3GPP TSG-T (Terminals) Meeting #9
Hawaii, USA, 20 - 22 September, 2000

Tdoc TP-000152

Source: T3

Title: Change Requests to TS 31.102 "Characteristics of the USIM application"

Agenda item: 6.3.3

Document for: Approval

This document contains several change requests to TS 31.102 v3.2.0 agreed by T3.

T3 Doc	Spec	CR	Rv	Rel	Subject
T3-000444	31.102	044	1	R99	Correction to call information access conditions and correction of DF_GSM file IDs
T3-000404	31.102	045		R99	Clarification of the type 3 links of the phonebook
T3-000405	31.102	046		R99	Alignment of EF(CCP2) with EF(ECCP)
T3-000410	31.102	047	1	R99	Correction of record length, editorial errors, missing FID
T3-000408	31.102	048		R99	APN Control List coding
T3-000409	31.102	049		R99	Alignment with TS 33.102 regarding authentication Sequence Numbers
T3-000452	31.102	050		R99	Preferred language selection
T3-000475	31.102	051		R99	Application Selection by partial AID
T3-000481	31.102	052		R99	Addition of warning regarding network selection with access technology
T3-000482	31.102	053		R99	Phone book clarifications

3GPP TSG-T3 (USIM) Meeting #15
San Diego, USA, 16-18 August 2000

Document* *T3-000444
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

TS 31.102	**CR**	**044r1**	Current Version:	V3.2.0
GSM (AA.BB) or 3G (AA.BBB) specification number ↑		↑ *CR number as allocated by MCC support team*		

For submission to:	TSG-T #09	for approval	☒	strategic	□	*(for SMG use only)*
list expected approval meeting # here ↑		for information	□	non-strategic	□	

Form: CR cover sheet, version 2 for 3GPP and SMG   The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM ☒ ME ☒ UTRAN / Radio □ Core Network □
(at least one should be marked with an X)

Source: T3 **Date:** 17/08/2000

Subject: Correction to call information access conditions and correction of DF_GSM file IDs

Work item: TEI

Category:	F	Correction	☒	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	□		Release 99	☒
					Release 00	□

Reason for change:
- EF_ARR is linear fixed structure. It has record length for size parameter.
- EF file IDs for 2nd level DFs is 4F XX.

Clauses affected: 4.2.55, 4.4.3.4, 4.4.3.5, 4.7

Other specs affected:	Other 3G core specifications	□	→ List of CRs:	
	Other GSM core specifications	□	→ List of CRs:	
	MS test specifications	□	→ List of CRs:	
	BSS test specifications	□	→ List of CRs:	
	O&M specifications	□	→ List of CRs:	

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

4.2.55 $\mathrm{EF}_{\mathrm{ARR}}$ (Access Rule Reference)

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

Structure of $\mathrm{EF}_{\mathrm{ARR}}$ at ADF-level

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

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

4.4.3.4 EF$_{CPBCCH}$ (CPBCCH Information)

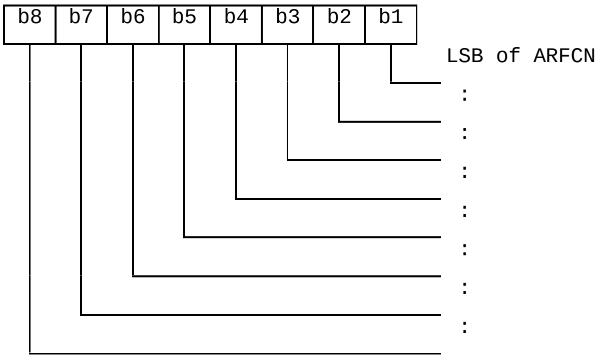
This EF contains information concerning the CPBCCH according to GSM 04.18 [28].

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

Identifier: '~~6F~~4F75'	Structure: transparent		Optional
File size: 2n bytes		Update activity: high	
Access Conditions: READ PIN UPDATE PIN INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 to 2	Element 1 of CPBCCH carrier list	M	2 bytes
2n-1 to 2n	Element n of CPBCCH carrier list	M	2 bytes

- Element in CPBCCH carrier list
  Coding:

  Byte 1: first byte of CPBCCH carrier list element



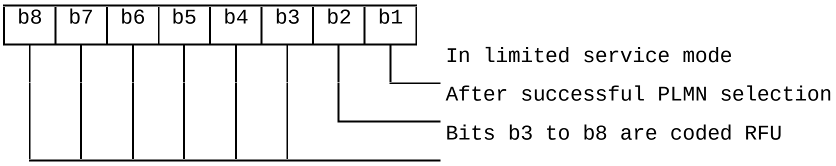
4.4.3.5 EF$_{\text{InvScan}}$ (Investigation Scan)

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

<table>
<tr><td colspan="2">Identifier: '~~6F~~4F76'</td><td colspan="2">Structure: transparent</td><td>Optional</td></tr>
<tr><td colspan="3">File size: 1 byte</td><td colspan="2">Update activity: low</td></tr>
<tr><td colspan="5">Access Conditions:
READ PIN
UPDATE ADM
INVALIDATE ADM
REHABILITATE ADM</td></tr>
<tr><td>Bytes</td><td colspan="2">Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1</td><td colspan="2">Investigation scan flags</td><td>M</td><td>1 byte</td></tr>
</table>

- Investigation scan flags

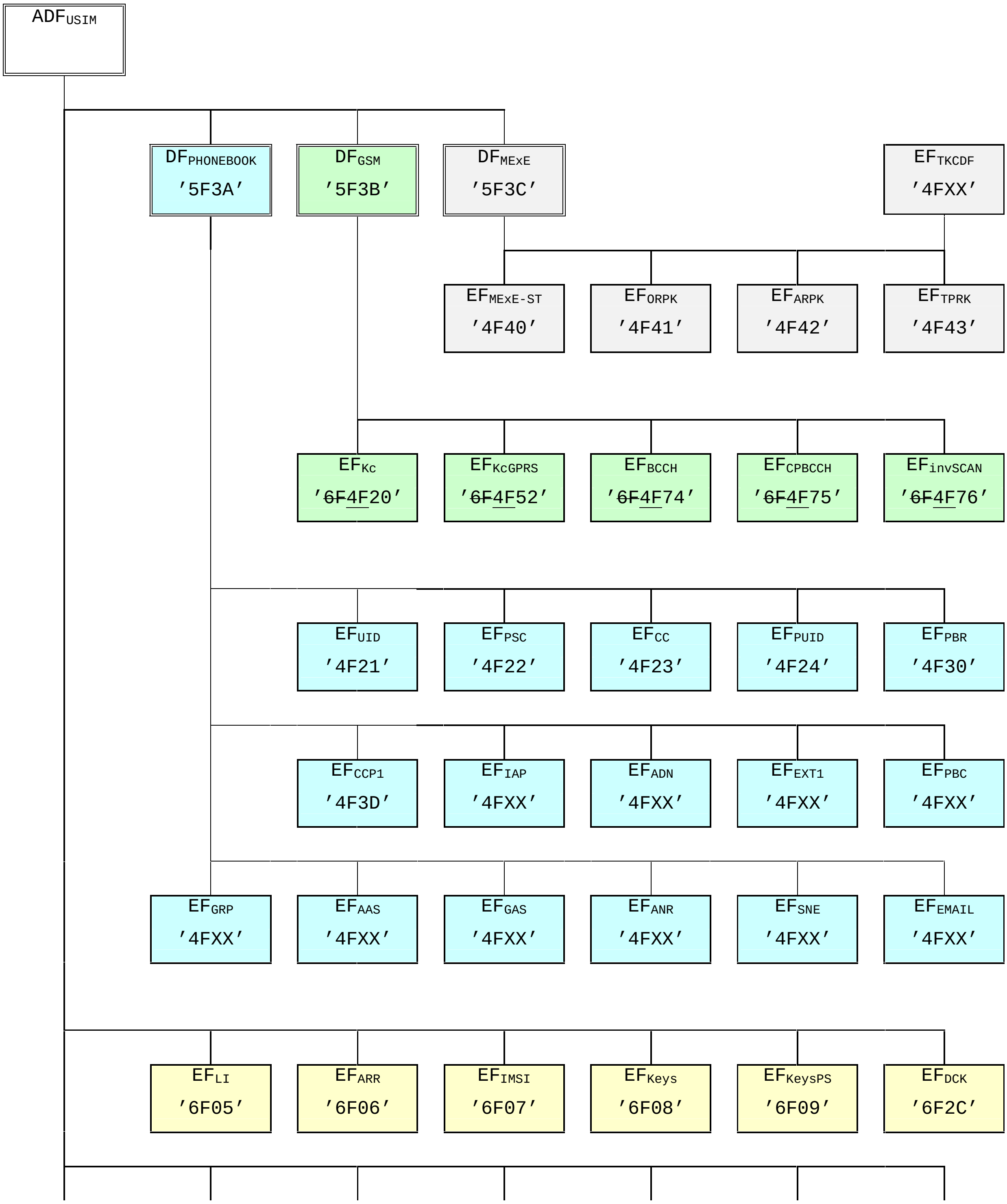
Coding:



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

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

4.7 Files of USIM



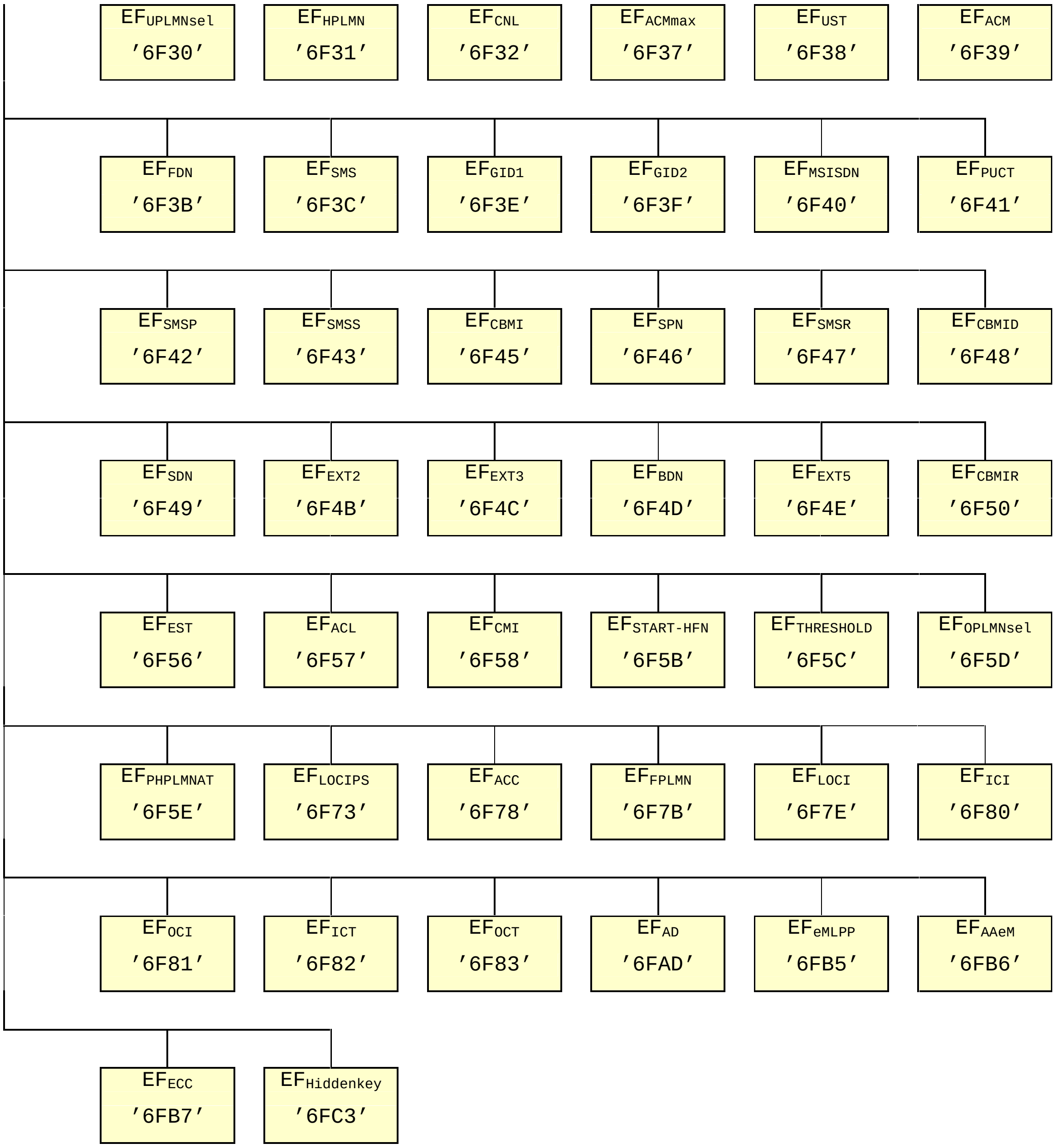


Figure 4.2: File identifiers and directory structures of USIM

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

3GPP TSG-T3 (USIM) Meeting #15
San Diego, USA, 16-18 August 2000

Document T3-000404
revised from T3-000374

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

TS 31.102 CR 045 Current Version: V3.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: TSG-T #9 for approval ☒ strategic ☐ *(for SMG*
list expected approval meeting # here ↑ for information ☐ non-strategic ☐ *use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM ☒ ME ☒ UTRAN / Radio ☐ Core Network ☐
(at least one should be marked with an X)

Source: T3 **Date:** 17/08/2000

Subject: clarification of the type 3 links of the phonebook

Work item: T.E.I.

