byte of RAI



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 GSM 04.08 [15].
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 subclause 9.3).

4.2.25 EF_{FDN} (Fixed dialling numbers)

Editor's note: This EF may be modified according to the implementation of the FDN / BDN machanism that is still under definition.

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. 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	PIN1
UPDATE	PIN2
INVALIDATE	ADM
REHABILITATE	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	Extension2 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of the EF_{ADN} (subclause 4.4.1), 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}.

4.2.26 EF_{SMS} (Short messages)

Editor's note: This EF may need to be modified according to the 3G requirements.
The interaction with GSM is for further study

This EF contains information in accordance with GSM 03.40 [13] comprising short messages (and associated parameters) which have either been received by the MS from the network, or are to be used as an MS originated message.

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

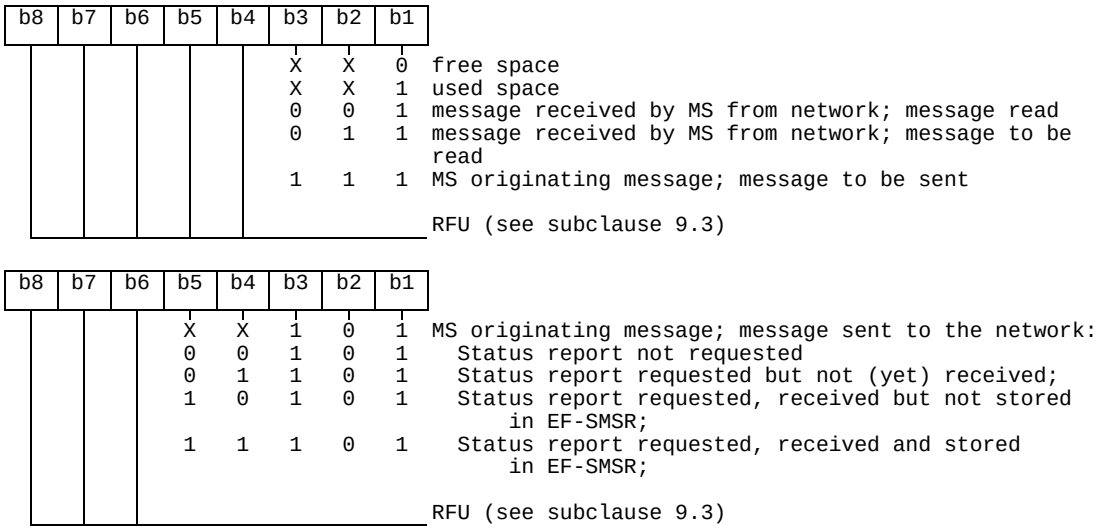
Access Conditions:

READ	PIN1
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	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 SEEK command. For MS originating messages sent to the network, the status shall be updated when the MS receives a status report, or sends a successful SMS Command relating to the status report.

  Coding:



- Remainder
  Contents:
  This data item commences with the TS-Service-Centre-Address as specified in GSM 04.11 [16]. The bytes immediately following the TS-Service-Centre-Address contain an appropriate short message TPDU as specified in GSM 03.40 [13], with identical coding and ordering of parameters.
  Coding:
  according to GSM 03.40 [13] and GSM 04.11 [16]. Any TP-message reference contained in an MS originated message stored in the SIM, 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 terminal shall store in the SIM 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.

4.2.27 EF_{MSISDN} (MSISDN)

Editor's note: This EF may need to be modified to store numbers for e.g. Fax and Data as well (The note comes from T3#2(99)052. The intention of the note should be confirmed.). The Access condition of UPDATE was modified based on the agreement in T3#4 (refer to T3#4(99)113).

This EF contains MSISDN(s) related to the subscriber. In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. 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	PIN1
UPDATE	PIN1/ADM (fixed during administrative management)
INVALIDATE	ADM
REHABILITATE	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

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

NOTE 1: If the USIM stores more than one MSISDN number and the terminal displays the MSISDN number(s) within the initialization procedure then the one stored in the first record shall be displayed with priority.

NOTE 2: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

4.2.28 EF_{SMSP} (Short message service parameters)

Editor's note: This EF may need to be modified according to the 3G requirements.

This EF contains values for Short Message Service header Parameters (SMSP), which can be used by the terminal 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 MS, 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	PIN1
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	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 4.4.1 (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 terminal 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 GSM 03.40 [13].

- TP-Service Centre Address
  Contents and Coding: As defined for RP-Destination address Centre Address in GSM 04.11 [16].

- TP-Protocol Identifier
  Contents and Coding: As defined in GSM 03.40 [13].

- TP-Data Coding Scheme
  Contents and Coding: As defined in GSM 03.38 [12].

- TP-Validity Period
  Contents and Coding: As defined in GSM 03.40 [13] for the relative time format.

4.2.29 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	PIN1
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	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 GSM 03.40 [13].
  Coding:
  as defined in GSM 03.40 [13].

- 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 MS becomes available, the Network can be informed. The process for this is described in GSM 03.40 [13].
  Coding:
  b1=1 means flag unset; memory capacity available
  b1=0 means flag set
  b2 to b8 are reserved and set to 1.

4.2.30 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. It may also contain associated alpha-tagging.

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

Access Conditions:

READ	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	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 4.4.1), 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}.

4.2.31 EF_{EXT2} (Extension2)

This EF contains extension data of an FDN/SSC (see EXT2 in 10.4.2).

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

Access Conditions:

READ	PIN1
UPDATE	PIN2
INVALIDATE	ADM
REHABILITATE	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 10.4.10 (EF_{EXT1}).

4.2.32 EF_{EXT3} (Extension3)

This EF contains extension data of an SDN (see EXT3 in 10.4.9).

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

Access Conditions:

READ	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	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 10.4.10 EF_{EXT1}.

4.2.33 EF_{SMSR} (Short message status reports)

Editor's note: This EF may need to be modified according to the 3G requirements.

This EF contains information in accordance with GSM 03.40 [13] comprising short message status reports which have been received by the MS 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	PIN1
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	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 GSM 03.40 [13], with identical coding and ordering of parameters.
  Coding:
  according to GSM 03.40 [13]. Any bytes in the record following the TPDU shall be filled with 'FF'.

4.2.34 EF_{ICI} (Incoming Call Information)

This EF is application related and 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 is stored in this EF. This EF can also contain an alpha identifier that may be supplied with the incoming call. This EF is of cyclic structure and contains a limited amount of entries. When the EF is full the next entry overwrites the first entry in the file.

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 terminal if the code for the secret entry has not been verified. The terminal shall not ask for the secret code to be entered at this point.

The public part of the phone book is located in $DF_{TELECOM}$ where as the application specific phone book files are located within the USIM. In order to link the correct phone book and the correct entry to the incoming call information, an indication of where the phone book is located is provided. The indication of the phone book location is through EF_{DIR}. Each record in EF_{ICI} contains a reference pointer to the application ID/path in EF_{DIR}. The location of $DF_{TELECOM}$ is specified in the EF_{DIR} as well as the location of the USIM application.

As the phone book may consist of more than one EF_{ADN} with associated information the record in EF_{ICI} shall be linked to the correct EF_{ADN} and the correct record in EF_{ADN}. Linking is achieved by referring to the appropriate reference file and the record number in the reference file (this gives the correct EF_{ADN}).

Each record in the reference file contains a list of EFs associated with the EF_{ADN} and the file ID of the EF_{ADN} itself (this gives the EF_{ADN} location). Each record in the EF_{ICI} also contains a pointer to the record in EF_{ADN} (this gives the location of the record in EF_{ADN}).

This allows the usage of one EF_{ICI} to be associated with several EF_{ADN} files. The structure of EF_{ICI} is shown in table 13. The number content is coded using the rules for EF_{ADN} .

Table 13: Structure of EF_{ICI}

Identifier: 'XXXX'	Structure: Cyclic	Optional
Record length: X+26 bytes	Update activity: high	

Access Conditions:

READ	PIN1
UPDATE	PIN1
INVALIDATE	PIN2
REHABILITATE	PIN2

Bytes	Description	M/O	Length
1 - X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2 - X+11	Incoming Call Number/SSC String	M	10 bytes
X+12 – X+19	Incoming call date and time (see detail 1)	M	8 bytes
X+20 – X-22	Incoming call duration (see detail 2)	M	3 bytes
X+23	Incoming call status (see detail 3)	M	1 byte
X+24	Pointer to application in EF_{DIR}	M	1 byte
X+25	Pointer to Phone book reference file record ID (see note)	M	1 byte
X+26	Pointer to ADN record number ID/EXT1 record ID	M	1 byte

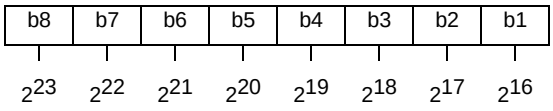
Note: If the reference file record ID, byte 25, is set to 'FF' it indicates that no link to the phone book exists. In this case the value in byte X+26 is pointing to a record in the EXT1 file.

Detail 1 Coding of date and time

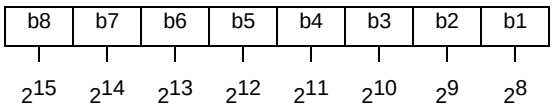
The date and time is coded on 4 bytes. The coding used is BCD. Byte 1 encodes the day, byte 2 the month and the year is coded over bytes 3 and 4. (dd.mm.yyyy). The time is coded over 3 bytes. Byte 5 encodes the hour, byte 6 the minute and byte 7 the second (hh.mm.ss).

Detail 2 Coding of call duration

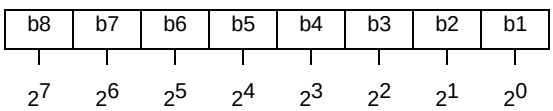
First byte:



Second byte:

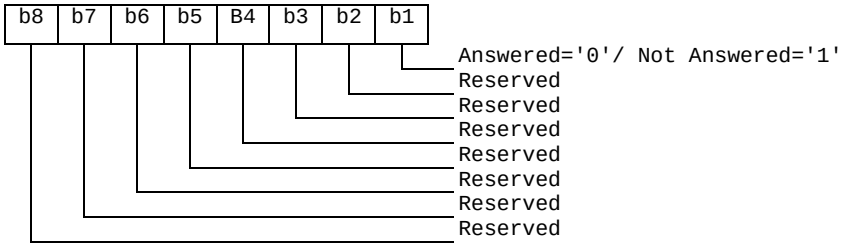


Third byte:



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

Detail 3 Coding of Call status



4.2.35 EF_{OCI} (Outgoing Call Information)

Editor's Note: The identical identifier to EF_{LDN} ('6F44') can be used for EF_{OCI}.

This EF is application related and 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 is stored in this EF. This EF is of cyclic structure and contains a limited amount of entries. When the EF is full the next entry overwrites the first entry in the file.

If the dialled phone number matches a number stored in the phone book the outgoing call information is linked to the corresponding information in the phone book. If no match is found in the phone book the pointers to the phone book reference file record ID and pointer to index administration file record number/ID are set to 'FF'. 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 terminal, if the hidden code has not been verified. The terminal shall not perform hidden code verification at this point.

The public part of the phone book is located in $DF_{TELECOM}$ where as the application specific phone book is located within the USIM. In order to link the correct phone book and the correct entry to the incoming call information and indication of where the phone book is located shall be provided. The indication of the phone book location is through EF_{DIR}. Each record in EF_{OCI} contains a reference pointer to the application ID/path in EF_{DIR}. The location of $DF_{TELECOM}$ is specified in EF_{DIR} as well as the location of the USIM application.

As the phone book may consist of more than one EF_{ADN} with associated information the record in EF_{ICI} shall be linked to the correct EF_{ADN} and the correct record in EF_{ADN}. Linking is achieved by referring to the appropriate reference file and the record number in the reference file (this gives the correct EF_{ADN}).

Each record in the reference file contains a list of EFs associated with the EF_{ADN} and the file ID of the EF_{ADN} itself (this gives the EF_{ADN} location). Each record in the EF_{OCI} also contains a pointer to the record EF_{ADN} (this gives the location of the record in EF_{ADN}).

This allows the usage of one EF_{OCI} to be associated with several EF_{ADN} files. The structure of EF_{OCI} is shown in table 14. The number content is coded using the rules for EF_{ADN} . The encoding of the date and time is the same as for EF_{ICI}

Table 14: Structure of EF_{OCI}

Identifier: 'XXXX'	Structure: Cyclic	Mandatory
Record length: 25 bytes	Update activity: high	
Access Conditions: READ PIN1 UPDATE PIN1 INVALIDATE PIN2 REHABILITATE PIN2		

Bytes	Description	M/O	Length
1	Length of BCD number/SSC contents	M	1 byte
2 - 11	Outgoing Call Number/SSC String	M	10 bytes
12 – 19	Outgoing call date and time	M	8 bytes
20 – 22	Outgoing call duration	M	3 bytes
23	Pointer to application in EF_{DIR}	M	1 byte
24	Pointer to Phone book reference file record ID (see note)	M	1 byte
25	Pointer to ADN record number ID/EXT1 record ID	M	1 byte

Note: If the reference file record ID is set to 'FF' it indicates that no link to the phone book exists. In this case the value in byte X+25 is pointing to the record EXT1 file

4.2.36 EF_{ICT} (Incoming Call Counter)

This EF contains the accumulated call counter value for the current call and previous calls. The EF is USIM specific and resides within the USIM application. The structure of EF_{ICT} is shown in table 15.

Table 15: Structure of EF_{ICT}

Identifier: '6FXX'	Structure: cyclic	Optional
Record length: 3 bytes	Update activity: high	
Access Conditions: READ PIN1 UPDATE PIN1/PIN2 (fixed during administrative management) INCREASE PIN1 INVALIDATE ADM REHABILITATE ADM		

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

Coding:

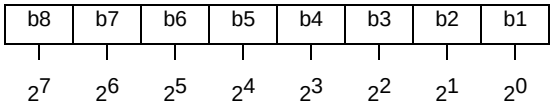
First byte:

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:



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

4.2.37 EF_{OCT} (Outgoing Call Counter)

This EF contains the accumulated call counter value for the current call and previous calls. The EF is USIM specific and resides within the USIM application. The structure of EF_{OCT} is shown in table

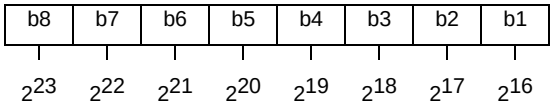
Table 15: Structure of EF_{OCT}

Identifier: '6FXX'	Structure: cyclic	Optional
Record length: 3 bytes	Update activity: high	
Access Conditions: READ PIN1 UPDATE PIN1/PIN2 (fixed during administrative management) INCREASE PIN1 INVALIDATE ADM REHABILITATE ADM		

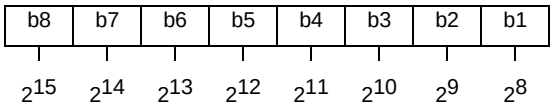
Bytes	Description	M/O	Length
1 - 3	Accumulated count of units	M	3 bytes

Coding:

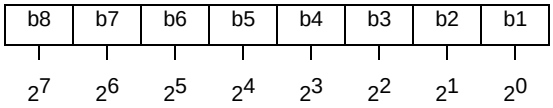
First byte:



Second byte:



Third byte:



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

4.2.38 Files required for 2G Access

The EFs described in this chapter are mandatory for if the USIM application shall be able to gain network access through a GSM radio path.

The presence of these files and thus the support of a 2G access is indicated in the 'USIM Service Table' as service no. 'xx tbd' being allocated and activated.

4.2.38.1 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.

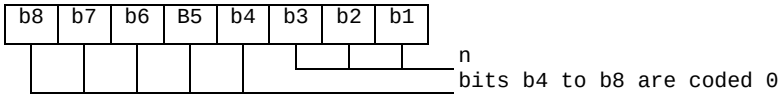
Identifier: '6F20'	Structure: transparent	Mandatory
File size: 9 bytes	Update activity: high	

Access Conditions:

READ	PIN1
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 – 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: GSM 04.08 [15] defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administrative phase.

4.2.38.2 EF_{ACC} (Access control class)

Editor's note: Deviating from the general working assumption that all services are similar to GSM if not specified otherwise, for these feature it is assumed that the implementation differs between 2G and 3G. Should this not be the case than this could become a shared file, too.

This EF contains the assigned access control class(es). GSM 02.11 [5] refers. The access control class is a parameter to control the RACH utilization. 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 GSM 02.11 [5].

Identifier: '6F78'	Structure: transparent	Mandatory
File size: 2 bytes	Update activity: low	

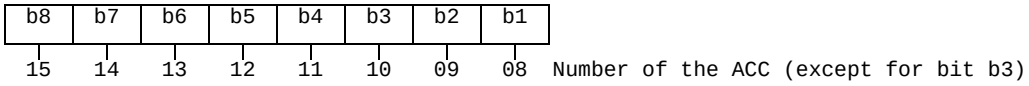
Access Conditions:

READ	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

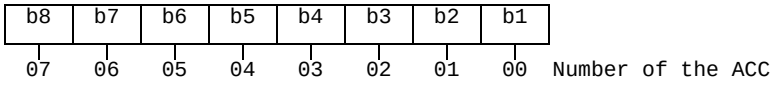
Bytes	Description	M/O	Length
1 - 2	Access control classes	M	2 bytes

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

Byte 1:



Byte 2:



4.2.38.3 EF_{KcGPRS} (GPRS Ciphering key KcGPRS)

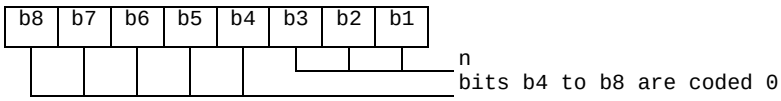
This EF contains the ciphering key KcGPRS and the ciphering key sequence number n for GPRS (see GSM 03.60 [32]).

Identifier: '6F52'	Structure: transparent	Mandatory
File size: 9 bytes	Update activity: high	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

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

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

- Ciphering key sequence number n for GPRS
  Coding:



NOTE: GSM 04.08 [15] defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administrative phase.

4.2.38.4 $EF_{LOCIGPRS}$ (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

Identifier: '6F53'	Structure: transparent	Mandatory
File size: 14 bytes	Update activity: high	

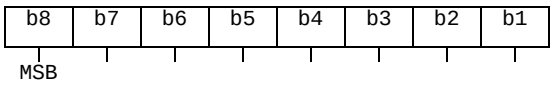
Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - 4	P-TMSI	M	4 bytes
5 – 7	P-TMSI signature value	M	3 bytes
8 - 13	RAI	M	6 bytes
14	Routing Area update status	M	1 byte

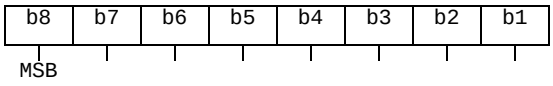
- P-TMSI
  Contents: Packet Temporary Mobile Subscriber Identity
  Coding: according to GSM 04.08 [15].

  Byte 1: first byte of P-TMSI



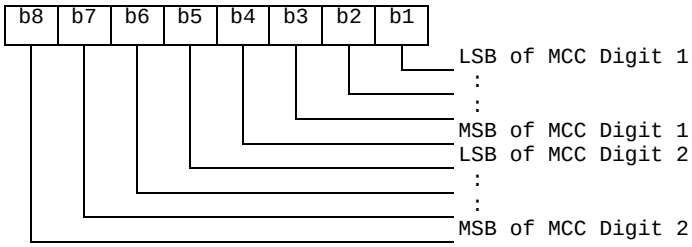
- P-TMSI signature value
  Contents: Packet Temporary Mobile Subscriber Identity signature value
  Coding: according to GSM 04.08 [15].

  Byte 1: first byte of P-TMSI signature value

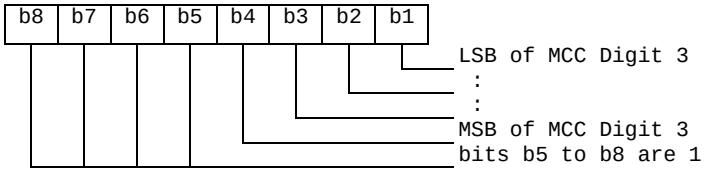


- RAI
  Contents: Routing Area Information
  Coding: according to GSM 04.08 [15].

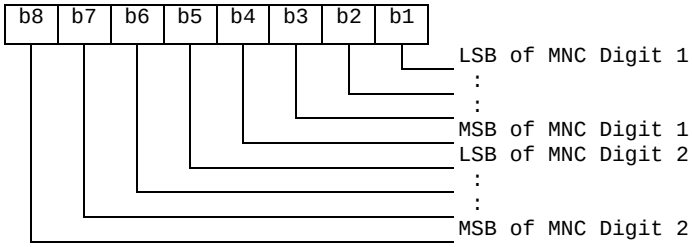
  Byte 5: first byte of RAI



  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 GSM 04.08 [15].
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 (see subclause 9.3).

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:

- $DF_{GRAPHICS}$ '5F50'
- DF_{SoLSA} '5F70'
- $DF_{PHONEBOOK}$ '5F3A'

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

Editor's note (6-SEP-99:Kobayashi) Need to check File ID value.

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

4.4.1 Contents of file at the ADF (Application DF) SoLSA level

This subclause specifies the EFs in the dedicated file DF_{SoLSA}. It only applies if the SoLSA feature is supported (see GSM 03.73 [33]).

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 MS 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 MS is out of the served area(s).

Identifier: '4F30'	Structure: transparent	Optional
Record length: X+1 bytes	Update activity: low	

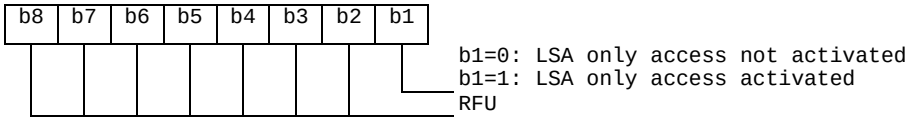
Access Conditions:

READ	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	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 MS is restricted to use LSA cells only or not.

  Coding:



- LSA only access indication text

  Contents: text to be displayed by the terminal when it's out of LSA area.

  Coding: the string shall use either
  - the SMS default 7-bit coded alphabet as defined in GSM 03.38 [12] 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 Annex B.

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	PIN1
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	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 terminal 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 GSM 03.38 [12] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF',

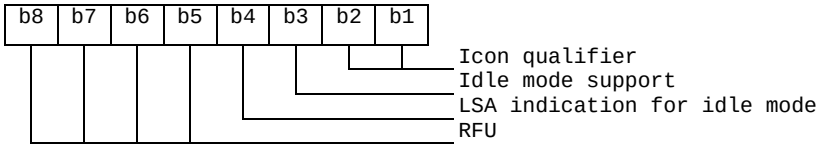
or

- one of the UCS2 coded options as defined in the annex of 3G TS 31.101 [35].

- 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 terminal 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 terminal 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 terminal shall display the LSA name when the terminal 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 subclause 9.3).

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

- Priority:
Contents: Priority of the LSA which gives the terminal the preference of this LSA relative to the other LSAs.
Coding: binary. '00' is lowest priority 'FF' is highest.

- PLMN code:
Contents: MCC + MNC for the LSA.
Coding: according to GSM 04.08 [15] 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 H.

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

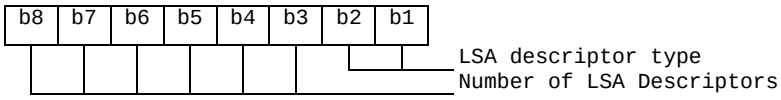
Access Conditions:

READ	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

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

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

  Coding:



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

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

- LSA Descriptor:
  Contents:
  Dependant of the coding indicated in the LSA descriptor type:
  - in case of LSA ID the field length 'X' is 3 bytes,
  - in case of LAC + CI the field length 'X' is 4 bytes,
  - in case of CI the field length 'X' is 2 bytes,
  - in case of LAC the field length 'X' is 2 bytes,
    Coding: according to GSM 04.08 [15].

- 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 6.6.

4.4.2 Contents of files at the ADF (Application DF) GRAPHICS level

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

4.4.2.1 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 USIM, 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	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	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	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 G;
'21' - colour image coding scheme as defined in annex G;
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 10.5.1.2), 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.

4.4.2.2 Image Instance Data Files

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

Identifier: '4FXX'	Structure: transparent	Optional
Record length: Y bytes	Update activity: low	

Access Conditions:

READ	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

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

Contents and coding:

Image instance data are accessed using the image instance descriptors provided by EF_{IMG} (see subclause 10.5.1.1).

The identifier '4FXX' shall be different from one image instance data file to the other. For the range of 'XX', see subclause 6.6. The length Y may be different from one image instance data file to the other.

4.4.3 Contents of files at the ADF (Application DF) PHONEBOOK level

This $DF_{PHONEBOOK}$ under ADF has the same contents as the $DF_{PHONEBOOK}$ under $DF_{TELECOM}$

The phone book related EFs are located under the DF $_{PHONEBOOK}$.