Category:	F	Correction	☒	**Release:**	Phase 2	☐
	A	Corresponds to a correction in an earlier release	☐		Release 96	☐
(only one category	B	Addition of feature	☐		Release 97	☐
shall be marked	C	Functional modification of feature	☐		Release 98	☐
with an X)	D	Editorial modification	☐		Release 99	☒
					Release 00	☐

Reason for change: - one sentence is misleading in subclause 4.4.2.1
– one table is misleading in Annex G

Clauses affected: 4.4.2.1, Annex G

Other specs affected:	Other 3G core specifications	☐	→ List of CRs:
	Other GSM core specifications	☐	→ List of CRs:
	MS test specifications	☐	→ List of CRs:
	BSS test specifications	☐	→ List of CRs:
	O&M specifications	☐	→ List of CRs:

Other comments:

4.4.2.1 EF_{PBR} (Phone Book Reference file)

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

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

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

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

- Type 1 files: Files that contain as many records as the reference/master file (EF_{ADN}, EF_{ADN1}) and are linked on record number bases (Rec1 -> Rec1). The master file record number is the reference.
- Type 2 files: Files that contain less entries than the master file and are linked via pointers in the index administration file (EF_{IAP}).
- Type 3 files are files that are linked by a TLV object in a record~~ (Grouping information in EF_{GAS})~~.

Table 4.1: Phone Book Reference file Constructed Tags

Tag Value	Constructed TAG Description
'D8'	Indicating files where the amount of records equal to master EF, type 1
'D9'	Indicating files that are linked using the index administration file, type 2. Order of pointer appearance in index administration EF is the same as the order of file IDs following this tag
'DA'	Indicating files that are addressed inside a TLV object, type 3. (The file pointed to is defined by the TLV object.)

The first file ID indicated using constructed Tag 'D8' is called the master EF. Access conditions for all other files in the index structure is set to the same as for the master EF unless otherwise specified.

File IDs indicated using constructed Tag 'D8' is a type 1 file and contains the same number of records as the first file that is indicated in the data part of this TLV object. All files following this Tag are mapped one to one using the record numbers/IDs of the first file indicated in this TLV object.

File IDs indicated using constructed Tag 'D9' are mapped to the master EF (the file ID indicated as the first data object in the TLV object using Tag 'D8') using the pointers in the index administration file. The order of the pointers in the index administration file is the same as the order of the file IDs presented after Tag 'D9'. If this Tag is not present in the reference file record the index administration file is not present in the structure. In case the index administration file is not present in the structure it is not indicated in the data following tag 'D8'.

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

Annex G (informative):
Phonebook Example

This example phonebook has more than 254 entries. Additional number (3 additional numbers) information, second name and e-mail information can be added to each ADN entry. In addition each entry has a 2 byte Unique ID (UID) attached to it. The phonebook also contains three files that are shared EF_{EXT1}, EF_{AAS} and EF_{GAS}. These files are addressed from inside a file. EF_{EXT1} is addressed via $EF_{ADN,}$ EF_{ADN1}, EF_{AAS} is addressed via $EF_{ANR1,}$ EF_{ANR1} and EF_{GAS} is addressed via $EF_{GRP,}$ EF_{GRP1}. The phonebook supports two levels of grouping and hidden entries in $EF_{PBC.}$

Two records are needed in the phonebook reference file PBR ’4F30’ for supporting more than 254 entries. The content of the phonebook reference file PBR ’4F30’ records is as shown in table G.2. The structure of the $DF_{PHONEBOOK}$ is shown in table G.1.

The content of phonebook entries in the range from 1-508 is described in the tables G.3 and G.4.

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

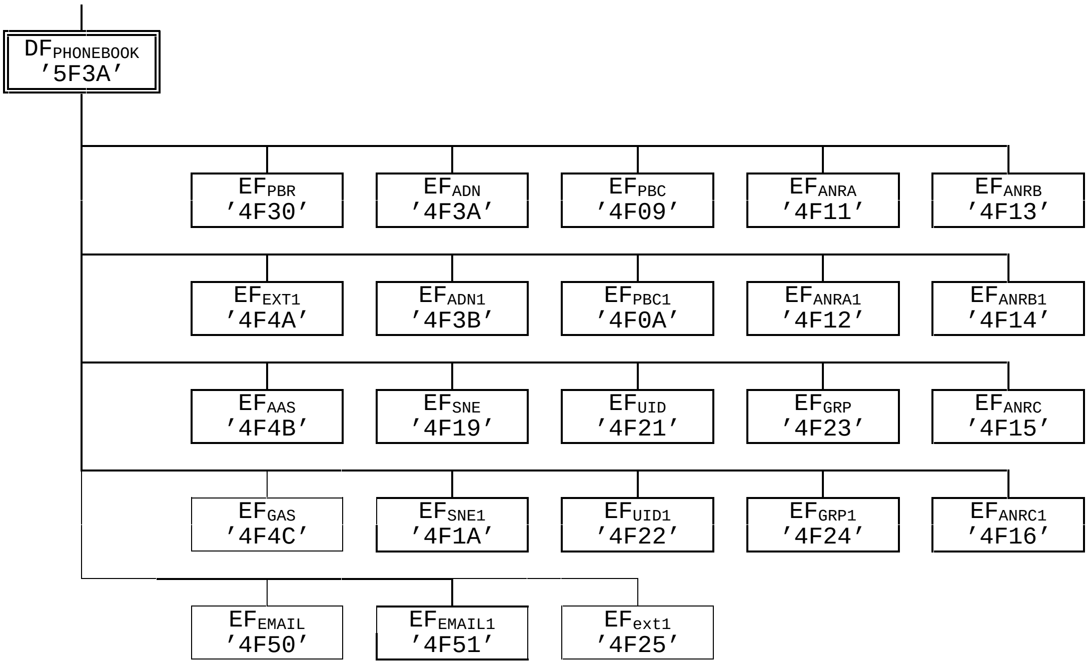


Table G.2: Contents of EF_{PBR}

Rec 1	Tag’D8’	L=’22’	Tag’C0’	L=’03’	’4F3A’	’01’	Tag’C5’	L=’03’	’4F09’	’02’	Tag’C4’	L=’02’	’4F11’	Tag’C4’
	L=’02’	’4F13’	Tag’C4’	L=’02’	’4F15’	Tag’C3’	L=’02’	’4F19’	Tag’C9’	L=’02’	’4F21’	Tag’CA’	L=’02’	’4F50’
	Tag’DA’	L=’0C’	Tag’C2’	L=’02’	’4F4A’	Tag’C7’	L=’02’	’4F4B’	Tag’C8’	L=’02’	’4F4C’	’FF’		
Rec 2	Tag’D8’	L=’20’	Tag’C0’	L=’02’	’4F3B’	Tag’C5’	L=’02’	’4F0A’	Tag’C4’	L=’02’	’4F12’	Tag’C4’	L=’02’	’4F14’
	Tag’C4’	L=’02’	’4F16’	Tag’C3’	L=’02’	’4F1A’	Tag’C9’	L=’02’	’4F22’	Tag’CA’	L=’02’	’4F51’	Tag’DA’	L=’0C’
	Tag’C2’	L=’02’	’4F25’	Tag’C7’	L=’02’	’4F4B’	Tag’C8’	L=’02’	’4F4C’	’FF’				

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

Phone book entry	ADN ’4F3A’ SFI ’01’		PBC ’4F09’ SFI ’02’	GRP ’4F23’	ANRA ’4F11’	ANRB ’4F13’	ANRC ’4F15’	SNE ’4F19’	UID ’4F21’	EXT1 ’4F4A’	AAS ’4F4B’	GAS ’4F4C’	EMAIL ’4F50’
# 1	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec ’02’	Hidden (AID rec N° 3)	Rec n°1 Rec n°3 '00'	ANR1 Rec n°1	ANR2 Rec n°2	ANR3 Rec n°3	Second Name Alpha String	UID	Rec '02'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP	email address
# 2	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '2A'	Not Hidden	Rec n°2 Rec n°1 Rec n°3	ANR1 Rec n°1	ANR2 Rec n°2	ANR3 Rec n°3	Second Name Alpha String	UID	Rec '2A'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP	email address
# 3													
:													
:													
:													
# 254													

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

Phone book entry	ADN1 ’4F3B’		PBC1 ’4F0A’	GRP1 ’4F24’	ANRA1 ’4F12’	ANRB1 ’4F14’	ANRC1 ’4F16’	SNE1 ’4F1A’	UID1 ’4F22’	EXT1 ’4F4A’	AAS ’4F4B’	GAS ’4F4C’	EMAIL1 ’4F51’
#255	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '02'	Hidden (AID Rec n° 3)	Rec n°1 Rec n°3 '00'	ANR1 Rec n°2	ANR2 Rec n°2	ANR3 Rec n°3	Second Name Alpha String	UID	Rec '02'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP1	email address
#256	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '2A'	Not Hidden	Rec n°2 Rec n°1 Rec n°3	ANR1 Rec n°2	ANR2 Rec n°2	ANR3 Rec n°3	Second Name Alpha String	UID	Rec '2A'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP1	email address
#257													
:													
:													
:													
#508													

Table G5, G6 and G7 show examples of which files may appear after the three main tags ’D8’,’D9’,’DA’.

Table G5: Tag D8

Description	Subclause
EF_{ADN}	4.4.2.3
EF_{IAP}	4.4.2.2
EF_{EXT1}	4.4.2.4
EF_{PBC}	4.4.2.5
EF_{GRP}	4.4.2.6
EF_{AAS}	4.4.2.7
EF_{ANR}	4.4.2.9
$EF_{E\text{-}mail}$	4.4.2.13
EF_{UID}	4.4.2.12.1

If present in the phone book record EF_{ADN} should be the first file ID specified after Tag D8, thus becoming the master file.

Table G6: Tag D9

Description	Subclause
EF$_{EXT1}$	4.4.2.4
EF$_{AAS}$	4.4.2.7
EF$_{ANR}$	4.4.2.9
EF$_{E\text{-}mail}$	4.4.2.13
EF$_{SNE}$	4.4.2.10

Table G7: Tag DA

Description	Subclause
EF$_{EXT1}$	4.4.2.4
EF~~$_{PAS}$~~$_{AAS}$	4.4.2.7
~~EF$_{E\text{-}mail}$~~	~~4.4.2.13~~
EF~~$_{ANR}$~~$_{GAS}$	4.4.2.8

3GPP TSG-T3 (USIM) Meeting #15
San Diego, USA, 16-18 August 2000

***Document* T3-000405**
revised from T3-000378

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

TS 31.102 CR 046 Current Version: V3.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T #9	for approval	☒	strategic	□	*(for SMG use only)*
list expected approval meeting # here ↑		for information	□	non-strategic	□	

Form: CR cover sheet, version 2 for 3GPP and SMG The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM ☒ ME ☒ UTRAN / Radio □ Core Network □
(at least one should be marked with an X)

Source:	T3	**Date:**	18/08/2000
Subject:	Alignment of EF(CCP2) with EF(ECCP)		
Work item:	T.E.I.		

Category:	F	Correction	☒	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	□		Release 99	☒
					Release 00	□

Reason for change: EF(CCP2) should have the same structure as EF(ECCP), as defined in GSM 11.11 R'99

Clauses affected: 4.2.38

Other specs affected:	Other 3G core specifications	□	→ List of CRs:
	Other GSM core specifications	□	→ List of CRs:
	MS test specifications	□	→ List of CRs:
	BSS test specifications	□	→ List of CRs:
	O&M specifications	□	→ List of CRs:

Other comments:

4.2.38 EF_{CCP2} (Capability Configuration Parameters 2)

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

Identifier: '6F4F'	Structure: linear fixed	Optional
SFI: '16'		
Record length: ~~14~~X bytes, X≥15	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

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

- Bearer capability information elements.
  - Contents and Coding:
    - see 3G TS 24.008 [9]. The Information Element Identity (IEI) shall be excluded, i.e. the first byte of the EF_{CCP2} record shall be Length of the bearer capability contents.
    - ~~Bytes 11-14 shall be set to 'FF' and shall not be interpreted by the terminal.~~
    - unused bytes are filled with 'FF'

3GPP TSG-T3 (USIM) Meeting #15
San Diego, USA, 16-18 August 2000

Document T3-000410

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

TS 31.102 **CR** **047rev1** (was marked 049r1

Current Version: V3.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: TSG-T #9
list expected approval meeting # here ↑

for approval	☒	strategic	□	*(for SMG use only)*
for information	□	non-strategic	□	

Form: CR cover sheet, version 2 for 3GPP and SMG The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM ☒ ME ☒ UTRAN / Radio □ Core Network □
(at least one should be marked with an X)

Source: T3 **Date:** 16/08/2000

Subject: Correction of record length, editorial errors, missing FID

Work item: T.E.I.