The UICC may contain either application specific or global phone book entities, or both in parallel.
- In case of an USIM application specific phone book this DF is located under the Application DF_{USIM}.
- In case of a global phone book on the UICC this DF is located under $DF_{TELECOM}$.

In case of a GSM application residing on the UICC the EFs ADN and EXT1 are mapped to $DF_{TELECOM}$ with their FIDs specified in GSM 11.11 [xx], i.e. EF_{ADN} = '6F3A' and EF_{EXT1} = '6F4A', respectively.

Editor's note: Can only the global phone book EFs be mapped to DF Telecom or also the application specific EFs in the USIM?
Which EFs will be mapped in case of both phone books being present (global and specific)?

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 PIN1. The application specific phone book is a copy of the file structure of the one specified for the public phone book under $DF_{PHONEBOOK}$. The application specific phonebook may contain a different set of files than the on in the public area under $DF_{TELECOM}$.

4.4.3.1 EF_{PBR} (Phone Book Reference file)

This file describes the structure of in this case the phonebook. The reference file is a file that contains information how the information in the different files are to be combined together to form a phonebook entry. The reference file contains records. Each record specifies the structure of up to 254 entries in the phone book. Each entry consists of data stored in files indicated in the reference file record. The Entry structure shall be the same over all the records. If more than 254 entries are to be stored, a second record is needed in the reference file. The different TLV objects that are stored in an 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 are files that contains as many records as the reference/master file (EF_{ADN}, EF_{ADN1}) are linked on record number bases (Rec1 -> Rec1). The master file record number is the reference

- Type 2 files are files that contains less entries than the master file 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_{PAS})

Table 1: Phone Book Reference file Constructed Tags

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

File IDs indicated using constructed Tag 'XZ' indicates 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 2: Tag definitions for the phone book type of file

Tag Value	TAG Description
'X0'	EF_{ADN} data object
'X1'	EF_{IAP} data object
'X2'	EF_{EXT1} data object
'X3'	EF_{SNE} data object
'X4'	EF_{ANR} data object
'X5'	EF_{EML} data object
'X6'	EF_{PBC} data object
'X7'	EF_{GRP} data object
'X8'	EF_{PAS} data object
'X9'	EF_{UID} data object

Table 3: Phone Book Reference file EF_{PBR} structure

Identifier: '4F30'		Structure: linear fixed		Optional
SFI: -				
Record Length: X bytes		Update activity: low		
Access Conditions: READ PIN1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM				
Bytes	Description		M/O	Length
1 - X	TLV object(s) for indicating EFs that are part of the phone book structure		M	X bytes

4.4.3.2 EF_{IAP} (Index Administration file)

This file is present if Tag 'XY' 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} is the same as the order of file IDs that appear in the TLV object indicated by Tag 'XY' in the reference file record.

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.

Table 4: Index administration file EF_{IAP} structure

Identifier: '4FXX'	Structure: linear fixed	Optional
SFI: mandatory		
Record Length: X bytes	Update activity: high	

Access Conditions:

READ	PIN1
UPDATE	PIN1
INVALIDATE	ADM
REHABILITATE	ADM

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

Note: The amount of bytes in a record is equal to the number of files indicated the EF_{PBR} following tag 'XY'

4.4.3.3 EF_{ADN} (Abbreviated dialling numbers)

The phone book is an extension of the existing ADN feature in the GSM SIM. The existing ADN feature contains the EF_{ADN} and EF_{EXT1}. These two data fields are mandatory in the phone book for GSM compatibility.

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

Identifier: '4F3A'	Structure: linear fixed	Mandatory
SFI: mandatory		
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	CHV2
REHABILITATE	CHV2

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 GSM 03.38 [12] 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 Annex B.

NOTE 1: The value of X may be from zero to 241. Using the command GET RESPONSE the terminal 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 10.5.10).

  Coding:

  according to GSM 04.08 [15].

- TON and NPI

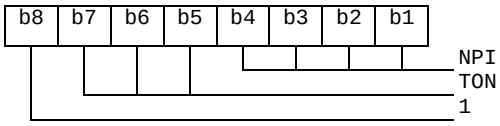
  Contents:

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

  Coding:

  according to GSM 04.08 [15]. 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 terminal (see note 2).

NOTE 2: If a dialling number is absent, no TON/NPI byte is transmitted over the radio interface (see GSM 04.08 [15]). Accordingly, the terminal should not interpret the value 'FF' and not send it over the radio interface.



- Dialling Number/SSC String

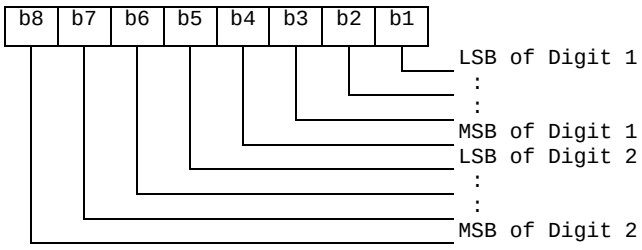
  Contents:

  up to 20 digits of the telephone number and/or SSC information.

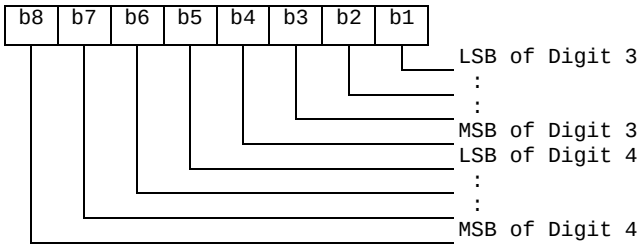
  Coding:

  according to GSM 04.08 [15] , GSM 02.30 [8] 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 10.5.10).
  Coding:
  binary.

NOTE 3: As EF_{ADN} is part of the $DF_{TELECOM}$ it may be used by GSM and also other applications in a multi-application card. If the non-GSM application does not recognize 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 GSM 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 [19] numbering plan

	TON	NPI	Digit field
GSM application	001	0001	abc...
Other application compatible with GSM	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 terminal acts upon the EF_{ADN} with a SEEK command in order to identify a character string in the alpha-identifier, it is the responsibility of the terminal to ensure that the number of characters used as SEEK parameters are less than or equal to the value of X if the MMI allows the user to offer a greater number.

Table 12: Extended BCD coding

BCD Value	Character/Meaning
'0'	"0"
...	...
'9'	"9"
'A'	"*"
'B'	"#"
'C'	DTMF Control digit separator (GSM 02.07 [3])
'D'	"Wild" value This will cause the MMI to prompt the user for a single digit (see GSM 02.07 [3]).
'E'	Expansion digit ("Shift Key"). It has the effect of adding '10' to the following digit. The following BCD digit will hence be interpreted in the range of '10'-'1E'. The purpose of digits in this range is for further study.
'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: The interpretation of values 'D', 'E' and 'F' as DTMF digits is for further study.

NOTE 6: A second or subsequent 'C' BCD value will be interpreted as a 3 second PAUSE (see GSM 02.07 [3]).

4.4.3.4 EF_{EXT1} (Extension1)

This EF contains extension data of an ADN/SSC, an MSISDN, or an LND. Extension data is caused by:

- an ADN/SSC (MSISDN, LND) which is greater than the 20 digit capacity of the ADN/SSC (MSISDN, LND) 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, LND) 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.

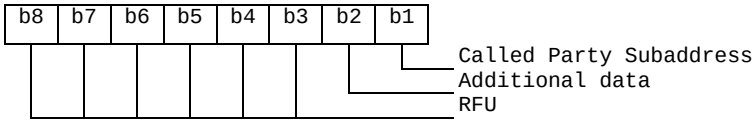
Identifier: '4F4A'	Structure: linear fixed	Mandatory
SFI: recommended		
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

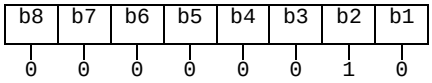
Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

- 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":

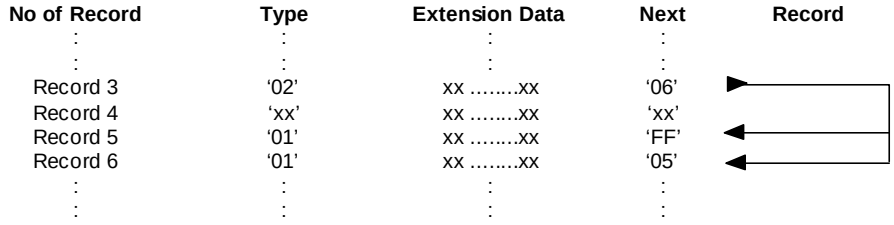


- Extension data
  Contents: Additional data or Called Party Subaddress depending on record type.
  Coding:
  Case 1, Extension1 record is additional data:
  The first byte of the extension data gives the number of bytes of the remainder of ADN/SSC (respectively MSISDN, LND). The coding of remaining bytes is BCD, according to the coding of ADN/SSC (MSISDN, LND). 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 GSM 04.08 [15]. All information defined in GSM 04.08, except the information element identifier, shall be stored in the SIM. 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.



  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).

4.4.3.5 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 entry control information and the hidden information.

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}).

Table 5: Structure of EF_{PBC}

Identifier: '4FXX'	Structure: linear fixed	Optional
SFI: recommended		
Record length: 2 bytes	Update activity: low	

Access Conditions:

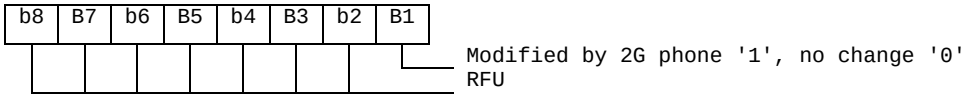
READ	PIN1
UPDATE	PIN1
INVALIDATE	PIN2 ?
REHABILITATE	PIN2 ?

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

- Entry Control Information

  Contents: provides some characteristics about the phone book entry (eg modification by a 2G mobile)

  Coding:



- Hidden Information

  Contents: Indicates to which USIM/GSM subscription of the UICC this entry belongs, so that the corresponding secret code can be verified to display the entry, other wise the entry is hidden.

Coding:
'00' – the phone book entry is not hidden
record number in EF_{DIR} of the associated USIM/GSM application

4.4.3.6 EF_{GRP} (Grouping file)

This EF contains the grouping information for each phone book entry. This file contains as many records than the associated EF_{ADN}. Each record contains a list of group identifiers the entry is belonging to.

Table 6: Grouping file EF_{GRP} structure

Identifier: '4FXX'	Structure: linear fixed		Optional
SFI: recommended			
Record Length: X bytes (1 ≤ X ≤10)		Update activity: high	
Access Conditions: READ PIN1 UPDATE PIN1 INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1	Group Name Identifier 1	M	1 byte
2	Group Name Identifier 2	O	1 byte
X	Group Name Identifier X	O	1 byte

- 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_{PAS}.
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_{PAS}

4.4.3.7 EF_{PAS} (Phone Book text information data field)

This file contains the alpha strings that are associated with the group name referred by EF_{GRP} and the user defined naming tag in EF_{ANR}.

ID following tag indicating user defined naming in EF_{SNE} points to a record number in EF_{PAS}. The alpha string stored in this EF is displayed by the terminal as the grouping information. The structure of this EF is as follows.

Table 7 Structure of EF_{PAS}

Identifier: '4FXX'	Structure: linear fixed		Mandatory
SFI: optional			
Record length: X bytes		Update activity: low	
Access Conditions: READ PIN1 UPDATE PIN1 INVALIDATE PIN2 ? REHABILITATE PIN2 ?			
Bytes	Description	M/O	Length
1 to X	Alpha text string	M	X bytes

- Alpha text string

Content: Group names and user defined text for additional number

Coding: same as the alpha identifier in EF_{ADN}.

4.4.3.8 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 weather the record is free or the type of number referring to the record number in EF_{PAS}, 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.

Table 8: Structure of EF_{ANR}

Identifier: '4FXX'	Structure: linear fixed	Optional
SFI: mandatory		
Record length: X+3 bytes	Update activity: low	

Access Conditions:

READ	PIN1
UPDATE	PIN1
INVALIDATE	PIN2 ?
REHABILITATE	PIN2 ?

Bytes	Description	M/O	Length
1	Type of Number identifier	M	1 byte
2-11	Additional number	M	10 bytes
12	ADN file SFI	O	1 byte
13	ADN file Record Identifier	O	1 byte

- Type of Number Identifier

  Content: describes the type of the additional number defined in the file EF_{PAS}.

  Coding:
  '00' – no additional number description
  'xx' – record number in EF_{PAS} 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

NOTE: 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 constellations these two bytes shall be present.

4.4.3.9 EF_{SNE} (Second Name)

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}. If the amount second name records are equal to the amount of ADN records byte X+2 is set to FF and the EF_{SNE} file ID is indicated in the reference file record using tag 'XX'. The structure of the EF_{SNE} (Second NamE) is identical to that of EF_{ADN} but the actual number information is missing. The amount of EF_{ADN} records

may exceed 254 and are then split into two data fields. In order to link the second name record to the correct EF_{ADN} entry the control information in a second name record contains a pointer to the reference file record identifier from where the correct EF_{ADN} can be found.

Table 9: Structure of EF_{SNE}

Identifier: '4FXX'	Structure: linear fixed	Optional
SFI: mandatory		
Record length: X+2 bytes	Update activity: low	
Access Conditions: READ PIN1 UPDATE PIN1 INVALIDATE PIN2 ? REHABILITATE PIN2 ?		

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

NOTE: 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 constellations these two bytes shall be present.

4.4.3.10 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 identifier (PID), a unique identifier for each phone book entry (UID) and change counter (CC) to indicate recent changes.

The synchronisation method is provided and used by the terminal (add reference to T2) in such a way that it can detect changes on the phone book by the means of the above identifiers and manage the synchronisation accordingly.

4.4.3.10.1 EF_{UID} (Unique Identifier)

For each phone book entry a unique identifier (UID) is assigned by the USIM application when the entry is created. This value unambiguously identifies a phone book record and does not change as long as the record exists.

Table 10: Structure of EF_{UID}

Identifier: '4F21'		Structure: linear fixed		Optional
SFI: optional				
Record length: 2 bytes		Update activity: low		
Access Conditions: READ PIN1 UPDATE PIN1 INVALIDATE PIN2 ? REHABILITATE PIN2 ?				
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: tbd, according to the T2 synchronisation method requirement

4.4.3.10.2 EF_{PID} (Phone Book Identifier)

The phone book identifier (PID) is used by the terminal to verify if the currently used phone book is the same as used in the previous session.

The initial value will be assigned : TBD, according to T2 discussion

The PID shall be changed by the USIM if one of the following 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

Table 10a: Structure of EF_{PID}

Identifier: '4F21'		Structure: transparent		Optional
SFI: optional				
File size: 4 bytes		Update activity: low		
Access Conditions: READ PIN1 UPDATE PIN1 INVALIDATE PIN2 ? REHABILITATE PIN2 ?				
Bytes	Description		M/O	Length
1 to 4	Phone Book Identifier (PID)		M	4 bytes

- PID: Unique Identifier of Phone Book
  Content: Number to unambiguously identify the phone book for synchronisation purposes
  Coding: tbd, according to the T2 synchronisation method discussion

4.4.3.10.2 EF_{CC} (Change Counter)

The change counter (CC) is used to indicate recent changes to phone book entries.

Every update/deletion of an existing phone book entry or the addition of a new phone book entry causes the USIM to increment the CC.

Table 10b: Structure of EF_{CC}

Identifier: '4F21'	Structure: transparent	Optional
SFI: optional		
File size: 2 bytes	Update activity: high	
Access Conditions: READ PIN1 UPDATE PIN1 INVALIDATE PIN2 ? REHABILITATE PIN2 ?		

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: tbd, according to the T2 synchronisation method discussion

4.4.3.11 EF_{CCP} (Capability Configuration Parameters)

This EF contains parameters of required network and 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.

Identifier: '4F3D'	Structure: linear fixed	Optional
SFI: optional		
Record length: 14 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE 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 GSM 04.08 [15]. 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 terminal.

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 of the UICC the EF_{ADN} of the $DF_{PHONEBOOK}$ is mapped to $DF_{TELECOM}$ to ensure backwards compatibility.

Editor's note: This EF is identical to the EF_{ADN} at the USIM application level. However this EF should be optional while it is necessary to decide if the EF_{ADN} at the UISM application level is mandatory or optional.

4.5.2 EF_{EXT1} (Extension1)

In case of a present GSM application of the UICC the EF_{EXT1} of the $DF_{PHONEBOOK}$ is mapped to $DF_{TELECOM}$ to ensure backwards compatibility.

Editor's note: This EF is identical to the EF_{EXT1} at the USIM application level. However this EF should be optional while it is necessary to decide if the EF_{EXT1} at the UISM application level is mandatory or optional.

4.6 DFs at the TELECOM level

There is only one DF at the TELECOM level.

$DF_{PHONEBOOK}$ '5F3A'

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

Editor's note(6-SEP-99:Kobayashi): Need to check File ID value

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 DF_{DIR}.

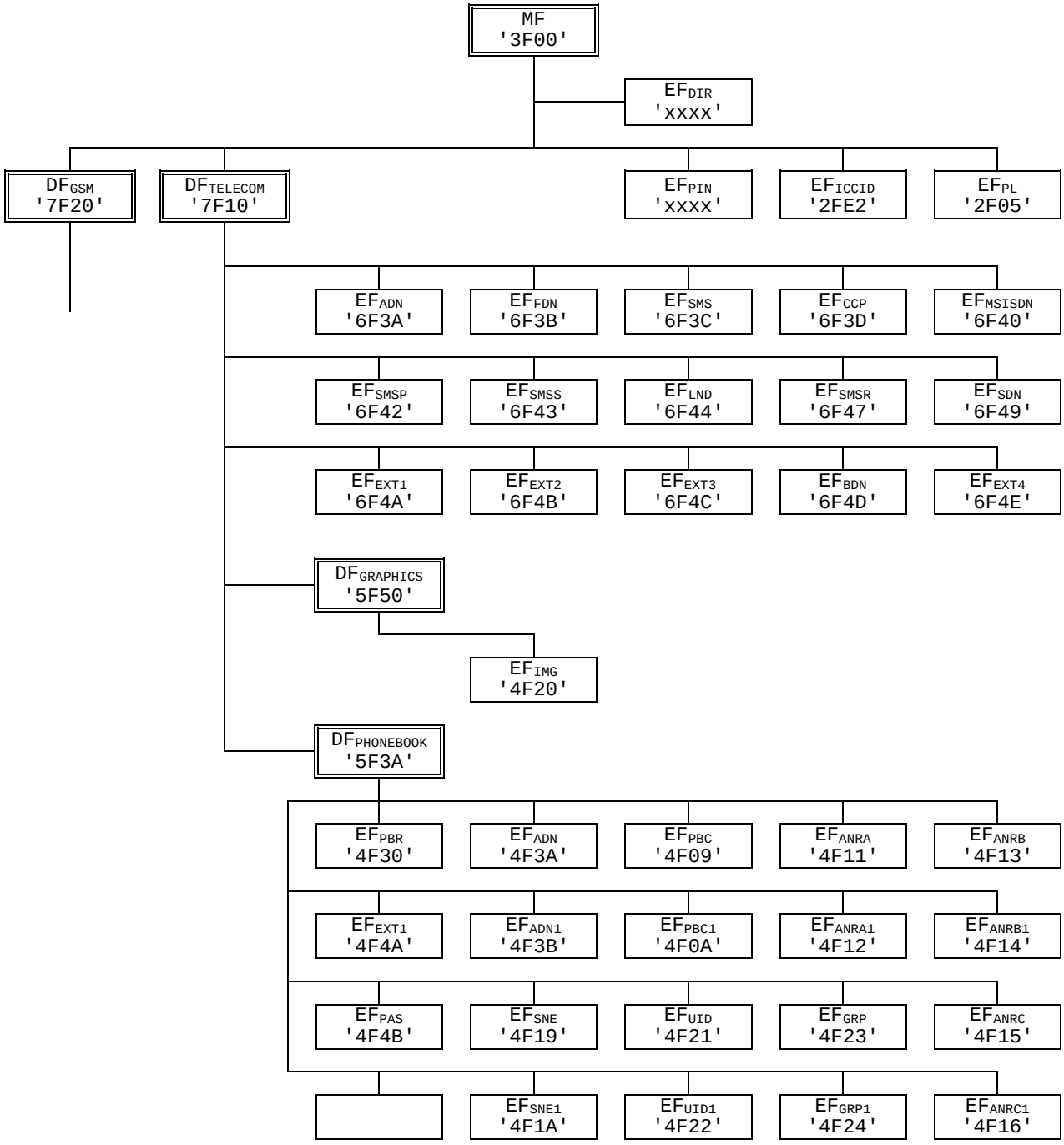


Figure 8: File identifiers and directory structures of UICC

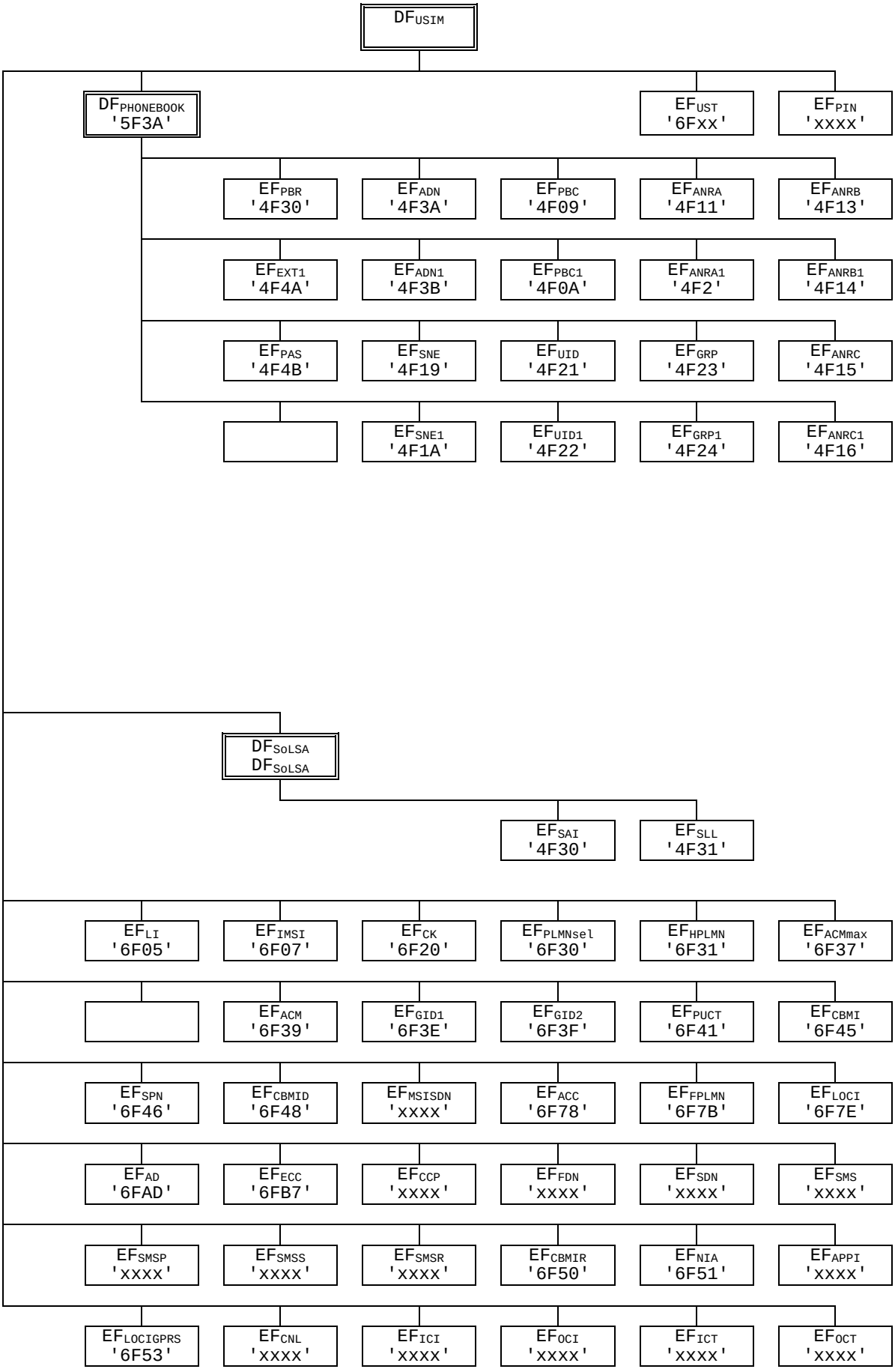


Figure 9: File identifiers and directory structures of USIM

5 Application protocol

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

When involved in 3G network operations the USIM interfaces with a terminal 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 terminal shall ensure that, when operated according to the manufacturer's manual, any unspecified interruption of the sequence of command/response pairs which realize the procedure, leads to the abortion of the procedure itself.
- a UMTS session of the USIM in the 3G application is the interval of time starting at the completion of the USIM initialization procedure and ending either with the start of the UMTS session termination procedure, or at the first instant the link between the SIM and the terminal is interrupted.