Category: *(only one category shall be marked with an X)*

F	Correction	☒	**Release:**	Phase 2	□
A	Corresponds to a correction in an earlier release	□		Release 96	□
B	Addition of feature	□		Release 97	□
C	Functional modification of feature	□		Release 98	□
D	Editorial modification	□		Release 99	☒
				Release 00	□

Reason for change: Correction of obvious errors (e.g. wrong references, inconsistencies in no. of bytes in an EF description, ..), as well as editorial corrections in the current version of the specification

Clauses affected: 3.3, 3.4, 4.1, 4.2.21, 4.2.34, 4.2.42, 4.2.48, 4.2.50, 4.4.3.4, 4.4.3.5, 4.4.4.1, 4.4.4.2, 4.4.4.3, 4.4.4.4, 4.4.4.5, 4.5.1, 4.7, 5.3.6, 6.4, 7.1.2

Other specs affected:

Other 3G core specifications	□	→ List of CRs:	
Other GSM core specifications	□	→ List of CRs:	
MS test specifications	□	→ List of CRs:	
BSS test specifications	□	→ List of CRs:	
O&M specifications	□	→ List of CRs:	

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
AC	Access Condition
ACL	APN Control List
ADF	Application Dedicated File

AID	Application IDentifier
AK	Anonymity key
ALW	ALWays
AMF	Authentication Management Field
AoC	Advice of Charge
APN	Access Point Name
AuC	Authentication Centre
AUTN	Authentication token
BDN	Barred Dialling Number
CCP	Capability Configuration Parameter
CK	Cipher key
CLI	Calling Line Identifier
CNL	Co-operative Network List
CPBCCH	COMPACT Packet BCCH
CS	Circuit switched
DCK	Depersonalisation Control Keys
DF	Dedicated File
DO	Data Object
EF	Elementary File
EMUI	Encrypted Mobile User Identity
FCP	File Control Parameters
FFS	For Further Study
GMSI	Group Identity
GSM	Global System for Mobile communications
HE	Home Environment
ICC	Integrated Circuit Card
ICI	Incoming Call Information
ICT	Incoming Call Timer
ID	IDentifier
IK	Integrity key
IMSI	International Mobile Subscriber Identity
K	USIM Individual key
K_C	Cryptographic key used by the cipher A5
KSI	Key Set Identifier
LI	Language Indication
LSB	Least Significant Bit
MAC	Message authentication code
MAC-A	MAC used for authentication and key agreement
MAC-I	MAC used for data integrity of signalling messages
MCC	Mobile Country Code
MExE	Mobile Execution Environment
MF	Master File
MMI	Man Machine Interface
MNC	Mobile Network Code
MODE	Indication packet switched / circuit switched mode
MSB	Most Significant Bit
NEV	NEVer
NPI	Numbering Plan Identifier
OCI	Outgoing Call Information
OCT	Outgoing Call Timer
OFM	Operational Feature Monitor
PIN	Personal Identification Number
PL	Preferred Languages
PS	Packet switched
PS_DO	PIN Status Data Object
RAND	Random challenge
$RAND_{MS}$	Random challenge stored in the USIM
RES	User response
RFU	Reserved for Future Use
RST	Reset
SDN	Service dialling number
SE	Security Environment

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

3.4 Coding Conventions

The following coding conventions apply to the present document.

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

The coding of Data Objects in the present document is according to ISO/IEC 7816-6 [16].

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

4.1 Contents of the EFs at the MF level

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

4.2.21 EF_{ECC} (Emergency Call Codes)

This EF contains emergency call codes.

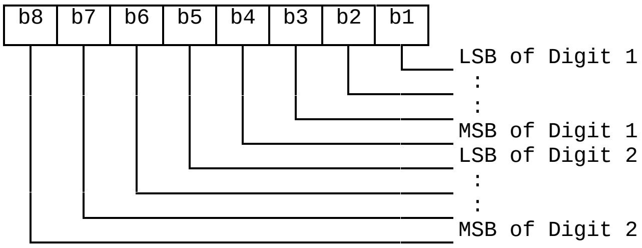
Identifier: '6FB7'	Structure: linear fixed	Mandatory
SFI: '01'		
Record size~~ size~~: X+~~6~~ 4 bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 3	Emergency Call Code	M	3 bytes
4 to X+~~4~~3	Emergency Call Code Alpha Identifier	O	X bytes
X+4 ~~5 to X+6~~	Emergency Call Type Indicator	M	1 byte

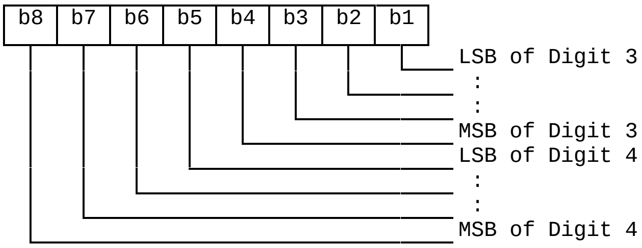
- Emergency Call Code.
  Contents:
  - Emergency Call Code.

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

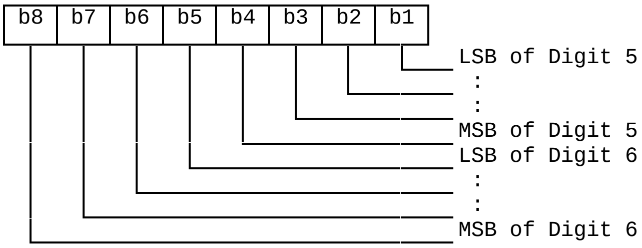
Byte 1:



Byte 2:



Byte 3:



- Emergency Call Code Alpha Identifier.
  Contents:
  Information about the dialled emergency number to be displayed to the user.
  Coding:
  this alpha-tagging shall use
    either:
  - the SMS default 7-bit coded alphabet as defined in 3G TS 23.038 [5] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'.

  Or
  - one of the UCS2 coded options as defined in the annex of 3G TS 31.101 [11].
- Emergency Call Type Indicator.
  Contents:
  Set to RFU. Information to be sent to the network indicating the type of emergency call.
  Coding:
  Coding according to 24.008 [9].

NOTE The coding is not yet defined and therefore this byte is set to RFU. A terminal shall not interpret the Emergency Call Type Indicator that has its value set to RFU. Furthermore a terminal not supporting the emergency call type indication towards the network shall not interpret the Emergency Call Type Indicator byte in this EF.

4.2.34 EF$_{OCI}$ (Outgoing Call Information)

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

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

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

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

Coding scheme is according to EF$_{ICI}$.

Structure of EF$_{OCI}$

<table>
<tr><td colspan="2">Identifier: '6F81'</td><td>Structure: Cyclic</td><td>Optional</td></tr>
<tr><td colspan="2">SFI: '15'</td><td colspan="2"></td></tr>
<tr><td colspan="2">Record length: X+~~26~~ 27 bytes</td><td colspan="2">Update activity: high</td></tr>
<tr><td colspan="4">Access Conditions:
READ PIN
UPDATE PIN
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td>Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1 to X</td><td>Alpha Identifier</td><td>O</td><td>X bytes</td></tr>
<tr><td>X+1</td><td>Length of BCD number/SSC contents</td><td>M</td><td>1 byte</td></tr>
<tr><td>X+2</td><td>TON and NPI</td><td>M</td><td>1 byte</td></tr>
<tr><td>X+3 to X+12</td><td>Outgoing Call Number/SSC String</td><td>M</td><td>10 bytes</td></tr>
<tr><td>X+13</td><td>Capability/Configuration2 Identifier</td><td>M</td><td>1 byte</td></tr>
<tr><td>X+14</td><td>Extension5 Record Identifier</td><td>M</td><td>1 byte</td></tr>
<tr><td>X+15 to X+21</td><td>Outgoing call date and time</td><td>M</td><td>7 bytes</td></tr>
<tr><td>X+22 to X+24</td><td>Outgoing call duration</td><td>M</td><td>3 bytes</td></tr>
<tr><td>X+25 to X+27</td><td>Link to Phone Book Entry</td><td>M</td><td>3 bytes</td></tr>
</table>

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

4.2.42 EF$_{\text{Hiddenkey}}$ (Key for hidden phone book entries)

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

Identifier: ’6FC3’	Structure: transparent	Optional
File size: 4 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

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

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

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

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

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

Identifier: '6F57'	Structure: transparent	Optional
Record length: X bytes (X>1)	Update activity: low	
Access Conditions: READ PIN UPDATE PIN2 DEACTIVATE ADM ACTIVATE ADM		

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

For contents and coding of APN-TLVs see TS 23.003 [~~24~~25].

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

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

Identifier: '6F32'	Structure: transparent		Optional
File size: 6n bytes		Update activity: low	
Access Conditions: READ PIN UPDATE ADM ~~INVALIDATE~~DEACTIVATE ADM ~~REHABILITATE~~ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to 6	Element 1 of co-operative net list	M	6 bytes
6n-5 to 6n	Element n of co-operative net list	O	6 bytes

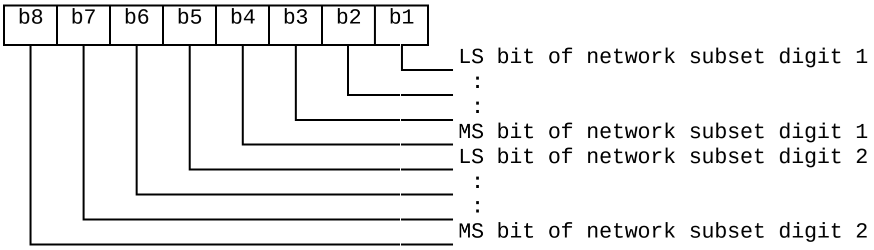
- Co-operative Network List.

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

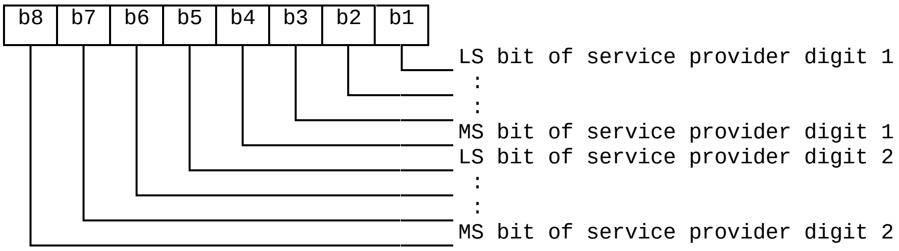
Coding:
- For each 6 byte list element.

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

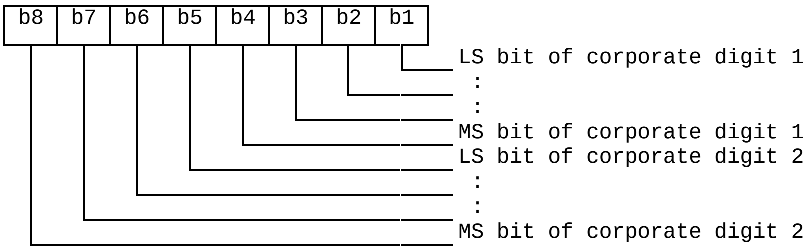
Byte 4:


b8
b7
b6
b5
b4
b3
b2
b1
LS bit of network subset digit 1
:
:
MS bit of network subset digit 1
LS bit of network subset digit 2
:
:
MS bit of network subset digit 2

Byte 5:


b8
b7
b6
b5
b4
b3
b2
b1
LS bit of service provider digit 1
:
:
MS bit of service provider digit 1
LS bit of service provider digit 2
:
:
MS bit of service provider digit 2

Byte 6:


b8
b7
b6
b5
b4
b3
b2
b1
LS bit of corporate digit 1
:
:
MS bit of corporate digit 1
LS bit of corporate digit 2
:
:
MS bit of corporate digit 2

- Empty fields shall be coded with 'FF'.

- The end of the list is delimited by the first MCC field coded 'FFF'.

4.4.3.4 EF$_{CPBCCH}$ (CPBCCH Information)

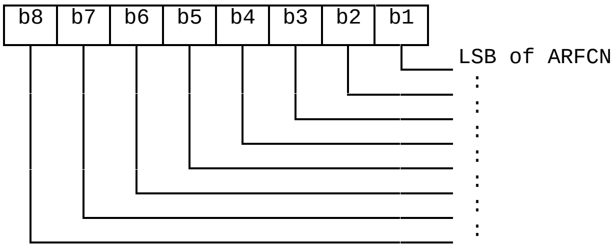
This EF contains information concerning the CPBCCH according to GSM 04.18 [28].