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

Some procedures at the USIM/terminal interface require MMI interactions. The descriptions hereafter do not intend to infer any specific implementation of the corresponding MMI. When MMI interaction is required, it is marked "MMI" in the list given below.

Some procedures are not clearly user dependent. They are directly caused by the interaction of the MS and the network. Such procedures are marked "NET" in the list given below.

Some procedures are automatically initiated by the terminal. They are marked "terminal" in the list given below.

The list of procedures at the USIM/terminal interface in 3G network operation is as follows:

USIM management procedures:

-	USIM initialization	terminal
-	UMTS session termination	terminal
-	USIM application closure	terminal
-	Emergency call codes request	terminal
-	Language indication request	terminal
-	Administrative information request	terminal
-	USIM service table request	terminal
-	Application profile indication request	terminal
-	UICC presence detection	terminal

USIM security related procedures:

-	Authentication algorithms computation	NET
-	IMUI request	NET
-	Access control information request	NET
-	HPLMN search period request	NET
-	Location Information	NET
-	Cipher key	NET
-	Forbidden PLMN information	NET
-	LSA information	NET

Subscription related procedures:

-	Dialling Numbers (ADN, FDN, MSISDN, LND, SDN, BDN)	MMI/terminal
-	Short messages (SMS)	MMI
-	Advice of Charge (AoC)	MMI
-	Capability Configuration Parameters (CCP)	MMI
-	PLMN Selector	MMI
-	Cell Broadcast Message Identifier (CBMI)	MMI
-	Group Identifier Level 1 (GID1)	MMI/terminal
-	Group Identifier Level 2 (GID2)	MMI/terminal
-	Service Provider Name (SPN)	terminal
-	Voice Group Call Service (VGCS)	MMI/terminal
-	Voice Broadcast Service (VBS)	MMI/terminal
-	Enhanced Multi Level Pre-emption and Priority (eMLPP)	MMI/terminal
-	Short message status reports (SMSR)	MMI

SIM Application Toolkit related procedures:

-	Data Download via SMS-CB (CBMID)	NET
-	Data Download via SMS-PP	NET
-	Menu selection	MMI
-	Call Control	MMI/terminal/NET
-	Proactive SIM	MMI/terminal/NET
-	Mobile Originated Short Message control by SIM	MMI/terminal/NET
-	Image Request	MMI/terminal

The procedures listed in subclause 5..2 are basically required for execution of the procedures in subclauses 5..3, 5..4 and 5..5. The procedures listed in subclauses 5..3 and 5..4 are mandatory (see GSM 02.17 [6]). The procedures listed in 5..5 are only executable if the associated services, which are optional, are provided in the SIM. However, if the procedures are implemented, it shall be in accordance with subclause 5..5.

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 avaible" (see subclause tbd). In all other cases this procedure shall not start.

5.1 USIM management procedures

Phase 2 MEs shall support all SIMs which comply with the mandatory requirements of Phase 1, even if these SIMs do not comply with all the mandatory requirements of Phase 2. Furthermore, Phase 2 MEs shall take care of potential incompatibilities with Phase 1 SIMs which could arise through use of inappropriate commands or misinterpretation of response data. Particular note should be taken of making a false interpretation of RFU bytes in a Phase 1 SIM having contradictory meaning in Phase 2; e.g. indication of EF invalidation state.

5.1.1 USIM initialization

- Selection of USIM by AID
- Open a logical channel for the USIM application (implicitly possible by selecting the application?)
- Read EF_{ECC}
- Select & Read EF_{LI} if present. terminal to adapt the language if entries present and supported by the terminal. Otherwise terminal keeps using the language selected during UICC initialisation by means of EF_{PL}.
- PIN1 verfication if required

After SIM activation (see subclause 4.3.2), the terminal selects the Dedicated File DF_{GSM} and optionally attempts to select EF_{ECC}. If EF_{ECC} is available, the terminal requests the emergency call codes.

The terminal requests the Extended Language Preference. The terminal only requests the Language Preference (EF_{LP}) if at least one of the following conditions holds:

- EF_{ELP} is not available;
- EF_{ELP} does not contain an entry corresponding to a language specified in ISO 639[30];
- the terminal does not support any of the languages in EF_{ELP}.

If both EFs are not available or none of the languages in the EFs is supported then the terminal selects a default language. It then runs the PIN1 verification procedure.

If the PIN1 verification procedure is performed successfully, the terminal then runs the USIM Phase request (EF_{APPI} evaluation) procedure.

The terminal has to evaluate if the FDN mode is enabled. The procedure is tbd.

In all other cases 3Gsession shall not start.

Afterwards, the terminal runs the following procedures:

- Administrative Information request;
- USIM Service Table request; (Note: Might to be performed earlier, if the FDN enabling is indicated in here)
- IMSI request;
- Access Control request;
- PLMN selector request;
- Location Information request;
- Cipher Key request;
- Forbidden PLMN request;
- Depending on the further services that are supported by both the terminal and the USIM the corresponding EFs have to be read.

After the SIM initialization has been completed successfully, the terminal is ready for a 3G session and indicates this to the USIM be sending a particular STATUS command.
Editor's Note: The particular parameters have to be defined and it has to be decided if they are reflected in 31.101.

5.1.2 UMTS session termination

NOTE 1: This procedure is not to be confused with the deactivation procedure in subclause 4.3.2.

The GSM session is terminated by the terminal as follows:

The terminal runs all the procedures which are necessary to transfer the following subscriber related information to the SIM:

- Location Information update;
- Cipher Key update;
- Advice of Charge increase;
- Forbidden PLMN update.

As soon as the USIM indicates that these procedures are completed, the terminal sends a particular STATUS command indicating the termination of the UMTS session. After issuing this command the USIM may be closed.

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

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

5.1.3 USIM Application Closure

After termination of the UMTS session as defined in 5.2.2 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 terminalperforms the reading procedure with EF_{ECC}.
Update: The terminal 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, PIN1 or PIN2.

5.1.5 Language indication

Request: The terminalperforms the reading procedure with EF_{LI}.
Update: The terminalperforms the updating procedure with EF_{LI}.

5.1.6 Administrative information request;

The terminalperforms the reading procedure with EF_{AD}.

5.1.7 USIM service table request

The terminalperforms the reading procedure with EF_{UST}.

5.1.8 Application profile indication request

The terminalperforms the reading procedure with EF_{APPI}.

5.1.9 UICC Presence Detection

terminalterminal

The terminal checks for the presence of the UICC according to 3G TS 31.101, section 14.5.2.

5.2 USIM security related procedures

5.2.1 Authentication algorithms computation

The terminalselects the USIM application and uses the INTERNAL AUTHENTICATE command(see tbd). The response (content tbd) is sent to the terminalwhen requested by a subsequent GET RESPONSE command.

5.2.2 IMUI request

The terminalperforms the reading procedure with EF_{IMUI}.

5.2.3 Access control request

The terminalperforms the reading procedure with EF_{ACC}.

5.2.4 HPLMN search period request

The terminalperforms the reading procedure with EF_{HPLMN}.

5.2.5 Location information

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

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

5.2.6 Cipher key

Request: The terminal performs the reading procedure with EF_{CK}.
Update: The terminal performs the updating procedure with EF_{CK}.

5.2.8 Forbidden PLMN

Request: The terminal performs the reading procedure with EF_{FPLMN}.
Update: The terminal performs the updating procedure with EF_{FPLMN}.

5.2.9 LSA information

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

5.3 Subscription related procedures

5.3.1 Dialling numbers

Editor's Note: The FDN/BDN procedures have to be defined based upon the implementation of the FDN/BDN features.
The whole section needs to be updated

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 SIM 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 terminal analyses and assembles the information to be stored as follows (the byte identifiers used below correspond to those in the description of the EFs in subclauses 10.5.1, 10.5.4 and 10.5.10):

i) The terminal 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 terminal seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the terminal 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 (see subclauses 10.5.1 and 10.5.10).

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 GSM 04.08 [15] for coding):

The terminal seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the terminal runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted.

The terminal 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 GSM 04.08 [15] for coding):

The terminal seeks for two free records in EF_{EXT1}. If no such two records are found, the terminal runs the Purge procedure. If two Extension1 records are still unavailable, the procedure is aborted.

The terminal 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 terminal performs the updating procedure with EF_{ADN}. If the SIM has no available empty space to store the received ADN/SSC, or if the procedure has been aborted, the terminal advises the user.

NOTE 1: For reasons of memory efficiency the terminal is allowed to analyse all Extension1 records to recognize if the additional or subaddress data to be stored is already existing in EF_{EXT1}. In this case the terminal may use the existing chain or the last part of the existing chain from more than one ADN (LND, MSISDN). The terminal is only allowed to store extension data in unused records. If existing records are used for multiple access, the terminal shall not change any data in those records to prevent corruption of existing chains.

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

Request: The terminal sends the identification of the information to be read. The terminal shall analyse the data of EF_{ADN} (subclause 10.5.1) to ascertain, whether additional data is associated in EF_{EXT1} or

EF_{CCP}. If necessary, then the terminal performs the reading procedure on these EFs to assemble the complete ADN/SSC.

Purge: The terminal 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 terminal. All Extension1 (Extension2) records not noted are then marked by the terminal as "free" by setting the whole record to 'FF'.

NOTE 2: Dependent upon the implementation of the terminal, 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 terminal has to check the state of service n°3, i.e. if FDN is "enabled" or "disabled". In case of enabled FDN, the terminal has to switch to a restrictive terminal mode (see GSM 02.07). To ascertain the state of FDN, the terminal checks in EF_{SST} whether or not ADN is activated. If ADN is not activated, service n°3 is enabled. If ADN is activated, the terminal checks the response data of EF_{ADN}. If EF_{ADN} is invalidated, service n°3 is enabled. In all other cases service n°3 is disabled.

FDN disabling. The FDN disabling procedure requires that PIN2 verification procedure has been performed successfully and that ADN is activated. If not, FDN disabling procedure will not be executed successfully. To disable FDN capability, the terminal rehabilitates EF_{ADN}. The invalidate/rehabilitate flag of EF_{ADN}, which is implicitly set by the REHABILITATE command, is at the same time the indicator for the state of the service n°3. If ADN is not activated, disabling of FDN is not possible and thus service n°3 is always enabled (see FDN capability request).

NOTE 3: If FDN is disabled (by rehabilitating EF_{ADN}) using an administrative terminal then the FDN disabling procedure of this administrative terminal need also to rehabilitate EF_{IMSI} and EF_{LOCI} to ensure normal operation of the SIM in a phase 1 terminal or a phase 2 terminal which does not support FDN.

FDN enabling. The FDN enabling procedure requires that PIN2 verification procedure has been performed successfully. If not, FDN enabling procedure will not be executed successfully. To enable FDN capability, the terminal invalidates EF_{ADN}. The invalidate/rehabilitate flag of EF_{ADN}, which is implicitly cleared by the INVALIDATE command, is at the same time the indicator for the state of the service n°3 (see FDN capability request). If ADN is not activated, service n°3 is always enabled.

Invalidated ADNs may optionally still be readable and updatable depending on the file status (see clause 9.3)

The following three procedures are only applicable to service n°31 (BDN).

BDN capability request. The terminal has to check the state of service n°31, i.e. if BDN is "enabled" or "disabled". BDN service is "enabled" only if service n°31 is allocated and activated, and EF_{BDN} is not invalidated. In all other cases, the BDN service is "disabled".

BDN disabling. The BDN disabling procedure requires that PIN2 verification procedure has been performed successfully. If not, BDN disabling procedure will not be executed successfully. To disable BDN capability, the terminal invalidates EF_{BDN}. The invalidate/rehabilitate flag of EF_{BDN}, which is implicitly cleared by the INVALIDATE command, is at the same time the indicator for the state of the service n°31 (see BDN capability request).

BDN enabling. The BDN enabling procedure requires that PIN2 verification procedure has been performed successfully. If not, BDN enabling procedure will not be executed successfully. To enable BDN capability, the terminal rehabilitates EF_{BDN}. The invalidate/rehabilitate flag of EF_{BDN}, which is implicitly set by the REHABILITATE command, is at the same time the indicator for the state of the service n°31 (see BDN capability request).

Invalidated BDNs (when BDN capability is disabled) may optionally still be readable and updatable depending on the file status (see clause 9.3).

5.3.2 Short messages

Requirement: Service n°tbd "available".

Request: The SIM seeks for the identified short message. If this message is found, the terminal performs the reading procedure with EF_{SMS}.

If service n°tbd is "allocated and activated" and the status of the SMS is '1D' (status report requested, received and stored in EF_{SMSR}), the terminal performs the reading procedure with the corresponding record in EF_{SMSR}. If the terminal does not find a corresponding record in EF_{SMSR}, then the terminal 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 SIM memory, the SIM indicates that to the terminal.

Update: The terminal 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 SIM to store the received short message, a specific MMI will have to take place in order not to loose the message.

Erasure: The terminal will select in the SIM 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 SIM is made available for a new incoming message. The memory of the SIM may still contain the old message until a new message is stored in this area.

If service n°35 is "allocated and activated" and the status of the SMS is '1D' (status report requested, received and stored in EF_{SMSR}), the terminal performs the erasure procedure for EF_{SMSR} with the corresponding record in EF_{SMSR}.

5.3.3 Advice of Charge (AoC)

Requirement: Service n°tbd "available".

Accumulated Call Meter.

Request: The terminal performs the reading procedure with EF_{ACM}. The USIM returns the last updated value of the ACM.

Initialization: The terminal performs the updating procedure with EF_{ACM} using the new initial value.

Increasing: The terminal performs the increasing procedure with EF_{ACM} sending the value which has to be added.

Accumulated Call Meter Maximum Value.

Request: The terminal performs the reading procedure with EF_{ACMmax}.

Initialization: The terminal performs the updating procedure with EF_{ACMmax} using the new initial maximum value.

Price per Unit and Currency Table (PUCT).

Request: The terminal performs the reading procedure with EF_{PUCT}.

Update: The terminal performs the updating procedure with EF_{PUCT}.

5.3.4 Capability configuration parameters

Requirement: Service n°tbd "available".

Request: The terminal performs the reading procedure with EF_{CCP}.

Update: The terminal performs the updating procedure with EF_{CCP}.

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

5.3.5 PLMN selector

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

5.3.6 Cell broadcast message identifier

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

5.3.7 Group identifier level 1

Requirement: Service n°tbd "available".
Request: The terminal performs the reading procedure with EF_{GID1}.

5.3.8 Group identifier level 2

Requirement: Service n°tbd "available".
Request: The terminal performs the reading procedure with EF_{GID2}.

5.3.9 Service Provider Name

Requirement: Service n°tbd "available".
Request: The terminal performs the reading procedure with EF_{SPN}.

5.3.10 Cell Broadcast Message range identifier

Requirement: Service n°tbd "available".
Request: The terminal performs the reading procedure with EF_{CBMIR}.
Update: The terminal performs the updating procedure with EF_{CBMIR}.

5.3.12 Short message status report

Requirement: Service n°tbd "available".

Request: If the status of a stored short message indicates that there is a corresponding status report, the terminal performs the seek function with EF_{SMSR} to identify the record containing the appropriate status report. The terminal performs the reading procedure with EF_{SMSR}.

Update: If a status report is received, the terminal 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 terminal seeks for a free entry in EF_{SMSR} for storage. If no free entry is found the terminal runs the Purge procedure with EF_{SMSR}. If there is still no free entry, the status report is not stored.

If the terminal 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 (see tbd) by performing the update procedure with EF_{SMS}.

Erasure: The terminal runs the update procedure with EF_{SMSR} by at least storing '00' in the first byte of the record. The terminal may optionally update the following bytes with 'FF'.

Purge: The terminal shall read the SMS record identifier (byte 1) of each record of EF_{SMSR}. With each record the terminal 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 terminal shall perform the erasure procedure with the appropriate record in EF_{SMSR}.

6 Security features

The security aspects of GSM are described in the normative references 3G TS 33.102 [36] and 3G TS 33.103 [37]. 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 key generation which are invoked by the network. For the specification of the corresponding procedures across the USIM/terminal interface see clause 5.

The mechanism achieves mutual authentication by the user and the network showing knowledge of a secret key K which is shared between and available only to the USIM and the AuC in the user's HE. In addition the USIM and the HE keep track of counters SQN_{MS} and SQN_{HE} respectively to support network authentication.

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 terminal 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 then 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 [36]. These are:

- f1: a message authentication function for network authentication
- f1*: a message authentication function for support to re-synchronisation;
- f2: a message authentication function for user authentication;

- f3: a key generating function to derive the cipher key;
- f4: a key generating function to derive the integrity key;
- f5: a key generating function to derive the anonymity key (optional).
- f6: the user identity encryption function to encrypt the IMUI (optional)

Editor's Note: TBD, if 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 to C4. These functions derive the required GSM parameters ($RAND_G$, SRES, cipher key kc) from available 3G parameters.

Editor's Note: The usage of the single functions and the according input / output parameters have to be specified.

6.4 File access conditions

Editor's Note: Modifications may be necessary according to the PIN concept that is still under definition in 31.101.
Do we assign access conditions to MF and/or the ADF and DFs?
Can PIN be disabled?
How is PIN2 managed?

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 SEEK 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 7: Access condition level coding

Level	Access Condition
0	ALWays
1	PIN
2	PIN2
3	Reserved for GSM Future Use
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 CHV2 value has already been presented to the SIM during the current session;
- UNBLOCK CHV2 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.

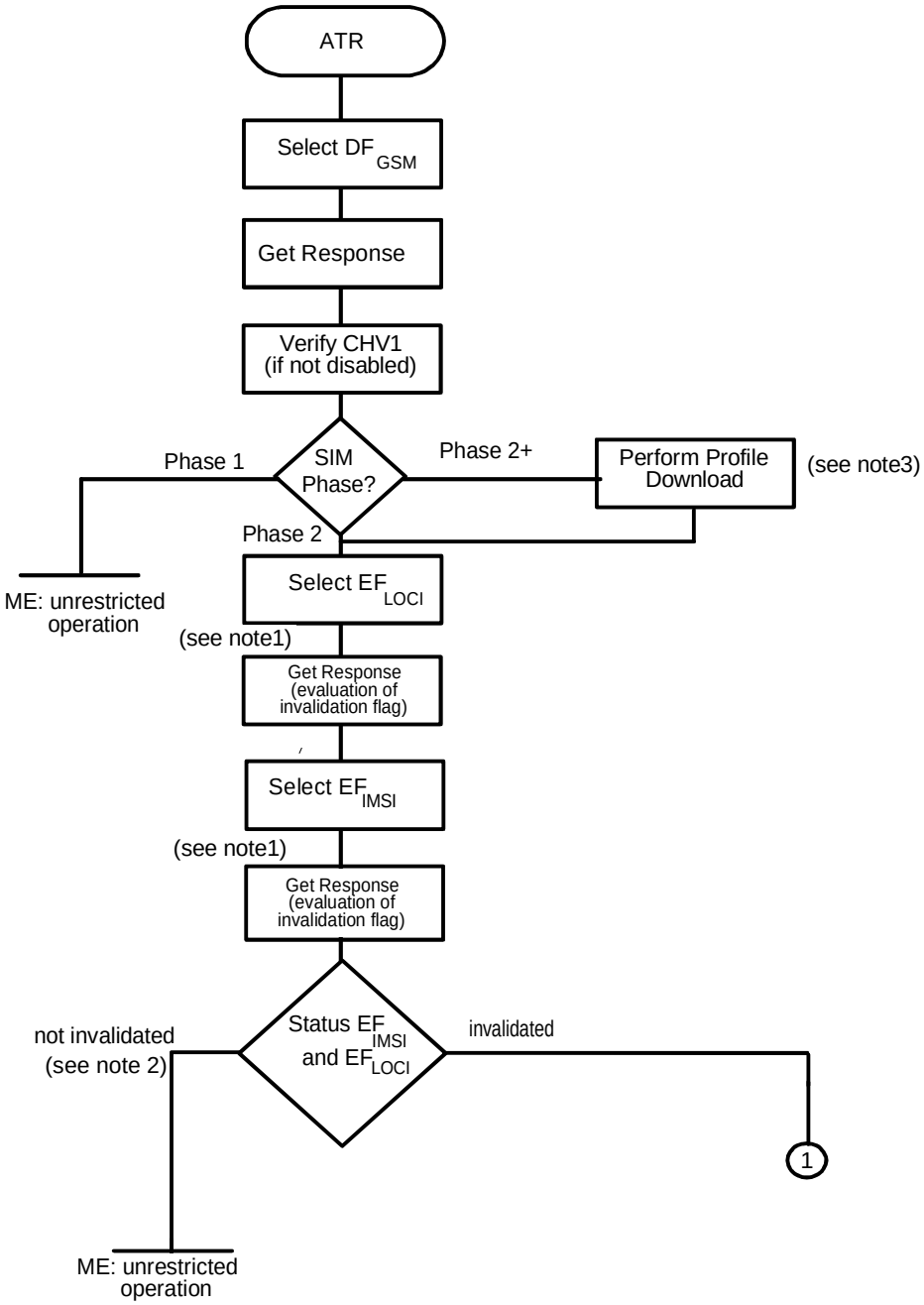
NEVER: The action cannot be performed over the USIM(UICC)/terminal interface. The USIM may perform the action internally.

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 terminal shall determine whether PIN2 is available by using the response to the STATUS command. If PIN2 is "not initialized" then PIN2 commands, e.g. VERIFY PIN2, shall not be executable.

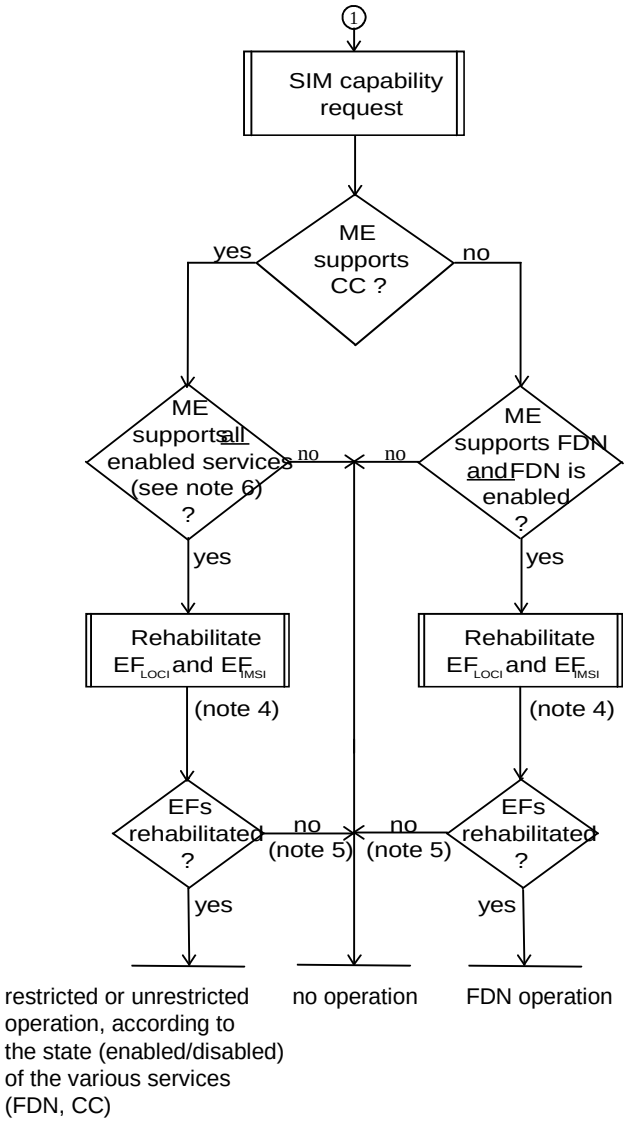
Annex A (informative): FDN Procedure

Editor's note: This annex is identical to the Annex C in GSM 11.11 V7.2.0 without the BDN procedure (the BDN procedure has not yet been excluded because of a technical reason on Word processor).
It will have to be modified according to the new FDN/BDN implementation that is still to be defined.



NOTE 1: In case of enabled FDN, the EF has been invalidated by the SIM at no later than this stage.

Fig A.1: Example of an Initialization Procedure of a FDN SIM (see tbd)



NOTE 4: In case of "BDN enabled", the SIM only allows rehabilitation of the EF_{IMSI} and EF_{LOCI}, if the terminal has indicated its CC-capability to the SIM (by PROFILE_DOWNLOAD).

NOTE 5: Possibility for future "restricting" services to use the internal SIM mechanism of invalidation of EF_{IMSI} and EF_{LOCI}.

NOTE 6: If the terminal does not support all enabled services (e.g. FDN, BDN), it does not operate. In case of enabled BDN, the support of the "Call Control Feature" by the terminal is sufficient for operation. For future use, there may be additional "restricting" services, which are not known to the terminal. In that case the terminal will perform the subsequent rehabilitation procedure but will fail to rehabilitate EF_{IMSI} and EF_{LOCI} (see note 4).