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

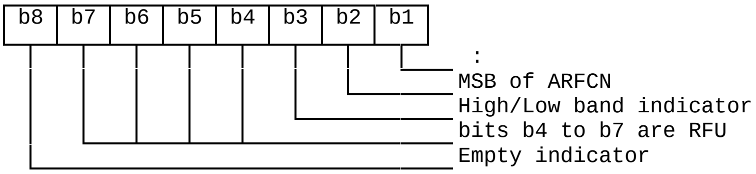
Identifier: '6F75'	Structure: transparent		Optional
File size: 2n bytes		Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE~~INVALIDATE~~ ADM ACTIVATE~~REHABILITATE~~ ADM			
Bytes	Description	M/O	Length
1 to 2	Element 1 of CPBCCH carrier list	M	2 bytes
2n-1 to 2n	Element n of CPBCCH carrier list	M	2 bytes

- Element in CPBCCH carrier list
  Coding:

  Byte 1: first byte of CPBCCH carrier list element



  Byte 2: second byte of CPBCCH carrier list element



- ARFCN (10 bits) as defined in GSM 05.05.

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

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

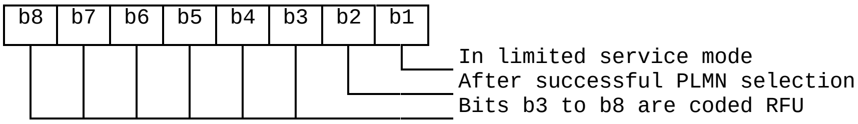
4.4.3.5 EF$_{InvScan}$ (Investigation Scan)

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

Identifier: ’6F76’	Structure: transparent		Optional
File size: 1 byte		Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE~~INVALIDATE~~ ADM ACTIVATE~~REHABILITATE~~ ADM			
Bytes	Description	M/O	Length
1	Investigation scan flags	M	1 byte

- Investigation scan flags

Coding:



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

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

4.4.4 Contents of files at the MExE level

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

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

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

This EF indicates which MExE services are allocated, and whether, if allocated, the service is activated. If a service is not allocated or not activated in the USIM, the ME shall not select this service.

<table>
<tr><td colspan="2">Identifier: ’4F40’</td><td colspan="2">Structure: transparent</td><td>Optional</td></tr>
<tr><td colspan="3">File size: X bytes, X □ 1</td><td colspan="2">Update activity: low</td></tr>
<tr><td colspan="5">Access Conditions:
READ PIN
UPDATE ADM
DEACTIVATE~~INVALIDATE~~ ADM
ACTIVATE~~REHABILITATE~~ ADM</td></tr>
<tr><td>Bytes</td><td colspan="2">Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1</td><td colspan="2">Services n°1 to n°8</td><td>M</td><td>1 byte</td></tr>
<tr><td>2</td><td colspan="2">Services n°9 to n°16</td><td>O</td><td>1 byte</td></tr>
<tr><td>etc.</td><td colspan="2"></td><td></td><td></td></tr>
<tr><td>X</td><td colspan="2">Services (8X-7) to (8X)</td><td>O</td><td>1 byte</td></tr>
</table>

-Services

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

Coding:

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

4.4.4.2 EF$_{ORPK}$ (Operator Root Public Key)

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

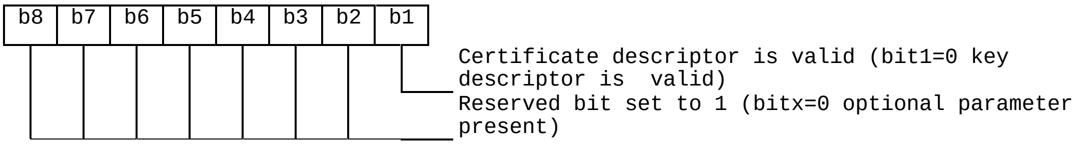
For example, an operator may provide a second key for recover disaster procedure in order to limit OTA data to load.

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

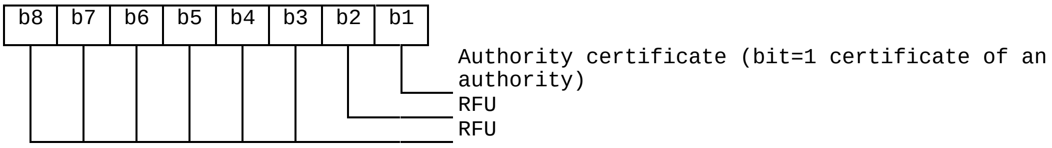
Access Conditions:
READ PIN
UPDATE ADM
DEACTIVATE~~INVALIDATE~~ ADM
ACTIVATE~~REHABILITATE~~ ADM

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

- Parameter indicator
  Contents:
  The parameter indicator indicates if record is full and which optional parameters are present
  Coding: bit string


b8
b7
b6
b5
b4
b3
b2
b1
Certificate descriptor is valid (bit1=0 key descriptor is valid)
Reserved bit set to 1 (bitx=0 optional parameter present)

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



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

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

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

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

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

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

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

4.4.4.3 EF$_{ARPK}$ (Administrator Root Public Key)

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

This file shall contain only one record.

Identifier: '4F42'	Structure: linear fixed	Optional
Record length: X + 10 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE~~INVALIDATE~~ ADM ACTIVATE~~REHABILITATE~~ ADM		

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

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

4.4.4.4 EF$_{TPRPK}$ (Third Party Root Public Key)

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

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

Identifier:'4F43'	Structure: linear fixed	Optional
Record length : X + 10 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE~~INVALIDATE~~ ADM ACTIVATE~~REHABILITATE~~ ADM		

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (k)	M	1 byte
11 to 10+k	Key identifier	M	k bytes
11+k to11+k	Certificate identifier length (m)	M	1 byte
12+k to11+k+m	Certificate identifier	M	m bytes

- Certificate identifier length

Contents:
This field gives length of certificate identifier
Coding:
binary

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

For contents and coding of all other data items see the respective data items of the EF$_{\mathrm{ORPK}}$ (sub-clause 4.4.4.2).

4.4.4.5 EF$_{\mathrm{TKCDF}}$ (Trusted Key/Certificates Data Files)

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

Identifier: ’4FXX’	Structure: transparent		Optional
Record length: Y bytes		Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE~~INVALIDATE~~ ADM ACTIVATE~~REHABILITATE~~ ADM			
Bytes	Description	M/O	Length
1 to Y	Key/Certicates Data	M	Y bytes

Contents and coding:

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

The identifier ’4FXX’ shall be different from one key/certificate data file to the other. For the range of ’XX’, see sub-clause 8.6 in 31.101 [11]. The length Y may be different from one key/certificate data file to the other.

4.5.1 EF_{ADN} (Abbreviated dialling numbers)

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

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

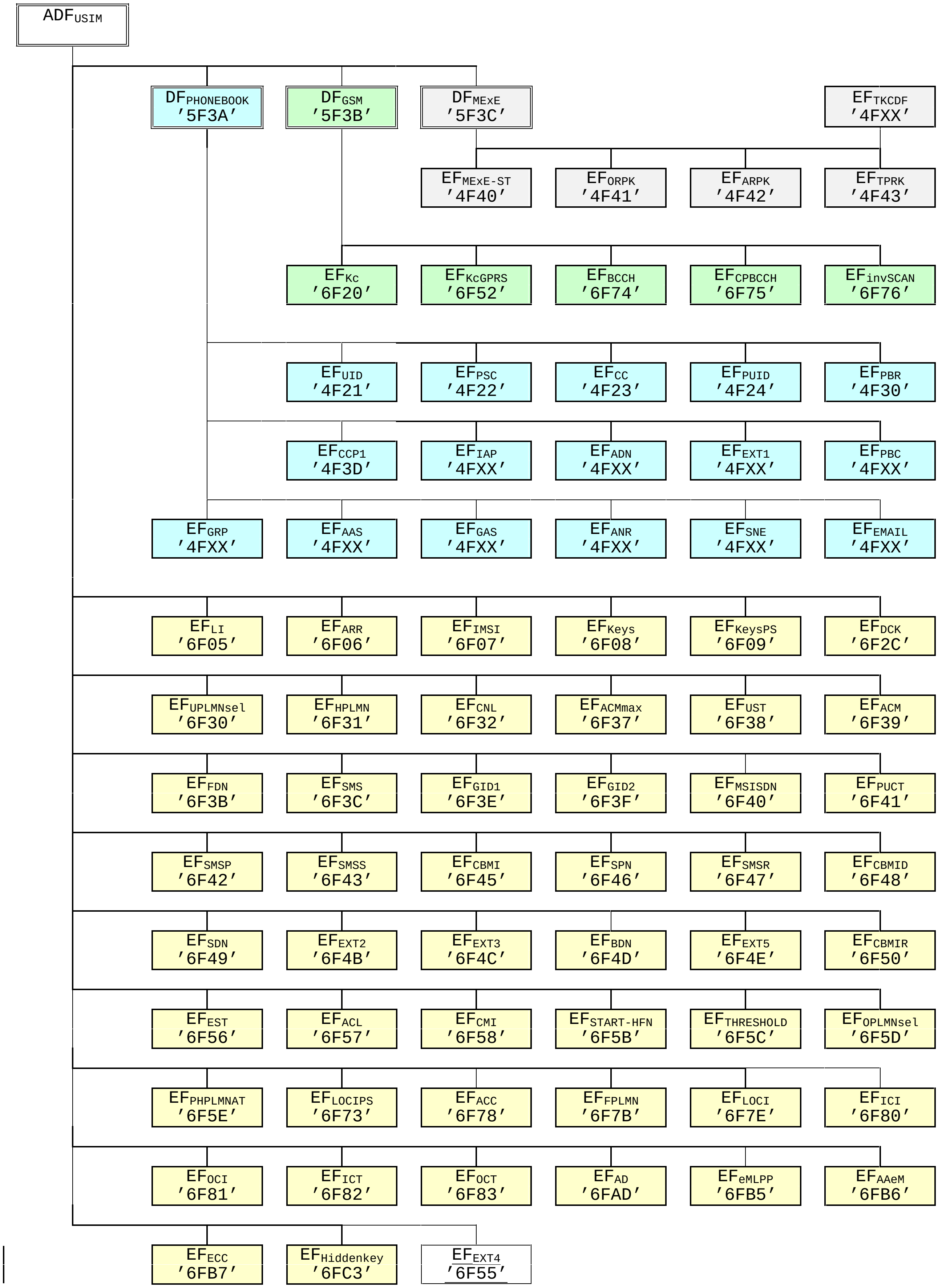


Figure 4.2: File identifiers and directory structures of USIM

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

5.3.6 PLMN selector

- Requirement: Service n°20 "available".
- Request: The ME performs the reading procedure with $EF_{UPLMNsel}$. followed by $EF_{OPLMNsel}$.
- Update: The ME performs the updating procedure with $EF_{\underline{U}PLMNsel}$.

6.4 User verification and file access conditions

The USIM application uses 2 PINs for user verification, PIN and PIN2. PIN2 is used only in the ADF. The PIN and PIN2 are mapped into key references as defined in 3G TS 31.101 [11]. Each key reference is associated with a usage qualifier as defined in ISO/IEC7816-9 [26]. The PIN status is indicated in the PS_DO, which is part of the FCP response when an ADF/DF is selected. The coding of the PS_DO is defined in 3G TS 31.101 [11].

PIN and PIN2 are coded on 8 bytes. Only (decimal) digits (0-9) shall be used, coded in CCITT T.50 [23] with bit 8 set to zero. The minimum number of digits is 4. If the number of digits presented by the user is less than 8 then the ME shall pad the presented PIN with 'FF' before sending it to the USIM.

The coding of the UNBLOCK PINs is identical to the coding of the PINs. However, the number of (decimal) digits is always 8.

The security architecture as defined in 3G TS 31.101 [11] applies to the USIM application with the following definitions and additions.

- The USIM application shall use key reference '01' as PIN and key reference '81' as PIN2. For access to DFTelecom the PIN shall be verified. Access with PIN2 is limited to the USIM application.
- The only valid usage qualifier is '08' which means user authentication knowledge based (PIN) as defined in ISO/IEC 7816-9 [26]. The terminal shall support the multi-application capabilities as defined in 31.101 [11].
- Every file in the USIM application shall have a reference to an access rule stored in EF_{ARR}.
- Every file under $DF_{Telecom}$ shall have a reference to an access rule stored in EF_{ARR} under $DF_{Telecom}$.
- A multi-application capability UICC (from the security context point of view) shall support the referenced format using SEID as defined in 3G TS 31.101 [11].
- A multi-application capability UICC (from the security context point of view) shall support the replacement of a USIM application PIN with the Universal PIN, key reference '01', as defined in 3G TS 31.101 [11]. Only the Universal PIN is allowed as a replacement.
- A terminal shall support the use of level 1 and level 2 user verification requirements as defined in 3G TS 31.101 [11].
- A terminal shall support the replacement of a USIM application PIN with the Universal PIN, key reference '01', as defined in 3G TS 31.101 [11].
- A terminal shall support the security attributes defined using tag's '8C', 'AB' and '8B' as defined in 3G TS 31.101 [11]. In addition both the referencing methods indicated by tag '8B' shall be supported as defined in 3G TS 31.101 [11].

The access rule is referenced in the FCP using tag '8B'. The TLV object contains the file ID (the file ID of EF_{ARR}) and record number, or file ID (the file ID of EF_{ARR}), SEID and record number, pointer to the record in EF_{ARR} where the access rule is stored. Each SEID refers to a record number in EF_{ARR}. EFs having the same access rule use the same record reference in EF_{ARR}. For a example EF_{ARR}, see 3G TS 31.101 [11]

~~A terminal conforming to the present document shall support the security attributes defined using tag's '8C', 'AB' and '8B' as defined in 3G TS 31.101. In addition both the referencing methods indicated by tag '8B' shall be supported as defined in 3G TS 31.101 [11].~~

7.1.2 Command parameters and data

Code	Value
CLA	As specified in 3G TS 31.101
INS	’88’
P1	’00’
P2	See table below
Lc	See below
Data	See below
Le	~~See below~~’00’, or maximum length of data expected in reponse

Parameter P2 specifies the authentication context as follows:

Coding of the reference control P2

Coding b8-b1	Meaning
’1-------’	Specific reference data (e.g. DF specific/application dependant key)
’-XXXXXX-’	’000000’
’-------X’	Authentication context: 0 GSM context 1 3G context

All other codings are RFU.

Command parameters/data:

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

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

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

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

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

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

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

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

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

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

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

3GPP T3 Meeting #15
San Diego, USA, 16 - 18 August, 2000

Tdoc T3-000408

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

31.102 CR 048 Current Version: 3.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: TSG-T #9
list expected approval meeting # here ↑

for approval	☒	strategic	□	*(for SMG use only)*
for information	□	non-strategic	□	

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: (U)SIM ☒ ME ☒ UTRAN / Radio □ Core Network □
(at least one should be marked with an X)

Source: T3 **Date:** 17/08/00

Subject: APN Control List coding

Work item:

Category:
(only one category shall be marked with an X)

F	Correction	☒	**Release:**	Phase 2	□
A	Corresponds to a correction in an earlier release	□		Release 96	□
B	Addition of feature	□		Release 97	□
C	Functional modification of feature	□		Release 98	□
D	Editorial modification	□		Release 99	☒
				Release 00	□

Reason for change: The actual implementation of APN Control List needs a Tag value for APNs stored in EF_{ACL}.

Clauses affected: Annex D

Other specs affected:

Other 3G core specifications	□	→ List of CRs:	
Other GSM core specifications	□	→ List of CRs:	
MS test specifications	□	→ List of CRs:	
BSS test specifications	□	→ List of CRs:	
O&M specifications	□	→ List of CRs:	

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

4.2.48 EF$_{ACL}$ (Access Point Name Control List)

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

Identifier: '6F57'	Structure: transparent		Optional
Record length: X bytes (X>1)	Update activity: low		
Access Conditions:			
READ	PIN		
UPDATE	PIN2		
DEACTIVATE	ADM		
ACTIVATE	ADM		
Bytes	Description	M/O	Length
1	Number of APNs	M	1 byte
2 to X	APN TLVs	M	X-1 byte

For contents and coding of APN-TLVs values see TS 23.003 [24]. The tag value of the APN-TLV shall be 'DD'.

Annex D (informative): Tags defined in 31.102

Tag	Name of Data Element	Usage
'D8'	Indicator for type 1 EFs (amount of records equal to master EF)	Phone Book Reference File (EF$_{PBR}$)
'D9'	Indicator for type 2 EFs (EFs linked via the index administration file)	Phone Book Reference File (EF$_{PBR}$)
'DA'	Indicator for type 3 EFs (EFs addressed inside a TLV object) The following are encapsulated under 'XZ': 'C0' EF$_{ADN}$ data object 'C1' EF$_{IAP}$ data object 'C2' EF$_{ECT1}$ data object 'C3' EF$_{SNE}$ data object 'C4' EF$_{ANR}$ data object 'C5' EF$_{PBC}$ data object 'C6' EF$_{GRP}$ data object 'C7' EF$_{AAS}$ data object 'C8' EF$_{GAS}$ data object 'C9' EF$_{UID}$ data object	Phone Book Reference File (EF$_{PBR}$)
'DC'	Synchronisation failure	Response to AUTHENTICATE
'DB'	Successful 3G authentication	Response to AUTHENTICATE
'DD'	Access Point Name	APN Control List (EF$_{ACL}$)

3GPP TSG T3 #15
San Diego, USA, 16-18 August 2000

Document T3-00-409
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

31.102 CR 049 Current Version: 3.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T #9	for approval	X	strategic	□	*(for SMG use only)*
list expected approval meeting # here ↑		for information	□	non-strategic	□	

Form: CR cover sheet, version 2 for 3GPP and SMG The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM X ME X UTRAN / Radio □ Core Network □
(at least one should be marked with an X)

Source: T3 **Date:** 16-Aug-2000

Subject: Alignment with 33.102 regarding authentication sequence numbers

Work item: T.E.I.

Category:	F	Correction	X	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	□		Release 99	X
					Release 00	□

Reason for change:

1) TS 31.102 shall not use the term "SEQ" in the description of the authentication procedure as SEQ is only defined in an informative annex to TS 33.102. Instead, the general term "SQN" shall be used.

2) The description of the basic acceptance conditions for a sequence number shall more precisely reflect the requirements in TS 33.102.

3) Annex C shall be "informative" to align with TS 33.102.

Clauses affected: 6.1, 7.1.1.1, Annex C

Other specs affected:	Other 3G core specifications	□	→ List of CRs:	
	Other GSM core specifications	□	→ List of CRs:	
	MS test specifications	□	→ List of CRs:	
	BSS test specifications	□	→ List of CRs:	
	O&M specifications	□	→ List of CRs:	

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

6.1 Authentication and key agreement procedure

This subclause gives an overview of the authentication mechanism and cipher and integrity key generation which are invoked by the network. For the specification of the corresponding procedures across the USIM/ME interface see clause 5.

The mechanism achieves mutual authentication by the user and the network showing knowledge of a secret key K which is shared between and available only to the USIM and the AuC in the user's HE. In addition, the USIM and the HE keep track of counters ~~SEQ~~SQN$_{MS}$ and ~~SEQ~~SQN$_{HE}$ respectively to support network authentication. SQN$_{HE}$ is a counter in the HLR/AuC, individual for each user and SQN$_{MS}$ denotes the highest sequence number the USIM has ever accepted.

When the SN/VLR initiates an authentication and key agreement, it selects the next authentication vector and sends the parameters RAND and AUTN (authentication token) to the user. Each authentication token consists of the following components: a sequence number SQN, an Authentication Management Field (AMF) and a message authentication code MAC over the RAND, SQN and AMF.

The USIM checks whether AUTN can be accepted and, if so, produces a response RES which is sent back to the SN/VLR. The SN/VLR compares the received RES with XRES. If they match the SN/VLR considers the authentication and key agreement exchange to be successfully completed. The USIM also computes CK and IK. The established keys CK and IK will be used by the ME to perform ciphering and integrity functions.

A permanent secret key K is used in this procedure. This key K has a length of 128 bits and is stored within the USIM for use in the algorithms described below. Also more than one secret key K can be stored in the USIM. The active key to be used by the algorithms is signalled within the AMF field in the AUTN.

7.1.1.1 3G security context

The USIM first computes the anonymity key AK = f5$_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK.

Then the USIM computes XMAC = f1$_K$ (SQN || RAND || AMF) and compares this with the MAC which is included in AUTN. If they are different, the USIM abandons the function.

Next the USIM verifies that the received sequence number SQN is previously unused. If it is unused and its value is lower than SQN$_{MS}$, it shall still be accepted if it is among the last 50 sequence numbers generated. ~~in the correct range.~~ ~~This~~ A possible verification method is described in annex C.

NOTE: This implies that the USIM has to keep a list of the last used sequence numbers and the length of the list is at least 50 entries.

If the USIM detects the sequence numbers to be ~~not in the correct range~~invalid, this is considered as a synchronisation failure and the USIM abandons the function. In this case the command response is AUTS, where:

AUTS = Conc(~~SEQ~~SQN$_{MS}$ *) || MACS;*
Conc(~~SEQ~~SQN$_{MS}$*) = ~~SEQ~~SQN*$_{MS}$ *⊕ f5*$_K$*(MACS || 0...0)* is the concealed value of the counter *~~SEQ~~SQN*$_{MS}$ in the USIM; and.
*MACS = f1**$_K$*(~~SEQ~~SQN*$_{MS}$ || *RAND* || *AMF)* where:
RAND is the random value received in the current user authentication request;
the AMF assumes a dummy value of all zeroes so that it does not need to be transmitted in clear in the resynchronisation message.

If the sequence number is considered in the correct range, the USIM computes RES = f2$_K$ (RAND), the cipher key CK = f3$_K$ (RAND) and the integrity key IK = f4$_K$ (RAND) and includes these in the command response. Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND.

The use of AMF is HE specific and while processing the command, the content of the AMF has to be interpreted in the appropriate manner. The AMF may e.g. be used for support of multiple algorithms or keys or for changing the size of lists, see 3G TS 33.102 [13].

If Service n°27 is "available", the USIM calculates the GSM response parameter K$_C$, using the conversion function defined in 3G TS 33.102 [13].

Input:

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

Output:

- RES, CK, IK if Service n°27 is "not available".

or

- RES, CK, IK, K$_C$ if Service n°27 is "available".

or

- AUTS.

Annex C (~~normative~~informative): Management of Sequence Numbers

The following is a recommendation for the management of sequence numbers SQN in the USIM. For efficiency reasons, it is taken into account that authentication vectors may be generated in batches (such that all authentication vectors in one batch are sent to the same SN/VLR).

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

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

C.1 Acceptance rule

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

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

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

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

NOTE 1: The purpose of condition (i) is to protect against wrap around of the counter in the USIM.

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

NOTE 2: This allows for a memory-efficient storage of batch numbers: With the exception of SEQ_{MS}, the batch numbers in the list need not be stored in full length, if those entries in the list which would cause the limit *L* to be exceeded are removed from the list after a new sequence number has been accepted.

C.2 List update

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

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

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

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

- Then *IND(SEQ)* is set to *IND*.

If a sequence number received in a user authentication request is rejected the list remains unaltered.

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

3GPP TSG-T3 (USIM) Meeting #15
San Diego, USA, August 16-18, 2000

***Document* T3-000452**
Revised from Tdoc T3-000431

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

TS 31.102 **CR** **050** Current Version: 3.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: TSG-T #09
list expected approval meeting # here ↑

for approval	X	strategic	□	*(for SMG*
for information	□	non-strategic	□	*use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM X ME X UTRAN / Radio □ Core Network □
(at least one should be marked with an X)

Source: T3 **Date:** 18-08-00

Subject: Preferred language selection

Work item: TEI

Category:	F	Correction	X	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	□		Release 99	X
					Release 00	□

Reason for change: This CR contains a procedure to define the selection criteria for language selection. This procedure was missing.

Clauses affected: 5.1.1

Other specs affected:	Other 3G core specifications	□	→ List of CRs:
	Other GSM core specifications	□	→ List of CRs:
	MS test specifications	□	→ List of CRs:
	BSS test specifications	□	→ List of CRs:
	O&M specifications	□	→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

5.1 USIM management procedures

5.1.1 USIM initialisation

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

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

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

- ~~EF$_{LI}$ is not available;~~

- ~~EF$_{LI}$ does not contain an entry corresponding to a language specified in ISO 639[19];~~

- ~~the ME does not support any of the languages in EF$_{LI}$.~~

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

The preferred language selection shall always use the EF$_{LI}$ in preference to the EF$_{PL}$ at the MF unless any of the following conditions applies:

- If the EF$_{LI}$ has the value ‘FFFF’ in its highest priority position then the preferred language selection shall be the language preference in the EF$_{PL}$ at the MF level according the procedure defined in 3G TS 31.101[11].

- If the ME does not support any of the language codes indicated in EF$_{LI}$, or if EF$_{LI}$ is not present, then the language selection shall be as defined in EF$_{PL}$ at the MF level according the procedure defined in 3G TS 31.101[11].

- If neither the language of the EF$_{LI ,}$ nor the EF$_{PL}$ is supported by the terminal then it shall use its own internal default selection.

3GPP TSG-T3 (USIM) Meeting #15
San Diego, USA, August 16-18, 2000

Document T3-000475
Supersedes T3-000466 (includes CR number)

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

TS 31.102 CR 051 Current Version: 3.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: TSG-T #9
list expected approval meeting # here ↑

for approval □
for information □

strategic □
non-strategic □
(for SMG use only)

Form: CR cover sheet, version 2 for 3GPP and SMG The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects:
(at least one should be marked with an X)

(U)SIM ☒ ME ☒ UTRAN / Radio □ Core Network □

Source: T3 **Date:** 18.8.2000

Subject: Application Selection by partial AID

Work item:

Category:
(only one category shall be marked with an X)

F Correction ☒
A Corresponds to a correction in an earlier release □
B Addition of feature □
C Functional modification of feature □
D Editorial modification □

Release:
Phase 2 □
Release 96 □
Release 97 □
Release 98 □
Release 99 ☒
Release 00 □

Reason for change: The application selection by partial DF name has been added in order to support the selection of the last selected application as requested by S1 for release 99.