Figure A.2: Example of an Initialization Procedure of a FDN SIM (continued)

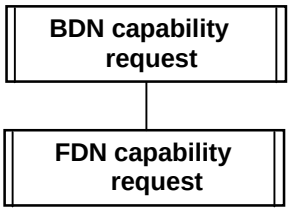
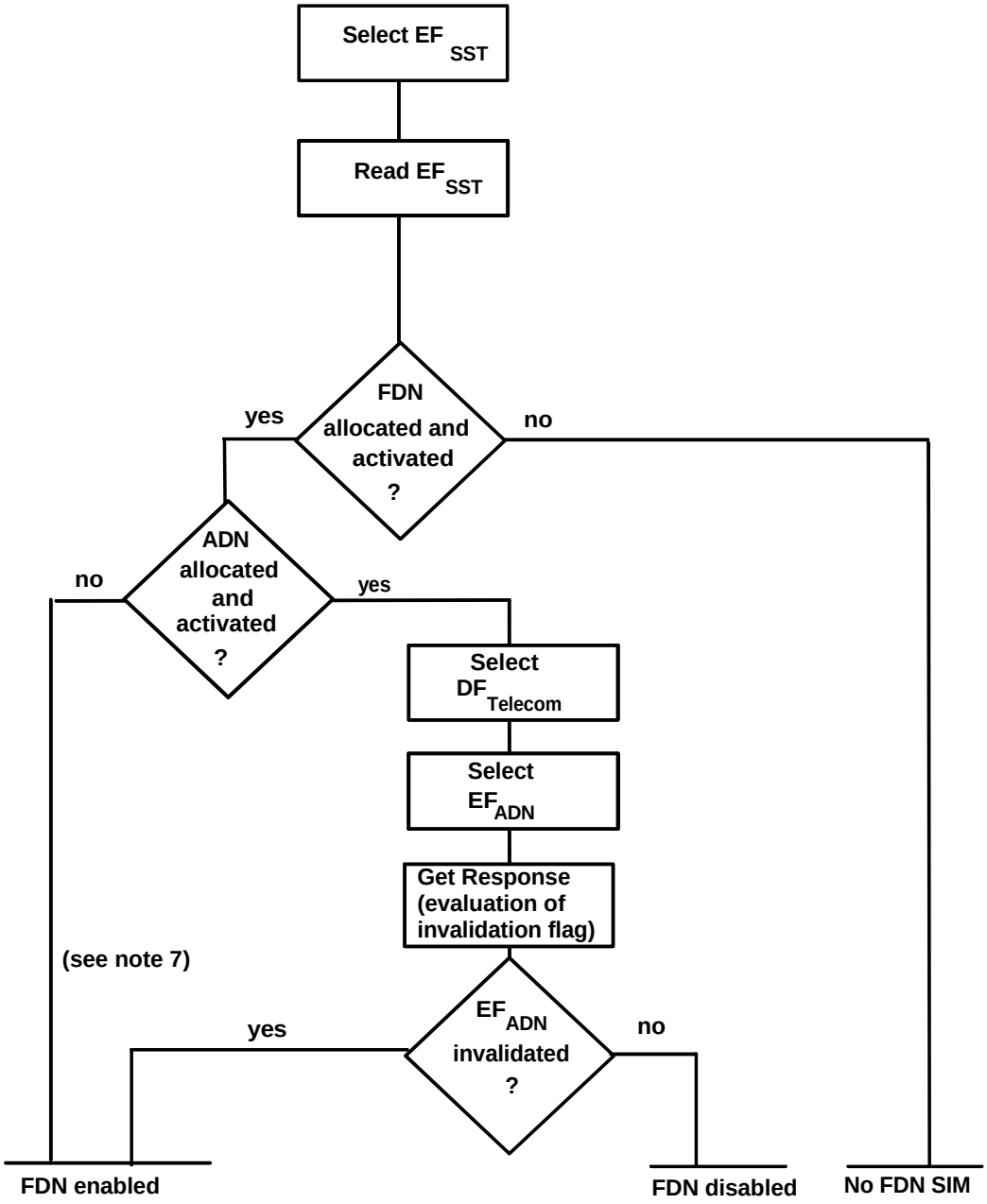


Figure A.3: SIM capability request



NOTE 7: In this case FDN is enabled without the possibility of disabling.

Figure A.4: FDN capability request (see 11.5.1)

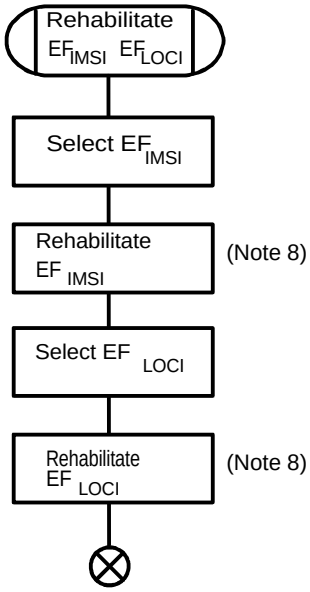


Figure A.5: Procedure to rehabilitate GSM files

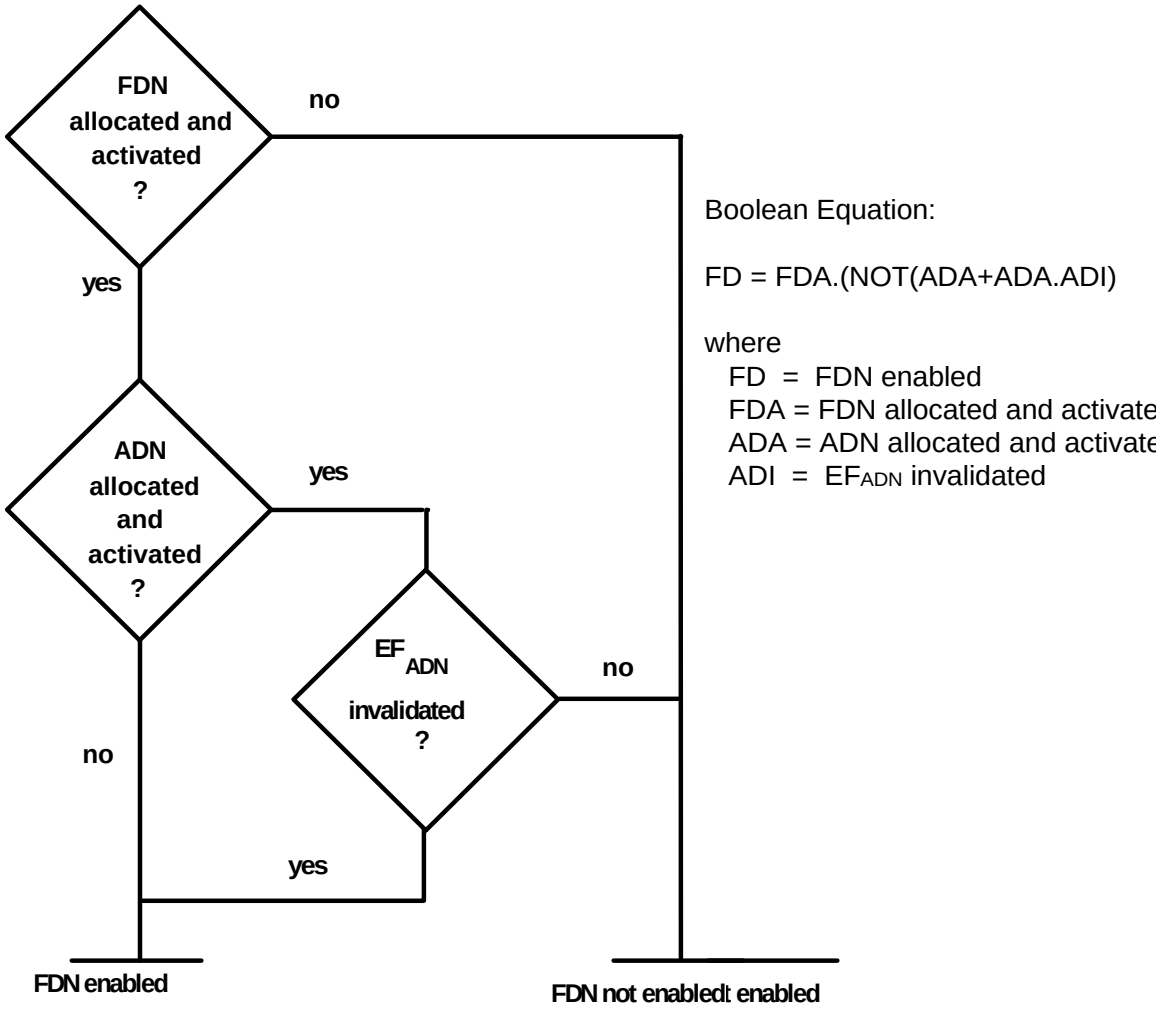


Figure A.6: Coding for state of FDN

Annex B (informative): Suggested contents of the EFs at pre-personalization

Editor's note: This annex is identical to the Annex C in GSM 11.11 V7.2.0. It is necessary to modify this annex according to 3G requirements and EFs which will be defined in the present document.

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 (see 10.1.1)
'2F 05'	Extended Language preference	'FF…FF'
'6F 05'	Language preference	'FF'
'6F 07'	IMSI	operator dependant (see 10.3.2)
'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'	SIM service table	operator dependant (see 10.3.7)
'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 (see 10.1.12)
'6F 7B'	Forbidden PLMNs	'FF...FF'
'6F 7E	Location information	'FFFFFFFF xxFxxx 0000 FF 01' (see note 2)
'6F AD'	Administrative data	operator dependant (see 10.3.15)
'6F AE'	Phase identification	see 10.3.16
'6F 3A'	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 44'	Last number dialled	'FF...FF'
'6F 47'	Short message status reports	'00FF…FF'
'6F 4A'	Extension 1	'FF...FF'
'6F 4B'	Extension 2	'FF...FF'
'6F 4C'	Extension 3	'FF...FF'
'6F 4D'	Barred dialling numbers	'FF...FF'
'6F 4E'	Extension 4	'FF...FF'
'6F 51'	Network's indication of alerting	'FF...FF'
'6F 52'	GPRS Ciphering key KcGPRS	'FF...FF07'
'6F 53'	GPRS Location Information	'FFFFFFFF FFFFFF xxFxxx 0000 FF 01'
'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 GSM 04.08 [15].

Annex C (informative): Examples of coding of LSA Descriptor files for SoLSA

Editor's note: This annex is identical to the Annex F in GSM 11.11 V7.2.0. It may be necessary to modify this annex according to 3G requirements.

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 D (normative): Image Coding Schemes

Editor's note: This annex is identical to the Annex G in GSM 11.11 V7.2.0.

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.

D.1 Basic Image Coding Scheme

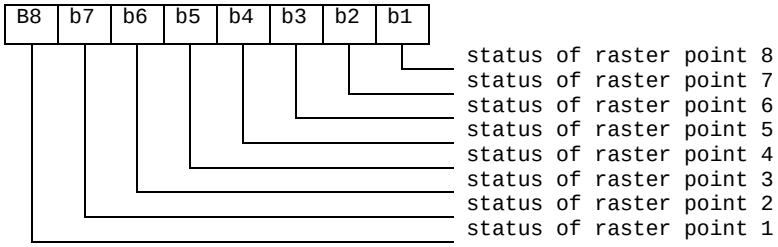
This coding scheme applies to rectangular raster images made up of raster points that are either set or not set. This coding scheme does not support any notion of colour. Image data are coded as follows:

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

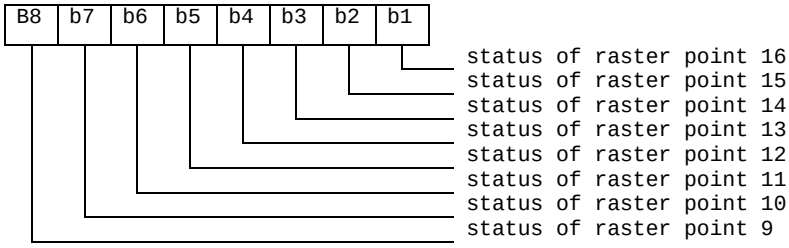
Coding of image body:

The status of each raster image point is coded in one bit, to indicate whether the point is set (status = 1) or not set (status = 0).

Byte 1:



Byte 2:



etc.

Unused bits shall be set to 1

D.2 Colour Image Coding Scheme

This coding scheme applies to coloured rectangular raster images. Raster image point colours are defined as references into a colour look-up table (CLUT), which contains a subset of the red-green-blue colour space. The CLUT in turn is located in the same transparent file as the image instance data themselves, at an offset defined within the image instance data.