Clauses affected: 5.1.1.1, 5.1.1.2, 5.1.1.3

Other specs affected:

Other 3G core specifications	□	→ List of CRs:	
Other GSM core specifications	□	→ List of CRs:	
MS test specifications	□	→ List of CRs:	
BSS test specifications	□	→ List of CRs:	
O&M specifications	□	→ List of CRs:	

Other comments: Accompanying CR to TS 102 221

help.doc

<---------- double-click here for help and instructions on how to create a CR.

5.1 USIM management procedures

5.1.1 Initialisation

5.1.1.1 USIM application selection

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

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

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

5.1.1.2~~1~~ USIM initialisation

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

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

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

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

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

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

The ME performs the administrative information request.

The ME performs the USIM Service Table request.

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

The ME performs the Enabled Services Table Request.

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

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

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

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

TS 31.102 **CR** **052** Current Version: V3.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-T #9	for approval	☒	strategic	□	*(for SMG*
list expected approval meeting # here ↑		for information	□	non-strategic	□	*use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM ☒ ME ☒ UTRAN / Radio □ Core Network □
(at least one should be marked with an X)

Source: T3 **Date:** 18/08/2000

Subject: PLMN with access technology and PLMN selection with access technology

Work item: T.E.I.

Category:	F	Correction	☒	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	□		Release 99	☒
					Release 00	□

Reason for change: This CR contains a warning with respect to PLMN with access technology and selection, as the status with this issue is still under discussion within 3GPP TSG SA.

Clauses affected: 4.2.5, 4.2.53, 4.2.54, 5.1.1.1, 5.2.14, 5.3.6

Other specs affected:	Other 3G core specifications	□	→ List of CRs:
	Other GSM core specifications	□	→ List of CRs:
	MS test specifications	□	→ List of CRs:
	BSS test specifications	□	→ List of CRs:
	O&M specifications	□	→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

4.2.5 EF$_{\text{UPLMNsel}}$ (UPLMN selector)

Note: PLMN with access technology and PLMN selection with access technology are still under discussion by 3GPP TSG SA and may be subject to change.

This EF contains the coding for n PLMNs, where n is at least eight. This information is determined by the user and defines the preferred PLMNs of the user in priority order. The first record indicates the highest priority and the nth record indicates the lowest.

Identifier: '6F30'	Structure: transparent	Optional
SFI: '0A'		
File size: 5n (where n >=8) bytes	Update activity: low	

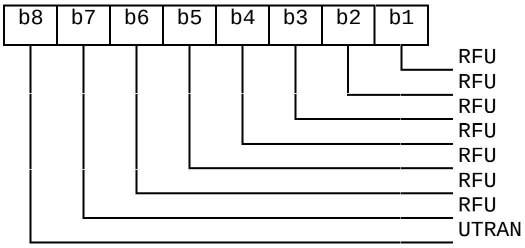
Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

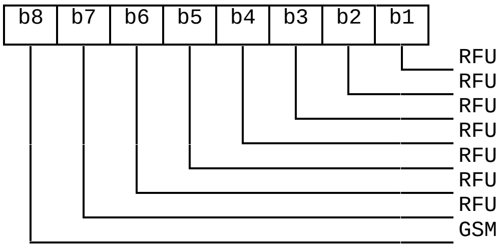
Bytes	Description	M/O	Length
1 to 3	1st PLMN (highest priority)	M	3 bytes
4 to 5	1st PLMN Access Technology Identifier	M	2 bytes
6 to 8	2nd PLMN	M	3 bytes
9 to 10	2nd PLMN Access Technology Identifier	M	2 bytes
:	:		
36 to 38	8th PLMN	M	3 bytes
39 to 40	8th PLMN Access Technology Identifier	M	2 bytes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

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

Byte 4:



Byte 5:



4.2.53 EF$_{\text{OPLMNsel}}$ (OPLMN selector)

Note: PLMN with access technology and PLMN selection with access technology are still under discussion by 3GPP TSG SA and may be subject to change.

This EF contains the coding for n PLMNs where n is determined by the operator. This information is determined by the operator and defines the preferred PLMNs in priority order. The first record indicates the highest priority and the nth record indicates the lowest.

Identifier: ’6F5D’	Structure: transparent	Optional
SFI: ’11’		
File size: 5n (where n >=8 bytes)	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

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

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

  Coding:
  - according to 3G TS 24.008 [9].
- Access Technology Identifier:
  Coding:
  - See EF$_{\text{UPLMNsel}}$ for coding.

4.2.54 EF$_{\text{PHPLMNAT}}$ (Preferred HPLMN Access Technology)

Note: PLMN with access technology and PLMN selection with access technology are still under discussion by 3GPP TSG SA and may be subject to change.

This EF contains the user preferred access technologies for the HPLMN.

Identifier: ’6F5E’	Structure: Transparent	Optional
SFI: ’13’		
File size: 2 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 2	Access Technology Identifier	M	2 bytes

- Access Technology Identifier:

Coding:

- See $EF_{UPLMNsel}$ for coding.

5.1 USIM management procedures

5.1.1 Initialisation

5.1.1.1 USIM initialisation

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

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

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

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

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

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

The ME performs the administrative information request.

The ME performs the USIM Service Table request.

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

The ME performs the Enabled Services Table Request.

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

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

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

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

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

- IMSI request.
- Access control information request.
- HPLMN search period request.
- HPLMN preferred access technology request.
- User PLMN selector request.
- Operator PLMN selector request.
- GSM initialisation requests.
- Location Information request for CS-and/or PS-mode.
- Cipher key and integrity key request for CS- and/or PS-mode.

- Forbidden PLMN request.
- Initialisation value for hyperframe number request.
- Maximum value of START request.
- CBMID request.
- Depending on the further services that are supported by both the ME and the USIM the corresponding EFs have to be read.

Note: PLMN with access technology and PLMN selection with access technology are still under discussion by 3GPP TSG SA and may be subject to change.

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

5.2.14 HPLMN preferred access technology request

Note: PLMN with access technology and PLMN selection with access technology are still under discussion by 3GPP TSG SA and may be subject to change.

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

5.3.6 PLMN selector

Note: PLMN with access technology and PLMN selection with access technology are still under discussion by 3GPP TSG SA and may be subject to change.

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

3GPP T3 Meeting #15
San Diego, USA, 16-18 Aug 2000

Document T3-000482
Superceedes T3-000464

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

31.102 CR 053 Current Version: 3.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: TSG-T #9
list expected approval meeting # here ↑

for approval	X	strategic		*(for SMG Use only)*
For information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM X ME X UTRAN / Radio □ Core Network □
(at least one should be marked with an X)

Source: T3 **Date:** 18/08/2000

Subject: Clarification of the phonebook

Work item: T.E.I.

Category:
(only one category shall be marked with an X)

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: This CR intents to provide clarifications to the phonebook by e.g. listing which files may exist in which type as well as explicitly introducing dependencies between files.

In addition some modifications are made to the phonebook example in Annex G.

Clauses affected: 4.4.2 and Annex G

Other specs Affected:

Other 3G core specifications		→ List of CRs:
Other GSM core specifications		→ List of CRs:
MS test specifications		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

4.4.2 Contents of files at the DF PHONEBOOK level

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

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

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

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

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

4.4.2.X Phonebook restrictions

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

- If a EF_{PBR} file contains more than one record then they shall all be formatted identically on a type-by-type basis, e.g. if EF_{PBR} record #1 contains one type 1 e-mail then all EF_{PBR} records shall have one type 1 email
- If a EF_{PBR} record contains more than one reference to a file of type then they shall all be formatted identically on a type-by-type basis, e.g. if a EF_{PBR} record has 2 email addresses then they shall have the same record size and the same number of records in each EF_{PBR} entry
- An EF_{PBR} record may contain TLV entries indicating that the file exist as a type 1 and 2 file, e.g. a phonebook entry may have two emails, one with a one-to-one mapping (type 1) and one with a indirect mapping (type 2). Regardless of the type, files in all entries have to have the same record configuration

Editor's note: this list is currently not complete

4.4.2.1 EF_{PBR} (Phone Book Reference file)

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

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

- Type 2 files: Files that contain less entries than the master file and are linked via pointers in the index administration file (EF_{IAP}).
- Type 3 files are files that are linked by a TLV object in a record (Grouping information in EF_{GAS}).

Table 4.1: Phone Book Reference file Constructed Tags

Tag Value	Constructed TAG Description
'D8'	Indicating files where the amount of records equal to master EF, type 1
'D9'	Indicating files that are linked using the index administration file, type 2. Order of pointer appearance in index administration EF is the same as the order of file IDs following this tag
'DA'	Indicating files that are addressed inside a TLV object, type 3. (The file pointed to is defined by the TLV object.)

The first file ID indicated using constructed Tag 'D8' is called the master EF. Access conditions for all other files in the index structure is set to the same as for the master EF unless otherwise specified.

File IDs indicated using constructed Tag 'D8' is a type 1 file and contains the same number of records as the first file that is indicated in the data part of this TLV object. All files following this Tag are mapped one to one using the record numbers/IDs of the first file indicated in this TLV object.

File IDs indicated using constructed Tag 'D9' are mapped to the master EF (the file ID indicated as the first data object in the TLV object using Tag 'D8') using the pointers in the index administration file. The order of the pointers in the index administration file is the same as the order of the file IDs presented after Tag 'D9'. If this Tag is not present in the reference file record the index administration file is not present in the structure. In case the index administration file is not present in the structure it is not indicated in the data following tag 'D8'.

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

Each constructed Tag contains a list of primitive Tags indicating the order and the type of data (e.g. ADN, IAP,…) of the reference structure. The primitive tag identifies clearly the type of data, its value field indicates the file identifier.

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

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

Table 4.X below list the allowed types for each file

Table 4.X: Presence of files as type

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

Phone Book Reference file EF_{PBR} structure

Identifier: ’4F30’	Structure: linear fixed	C~~Optional~~
SFI: Optional		
Record Length: X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	TLV object(s) for indicating EFs that are part of the phone book structure	M	X bytes

C: IF $DF_{Phonebook}$ is present this file is mandatory
ELSE not present.

4.4.2.2 EF_{IAP} (Index Administration Phone book)

This file is present if Tag ’D9’ is indicated in the reference file.

The EF contains pointers to the different records in the files that are part of the phone book. The index administration file record number/ID is mapped one to one with the corresponding EF_{ADN} (shall be record to record). The index administration file contains the same amount of records as EF_{ADN}. The order of the pointers in an EF_{IAP} shall be the same as the order of file IDs that appear in the TLV object indicated by Tag ’D9’ in the reference file record. The amount of bytes in a record is equal to the number of files indicated the EF_{PBR} following tag ’D9’.

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

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

Index administration file EF$_{IAP}$ structure

Identifier: ’4FXX’	Structure: linear fixed	~~Optional~~C
SFI: mandatory		
Record Length: X bytes	Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1	Record number of the first object indicated after Tag ’D9’	M	1 byte
2	Record number of the second object indicated after Tag ’D9’	M	1 byte
X	Record number of the xth object indicated after Tag ’D9’	M	1 byte
C: IF type 2 files are present then it is mandatory ELSE not present			

4.4.2.3 EF$_{ADN}$ (Abbreviated dialling numbers)

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

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

Identifier: ’4F3A	Structure: linear fixed	~~Optional~~C
SFI: mandatory		
Record length: X+14 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension1 Record Identifier	M	1 byte
C: IF DF$_{Phonebook}$ is present this file is mandatory ELSE not present.			

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

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

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

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

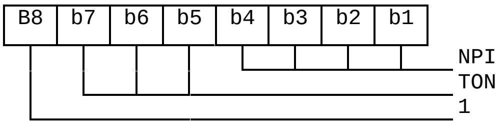
- Length of BCD number/SSC contents.
  Contents:
  - this byte gives the number of bytes of the following two data items containing actual BCD number/SSC information. This means that the maximum value is 11, even when the actual ADN/SSC information length is greater than 11. When an ADN/SSC has extension,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

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

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

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

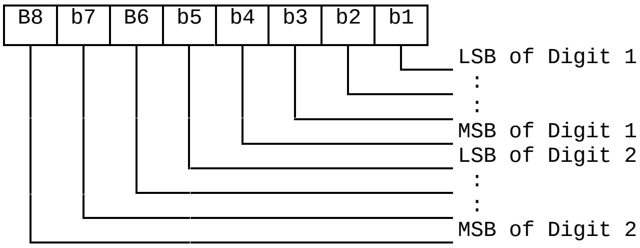
NOTE 2: If a dialling number is absent, no TON/NPI byte is transmitted over the radio interface (see 3G TS 24.008 [9]). Accordingly, the ME should not interpret the value 'FF' and not send it over the radio interface.



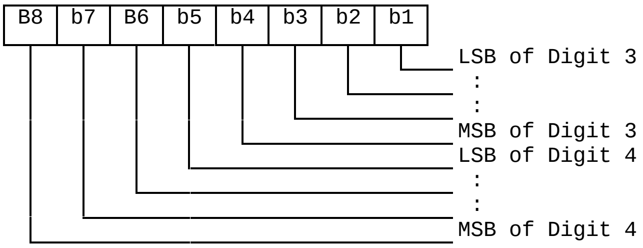
- Dialling Number/SSC String
  Contents:
  - up to 20 digits of the telephone number and/or SSC information.

  Coding:
  - according to 3G TS 24.008 [9] , 3G TS 22.030 [4] and the extended BCD-coding (see table 4.3). If the telephone number or SSC is longer than 20 digits, the first 20 digits are stored in this data item and the remainder is stored in an associated record in the EF_{EXT1}. The record is identified by the Extension1 Record Identifier. If ADN/SSC require less than 20 digits, excess nibbles at the end of the data item shall be set to 'F'. Where individual dialled numbers, in one or more records, of less than 20 digits share a common appended digit string the first digits are stored in this data item and the common digits stored in an associated record in the EF_{EXT1}. The record is identified by the Extension 1 Record Identifier. Excess nibbles at the end of the data item shall be set to 'F'.

Byte X+3



Byte X+4:



etc.

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

  Coding:
  - binary.

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

  Coding:
  - binary.

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

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

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

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

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

Table 4.3: Extended BCD coding

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

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

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

4.4.2.4 EF$_{EXT1}$ (Extension1)

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

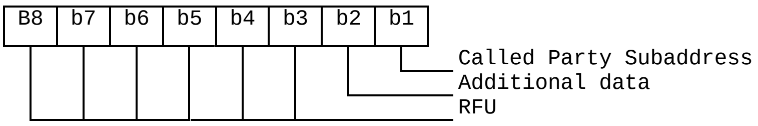
Extension data is caused by:

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

- an associated called party subaddress. The EXT1 record in this case is specified as subaddress data.

Identifier: ’4FXX’	Structure: linear fixed		Optional
SFI: Mandatory			
Record length: 13 bytes		Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

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



- b3-b8 are reserved and set to 0;

- a bit set to 1 identifies the type of record;

- only one type can be set;

- ’00’ indicates the type "unknown".

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

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

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

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

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

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

No of Record	Type	Extension Data	Next	Record
:	:	:	:	
:	:	:	:	
Record 3	‘02’	xx ……..xx	‘06’	
Record 4	‘xx’	xx ……..xx	‘xx’	
Record 5	‘01’	xx ……..xx	‘FF’	
Record 6	‘01’	xx ……..xx	‘05’	
:	:	:	:	
:	:	:	:	

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

4.4.2.5 EF$_{PBC}$ (Phone Book Control)

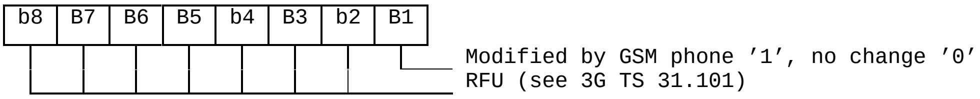
This EF contains control information related to each entry in the phone book. This EF contains as many records as the EF$_{ADN}$ associated with it (shall be record to record). Each record in EF$_{PBC}$ points to a record in its EF$_{ADN}$. This file indicates the control information and the hidden information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

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

Structure of control file EF_{PBC}

Identifier: '4FXX'	Structure: linear fixed		~~Optional~~C
SFI: Mandatory			
Record length: 2 bytes		Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1	Entry Control Information	M	1 byte
2	Hidden Information	M	1 byte
C: IF Hidden entries are supported or a GSM SIM application is supported in the UICC, this file is mandatory ELSE not present.			

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



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

4.4.2.6 EF_{GRP} (Grouping file)

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

Structure of grouping file EF_{GRP}

Identifier: '4FXX'	Structure: linear fixed		~~Optional~~C
SFI: Mandatory			
Record Length: X bytes (1 ≤ X ≤10)		Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1	Group Name Identifier 1	M	1 byte
2	Group Name Identifier 2	O	1 byte
X	Group Name Identifier X	O	1 byte
C: IF EF_{GAS} is present this file is mandatory ELSE not present.			

- Group Name Identifier x.

  Content:

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

  Coding:

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

4.4.2.7 EF_{AAS} (Additional number Alpha String)

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

Structure of EF_{AAS}

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

- Alpha text string.

  Content:

  - user defined text for additional number.

  Coding:

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

4.4.2.8 EF_{GAS} (Grouping information Alpha String)

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

Structure of EF$_{GAS}$

Identifier: '4FXX'	Structure: linear fixed		C~~optional~~
SFI: Recommended			
Record length: X bytes		Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to X	Alpha text string	M	X bytes
C: IF EF$_{GRP}$ is present this file is mandatory ELSE not present.			

- Alpha text string

Content:

- group names.

Coding:

- same as the alpha identifier in EF$_{ADN}$.

4.4.2.9 EF$_{ANR}$ (Additional Number)

Several phone numbers can be attached to one EF$_{ADN}$ record, using one or several EF$_{ANR}$. The amount of additional number entries may be less than or equal to the amount of records in EF$_{ADN}$. The EF structure is linear fixed. Each record contains an additional phone number. The first byte indicates whether the record is free or the type of additional number referring to the record number in EF$_{AAS}$, containing the text to be displayed. The following part indicates the additional number and the reference to the associated record in the EF$_{ADN}$ file.

Structure of EF$_{ANR}$

Identifier: '4FXX'	Structure: linear fixed		Optional
SFI: mandatory			
Record length: 12 or 14 ~~X+11~~ bytes		Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1	Additional Number identifier	M	1 byte
2 to 11	Additional number	M	10 bytes
12	Capability/Configuration Identifier	M	1 byte
13~~2~~	ADN file SFI	~~M/O~~ C	1 byte
14~~3~~	ADN file Record Identifier	~~M/O~~ C	1 byte
C: IF the file is of type 1, as specified in EF$_{PBR}$, then the field is not present ELSE the field is present			

- Additional Number Identifier

Content:

- describes the type of the additional number defined in the file EF$_{AAS}$.

Coding:

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

- Additional number

Content:

- additional phone number linked to the phone book entry.

Coding:

- - same than the dialling number /SSC string in EF$_{ADN.}$

- 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.

- ADN file SFI.

Content:

- Short File identifier of the associated EF$_{ADN}$ file.

Coding:

- as defined in the UICC specification.

- ADN file Record Identifier

Content:

- record identifier of the associated phone book entry.

Coding:

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

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

4.4.2.10 EF$_{SNE}$ (Second Name Entry)

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

Structure of EF$_{SNE}$

Identifier: ’4FXX’	Structure: linear fixed	Optional
SFI: mandatory		
Record length: X or X +2+~~2~~ bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier of Second Name	M	X bytes
X+1	ADN file SFI	C~~M/O~~	1 byte
X+2	ADN file Record Identifier	C~~M/O~~	1 byte
C: IF the file is of type 1, as specified in EF$_{PBR}$, then the field is not present ELSE the field is present			

- Alpha Identifier of Second Name.

  Content:

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

  Coding:

  - as the alpha identifier for EF$_{ADN}$.

- ADN file SFI.

  Content:

  - Short File identifier of the associated EF$_{ADN}$ file.

  Coding:

  - as defined in the UICC specification.

- ADN file Record Identifier

  Content:

  record identifier of the associated phone book entry.

  Coding:

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

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

4.4.2.11 EF$_{CCP1}$ (Capability Configuration Parameters 1)

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

Structure of EF$_{CCP1}$

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

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

- Bearer capability information element.

  Contents and Coding:

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

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

4.4.2.12 Phone Book Synchronisation

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

If synchronisation is supported in the phonebook EF$_{PSC}$, EF$_{UID}$, EF$_{PUID}$ and EF$_{CC}$ are all mandatory.

4.4.2.12.1 EF$_{UID}$ (Unique Identifier)

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

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

Structure of EF$_{UID}$

Identifier: ’4F21’	Structure: linear fixed	~~Optional~~C
SFI: optional		
Record length: 2 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 2	Unique Identifier (UID) of Phone Book Entry	M	2 bytes
C: IF synchronisation is supported in the phonebook this file is mandatory ELSE not present.			

- Unique Identifier of Phone Book Entry.

  Content:

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

  Coding:

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

4.4.2.12.2 EF$_{PSC}$ (Phone book Synchronisation Counter)

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

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

The PSC shall be regenerated by the terminal if one of the following situation applies:

- the values of the UIDs have run out of range;
- the whole phone book has been reset/deleted;
- the value of the CC has run out of range.

Structure of EF$_{PSC}$

Identifier: '4F22'	Structure: transparent		~~Optional~~C
SFI: optional			
File size: 4 bytes	Update activity: low		
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to 4	Phone book synchronisation counter (PSC)	M	4 bytes
C: IF synchronisation is supported in the phonebook this file is mandatory ELSE not present.			

- PSC: Unique synchronisation counter of Phone Book.

  Content:

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

  Coding:

  hexadecimal value.

  The phone book identifier coding based on the EF$_{PSC}$ is described hereafter:

- For a phone book residing in DF-telecom:

  - Phone book identifier = ICCid (10bytes) "fixed part" + 4 bytes (in EF$_{PSC}$) "variable part".

- For a phone book residing in an USIM application:

  - Phone book identifier = 10 last bytes of (ICCid XOR AID) "fixed part" + 4 bytes (in EF$_{PSC}$) "variable part".

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

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

    {Increment **PSC** mod ‘FF FF FF FF’; }.

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

  If CC = ‘FF FF’ then.

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

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

Incrementing **PSC** modulus 'FFFFFFFF'.

4.4.2.12.3 EF_{CC} (Change Counter)

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

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

Structure of EF_{CC}

Identifier: ’4F23’	Structure: transparent		~~Optional~~C
SFI: Mandatory			
File size: 2 bytes		Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to 2	Change Counter (CC) of Phone Book	M	2 bytes
C: IF synchronisation is supported in the phonebook this file is mandatory ELSE not present.			

- Change Counter of Phone Book.

  Content:

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

  Coding:

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

4.4.2.12.4 EF_{PUID} (Previous Unique Identifier)

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

Structure of EF$_{PUID}$

<table>
<tr><td colspan="2">Identifier: ’4F24’</td><td colspan="1">Structure: transparent</td><td>~~Optional~~C</td></tr>
<tr><td colspan="2">SFI: Mandatory</td><td colspan="2"></td></tr>
<tr><td colspan="2">File size: 2 bytes</td><td colspan="2">Update activity: high</td></tr>
<tr><td colspan="4">Access Conditions:
READ PIN
UPDATE PIN
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td>Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1 to 2</td><td>Previous Unique Identifier (PUID) of Phone Book Entry</td><td>M</td><td>2 bytes</td></tr>
<tr><td colspan="4">C: IF synchronisation is supported in the phonebook this file is mandatory
ELSE not present.</td></tr>
</table>

- Previous unique Identifier of Phone Book Entry.

  Content:

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

4.4.2.13 EF$_{EMAIL}$ (e-mail address)

This EF contains the e-mail addresses that may be linked to a phone book entry.

Several e-mail addresses can be attached to one EF$_{ADN}$ record, using one or several EF$_{EMAIL}$. The number of email addresses may be equal to or less than the amount of records in EF$_{ADN}$. Each record contains an e-mail address. The first part indicates the e-mail address, and the reference to the associated record in the EF$_{ADN}$ file.

Structure of EF$_{EMAIL}$

<table>
<tr><td colspan="2">Identifier: ’4FXX’</td><td>Structure: linear fixed</td><td>Optional</td></tr>
<tr><td colspan="2">SFI: Mandatory</td><td colspan="2"></td></tr>
<tr><td colspan="2">Record length: X ~~+ Y~~or X+2 b~~B~~ytes – see note</td><td colspan="2">Update activity: low</td></tr>
<tr><td colspan="4">Access Conditions:
READ PIN
UPDATE PIN
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td>Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1 to X</td><td>E-mail Address</td><td>M</td><td>X bytes</td></tr>
<tr><td>X+1</td><td>ADN file SFI</td><td>C~~M/O~~</td><td>1 byte</td></tr>
<tr><td>X+2</td><td>ADN file Record Identifier</td><td>C~~M/O~~</td><td>1 byte</td></tr>
<tr><td colspan="4">Note: If this file is configured as type 1, i.e. a one-to-one mapping, the ADN file SFI and the ADN file Record Identifier shall not be present, thus the length is X bytes. In all other cases these two bytes shall be present, thus the length is X+2 bytes.
C: IF the file is of type 1 then the field is present
ELSE it is not present</td></tr>
</table>

~~NOTE: Y =2 if items "ADN file SFI" and "ADN file Record Identifier exist", otherwise Y=0.~~

- E-mail Address.
  Content:

  - string defining the e-mail address

Coding:

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

- ADN file SFI.