Image data are coded as follows:

Byte(s)	Description	Length
1	Image width = X	1
2	Image height = Y	1
3	Bits per raster image point = B	1
4	Number of CLUT entries = C	1
5 to 6	Location of CLUT (Colour Look-up Table)	2
7 to K+6	Image body	K

- Bits per raster image point:

Contents:

The number B of bits used to encode references into the CLUT, thus defining a raster image point's colour.

B shall have a value between 1 and 8.

Coding:

Binary.

- Number of entries in CLUT:

Contents:

The number C of entries in the CLUT which may be referenced from inside the image body. CLUT entries are numbered from 0 to C-1.

C shall have a value between 1 and 2**B.

Coding:

Binary. The value 0 shall be interpreted as 256.

- Location of CLUT:

Contents:

This item specifies where the CLUT for this image instance may be found. The CLUT is always located in the same transparent file as the image instance data themselves, at an offset determined by these two bytes.

Coding:

Byte 1: high byte of offset into Image Instance File.

Byte 2: low byte of offset into Image Instance File.

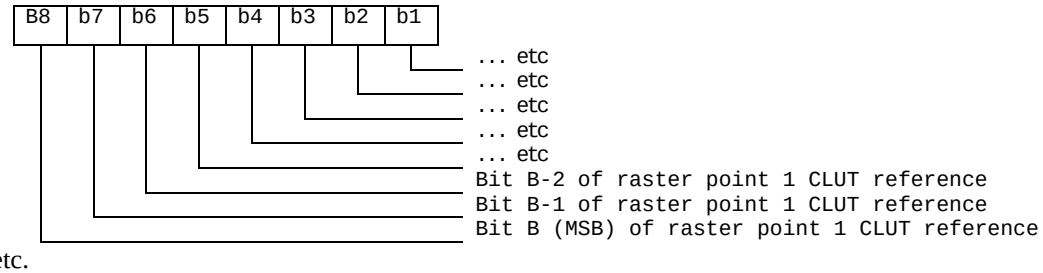
- Image body:

Coding:

Each raster image point uses B bits to reference one of the C CLUT entries for this image instance. The CLUT entry being thus referenced yields the raster image point's colour.

The image body is arrayed as for the Basic Colour Image Coding Scheme, that is, starting with the highest bit of the first raster image point's colour information.

Byte 1:



etc.

Unused bits shall be set to 1.

The CLUT (Colour Look-up Table) for an image instance with C colours is defined as follows:

Contents:

C CLUT entries defining one colour each.

Coding:

The C CLUT entries are arranged sequentially:

Byte(s) of CLUT	CLUT Entry
1-3	entry 0
...	...
3*(C-1) +1 to 3*C	Entry C-1

Each CLUT entry in turn comprises 3 bytes defining one colour in the red-green-blue colour space:

Byte(s) of CLUT enty	Intensity of Colour
1	Red
2	Green
3	Blue

A value of 'FF' means maximum intensity, so the definition 'FF' '00' 00' stands for fully saturated red.

NOTES:

- Two or more image instances located in the same file can share a single CLUT.
- Most MEs capable of displaying colour images are likely to support at least a basic palette of red, green, blue and white.

Annex E (normative): Coding of USIM Specific Data

E.1 SELECT Response Information

Table F.1 and F2 of this annexdescribe how the response information of the SELECT command is coded in case of MF, DF, ADF and EF selection, respectively.

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

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

Table E.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	PIN1 status (see detail 2)	1
18	UNBLOCK PIN1 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

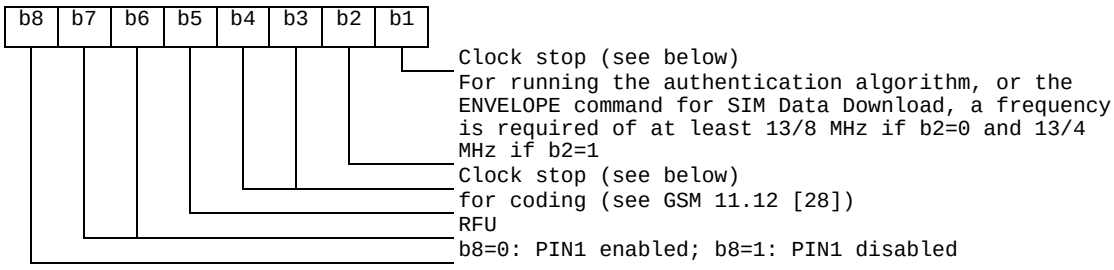
Bytes 1 - 20 are mandatory and shall be returned by a GSM application. Bytes 21 and following are optional and may not be returned by a GSM application.

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 terminals from the specific application directories. terminal 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



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

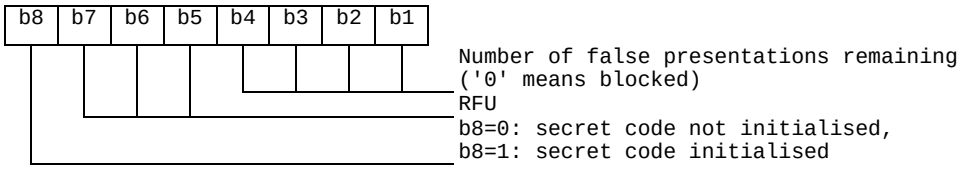


Table E.3: SELECT Response Information in case of an EF

Byte(s)	Description	Length
1 – 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 – 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 1-13 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.

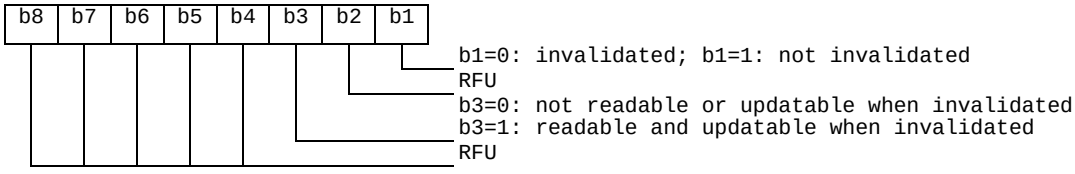
Detail 4: Byte 13

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.

E.2 Coding of telecom specific EF response data

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

File status:



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 invalidated, 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 disabled.

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 [20] 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 terminal shall pad the presented PIN with 'FF' before sending it to the SIM.

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

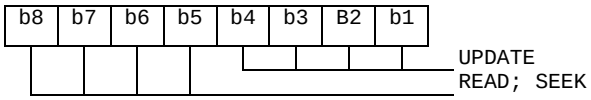
The access conditions for the commands are coded on bytes 9, 10 and 11 of the response data of the SELECT command. Each condition is coded on 4 bits as shown in table G.13.

Table F.12: Access conditions

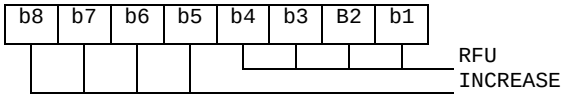
ALW	'0' *
PIN1	'1' *
Second PIN	'2' *
RFU	'3'
ADM	'4'
.....	..
ADM	'E'
NEV	'F' *

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.

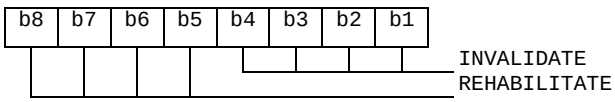
Byte 9:



Byte 10:



Byte 11:



E.3 Application Related Electrical Parameters

The power consumption of an 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 indicated in **Error! Reference source not found.** until an application is selected. An application is consideredto be selected when the access condition is successfully verified. If no access condition is required for the application, the application is consideredto 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 terminal 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 [5] 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 [4].

If no power consumption indication is available in the card, the terminal shall assume the application power consumption as specified in **Error! Reference source not found.** .

Table E.3: 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	

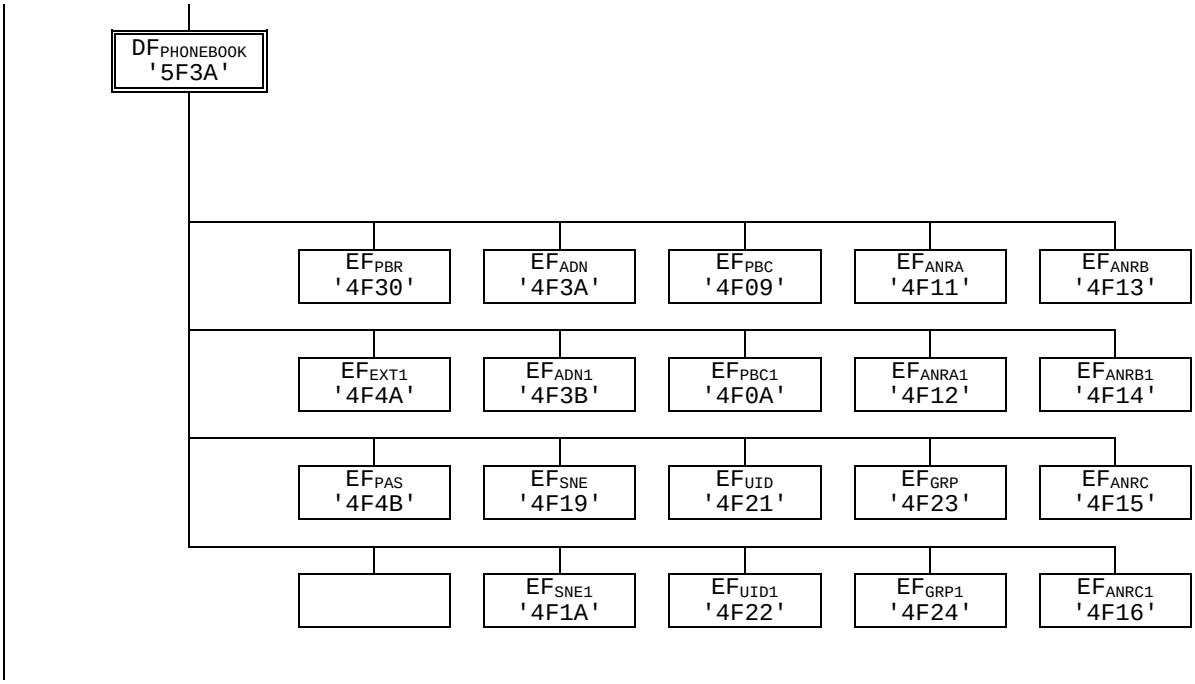
Annex F (Informative): Phonebook Example

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_{EXT1} and EF_{PAS}. These files are addressed from inside a file. EF_{EXT1} is addressed via $EF_{ADN,}$ EF_{ADN1} and EF_{PAS} is addressed via $EF_{PBC,}$ EF_{PBC1}. The phonebook supports two levels of grouping and hidden entries in $EF_{PBC.}$

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 $DF_{PHONEBOOK}$ for Case 1 is shown in table 1y.

Table 1y: Structure of EFs inside $DF_{PHONEBOOK}$



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

Table 1x: Contents of EF_{PBR}

Record 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'
Record 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'

Table 1d: 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
Rec3													
Rec 254													

Table 1e:Structure of phone book entries 255-508 (Rec1-254)

ADN '4F3B'			PBC '4F0A'	GRP '4F24'	ANR '4F12'	ANR '4F14'	ANR '4F16'	SNE'4F20'	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

Rec3													
Rec 254													

History

Document history		
V0.1.0	April 1999	1st draft version to be submitted into TSG T3 #4 meeting, 19-21 April 1999 in Tokyo.
V0.2.0	May 1999	2nd draft version to be submitted into TSG T3 adhoc meeting, 27-28 May 1999 in Copenhagen.
V0.3.0	May 1999	3rd draft version to be submitted into TSG T3 adhoc meeting, 27-28 May 1999 in Copenhagen.
V0.4.0	May 1999	4th draft version to be submitted into TSG T3 #5 meeting 31May – June 2 1999 in Aaland.
V0.5.0	June 1999	5th draft version to be submitted into TSG T3 #6 meeting June 14 – 16 1999 in Miami.
V0.6.0	July 1999	6th draft version to be submitted into TSG T3 #7 meeting July 5 - 7 1999 in Lund.
V0.7.0	September 1999	7th draft version to be submitted into TSG T3 ad hoc #2 September 14-16 1999 in Turku
V0.8.0	September 1999	8th draft version to be submitted into TSG T3 #9 October 4-6 1999 in Kyongju
V0.9.0	October 1999	9th draft version to be submitted into TSG T3 #9 October 4-6 1999 in Kyongju containing the results of this meeting for preparation of V1.0.0
V1.0.0	October 1999	Version 1.0.0 submitted to TSG-T #5 (7 - 8 October 1999) for information