  Content:

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

  Coding:

  - as defined in 3G TS 31.101.

- ADN file Record Identifier.

  Content:

  - record identifier of the associated phone book entry.

  Coding:

  - binary.

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

Annex G (informative): Phonebook Example

This example phonebook has more than 254 entries. Additional number (3 additional numbers) information, second name and e-mail information can be added to each ADN entry. In addition each entry has a 2 byte Unique ID (UID) attached to it. The phonebook also contains three files that are shared EF$_{\text{EXT1}}$, EF$_{\text{AAS}}$ and EF$_{\text{GAS}}$. These files are addressed from inside a file. EF$_{\text{EXT1}}$ is addressed via EF$_{\text{ADN,}}$ EF$_{\text{ADN1}}$, EF$_{\text{AAS}}$ is addressed via EF$_{\text{ANR1,}}$ EF$_{\text{ANR1}}$ and EF$_{\text{GAS}}$ is addresssed via EF$_{\text{GRP,}}$ EF$_{\text{GRP1}}$. The phonebook supports two levels of grouping and hidden entries in EF$_{\text{PBC.}}$

Two records are needed in the phonebook reference file PBR ’4F30’ for supporting more than 254 entries. The content of the phonebook reference file PBR ’4F30’ records is as shown in table G.2. The structure of the DF$_{\text{PHONEBOOK}}$ is shown in table G.1.

The content of phonebook entries in the range from 1-508 is described in the tables G.3 and G.4.

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

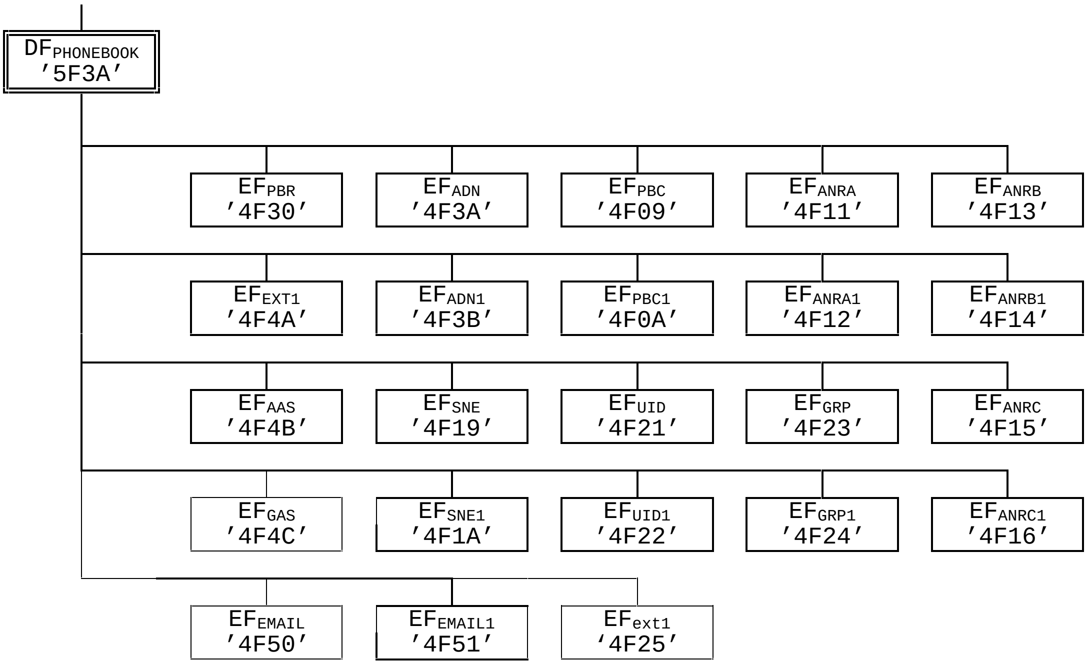


Table G.2: Contents of EF$_{\text{PBR}}$

Rec 1	Tag’D8’	L=’46’	Tag’C0’	L=’02’	’4F3A’	Tag’C5’	L=’02’	’4F09’	Tag’C4’	L=’02’	’4F11’	Tag’C4’	L=’02’	’4F13’
	Tag’C4’	L=’02’	’4F15’	Tag’C3’	L=’02’	’4F19’	Tag’C9’	L=’02’	’4F21’	Tag’CA’	L=’02’	’4F50’	Tag’DA’	L=’0C’
	Tag’C2’	L=’02’	’4F4A’	Tag’C7’	L=’02’	’4F4B’	Tag’C8’	L=’02’	’4F4C’	’FF’				
Rec 2	Tag’D8’	L=’46’	Tag’C0’	L=’02’	’4F3B’	Tag’C5’	L=’02’	’4F0A’	Tag’C4’	L=’02’	’4F12’	Tag’C4’	L=’02’	’4F14’
	Tag’C4’	L=’02’	’4F16’	Tag’C3’	L=’02’	’4F1A’	Tag’C9’	L=’02’	’4F22’	Tag’CA’	L=’02’	’4F51’	Tag’DA’	L=’0C’
	Tag’C2’	L=’02’	’4F25’	Tag’C7’	L=’02’	’4F4B’	Tag’C8’	L=’02’	’4F4C’	’FF’				

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

Phone book entry	AND ’4F3A’		PBC ’4F09’	GRP ’4F23’	ANRA ’4F11’	ANRB ’4F13’	ANRC ’4F15’	SNE ’4F19’	UID ’4F21’	EXT1 ’4F4A’	AAS ’4F4B’	GAS ’4F4C’	EMAIL ’4F50’
# 1	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec ’02’	Hidden (AID rec N° 3)	Rec n°1 Rec n°3 '00'	ANR1 Rec n°1	ANR2 Rec n°2	ANR3 Rec n°3	Second Name Alpha String	UID	Rec '02'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP	email address
# 2	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '2A'	Not Hidden	Rec n°2 Rec n°1 Rec n°3	ANR1 Rec n°1	ANR2 Rec n°2	ANR3 Rec n°3	Second Name Alpha String	UID	Rec '2A'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP	email address
# 3													
:													
:													
:													
# 254													

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

Phone book entry	AND ’4F3B’		PBC1 ’4F0A’	GRP1 ’4F24’	ANRA1 ’4F12’	ANRB1 ’4F14’	ANRC1 ’4F16’	SNE1 ’4F1A’	UID1 ’4F22’	EXT1 ’4F4A’	AAS ’4F4B’	GAS ’4F4C’	EMAIL1 ’4F51’
#255	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '02'	Hidden (AID Rec n° 3)	Rec n°1 Rec n°3 '00'	ANR1 Rec n°2	ANR2 Rec n°2	ANR3 Rec n°3	Second Name Alpha String	UID	Rec '02'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP1	email address
#256	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '2A'	Not Hidden	Rec n°2 Rec n°1 Rec n°3	ANR1 Rec n°2	ANR2 Rec n°2	ANR3 Rec n°3	Second Name Alpha String	UID	Rec '2A'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP1	email address
#257													
:													
:													
:													
#508													

~~Table G5, G6 and G7 show examples of which files may appear after the three main tags ‘D8’,’D9’,’DA’.~~

~~Table G5: Tag D8~~

~~Description~~	~~Subclause~~
~~EF$_{ADN}$~~	~~4.4.2.3~~
~~EF$_{IAP}$~~	~~4.4.2.2~~
~~EF$_{EXT1}$~~	~~4.4.2.4~~
~~EF$_{PBC}$~~	~~4.4.2.5~~
~~EF$_{GRP}$~~	~~4.4.2.6~~
~~EF$_{AAS}$~~	~~4.4.2.7~~
~~EF$_{ANR}$~~	~~4.4.2.9~~
~~EF$_{E-mail}$~~	~~4.4.2.13~~
~~EF$_{EXT1}$~~	~~****~~
~~EF$_{UID}$~~	~~4.4.2.12.1~~

~~If present in the phone book record EF$_{ADN}$ should be the first file ID specified after Tag D8, thus becoming the master file.~~

~~Table G6: Tag D9~~

~~**Description**~~	~~**Subclause**~~
~~EF$_{\text{EXT1}}$~~	~~4.4.2.4~~
~~EF$_{\text{AAS}}$~~	~~4.4.2.7~~
~~EF$_{\text{ANR}}$~~	~~4.4.2.9~~
~~EF$_{\text{E-mail}}$~~	~~4.4.2.13~~
~~EF$_{\text{EXT1}}$~~	****
~~EF$_{\text{SNE}}$~~	~~4.4.2.10~~

~~Table G7: Tag DA~~

~~**Description**~~	~~**Subclause**~~
~~EF$_{\text{EXT1}}$~~	~~4.4.2.4~~
~~EF$_{\text{PAS}}$~~	~~4.4.2.7~~
~~EF$_{\text{E-mail}}$~~	****
~~EF$_{\text{EXT1}}$~~	****
~~EF$_{\text{ANR}}$~~	~~4.4.2.8~~

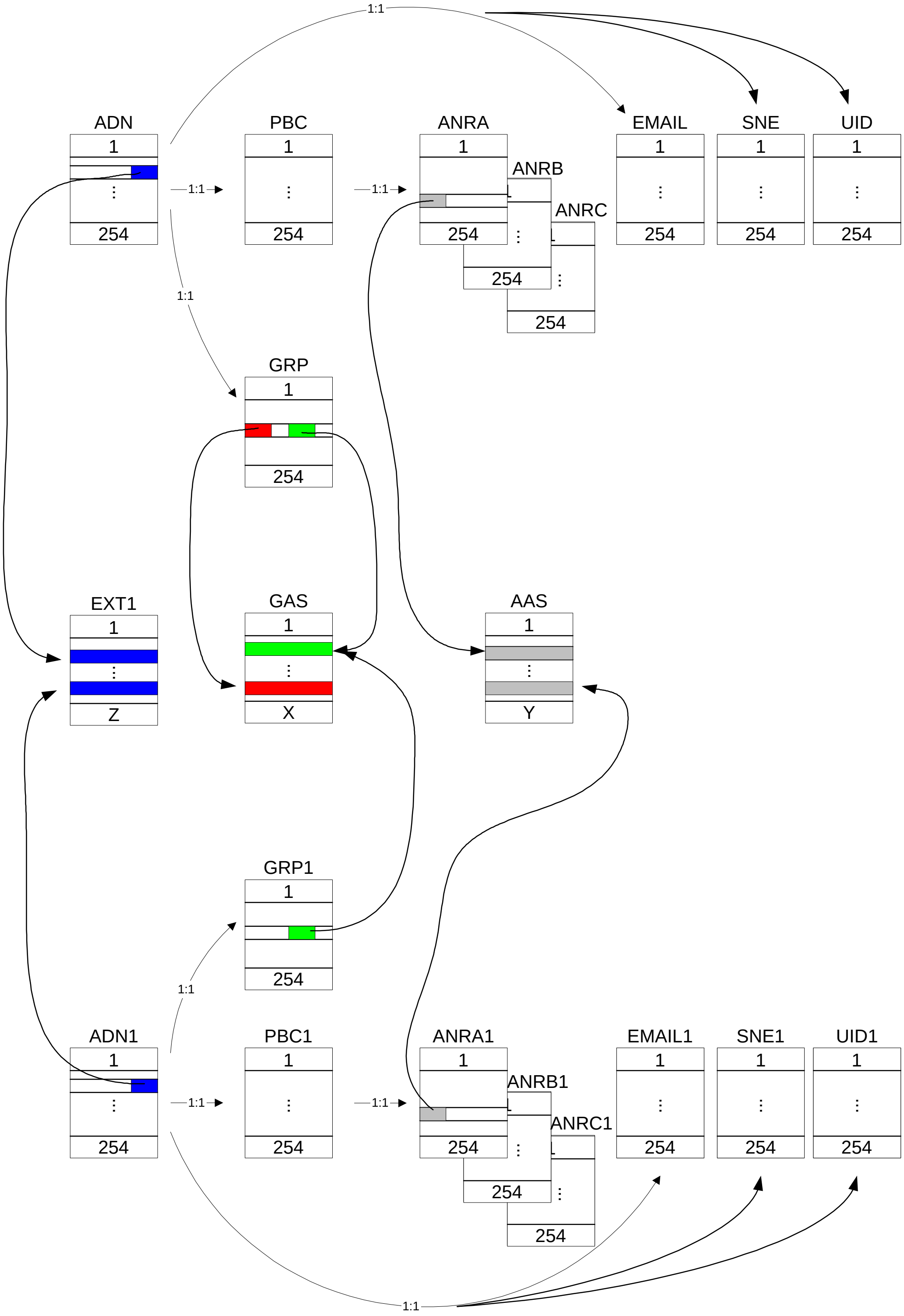


Figure G.1: Structure and Relations of the Example Phone Book