3GPP TSG-T (Terminals) Meeting #10
Bangkok, Thailand, 6 - 8 December, 2000

Tdoc TP-000203

Source: T3

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

Agenda item: 5.3.3

Document for: Approval

This document contains several change requests to TS 31.102 v3.3.0 agreed by T3.

T3 Doc	Spec	CR	Rv	Rel	Subject
T3-000617	31.102	055		R99	Corrections and clarifications on Phonebook
T3-000619	31.102	056		R99	Miscellaneous clarifications and minor corrections
T3-000620	31.102	057		R99	File-ID EFs of the phonebook
T3-000621	31.102	058		R99	Correction of the phonebook example
T3-000625	31.102	059		R99	Alignments with 3G TS 33.102 v3.6.0
T3-000596	31.102	062		R99	Phonebook correction on CCPs

3GPP TSG-T3 Meeting #16
Seoul, South Korea, 13-15 Nov. 2000

Tdoc T3-000617

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **055** ⌘ rev **-** ⌘ Current version: **3.3.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Corrections and clarifications on Phonebook
Source:	⌘	3GPP T3
Work item code:	⌘	***Date:*** ⌘ 15-11-2000
Category:	⌘	**F** ***Release:*** ⌘ R99

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

Use one of the following releases:

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

Reason for change:	⌘	The word "structure" is used in 4.4.2 with different meanings, leading to ambiguities. When to reset the flag EF_{PBC} in 4.4.2 is not indicated. When the terminal increment the value of the UID over 'FF FF', this one has to be regenerated. Introduction of a new abreviation :PBID for Phonebook Identifier
Summary of change:	⌘	Rephrasing for clarification
Consequences if not approved:	⌘	Specification can be misleading to some readers

Clauses affected:	⌘	3.3 , 4.4.2 , 4.4.2.12.1 and 4.4.2.12.2
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

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

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
AC	Access Condition
ACL	APN Control List
ADF	Application Dedicated File
AID	Application IDentifier
AK	Anonymity key
ALW	ALWays
AMF	Authentication Management Field
AoC	Advice of Charge
APN	Access Point Name
AuC	Authentication Centre
AUTN	Authentication token
PBID	Phonebook Identifier
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

4.4.2 Contents of files at the DF PHONEBOOK level

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

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

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

If the UICC is inserted into a GSM terminal and a record in the 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~~EF_{CC} ,and then reset the flag. A set flag in EF_{PBC} results in a full synchronisation of the phone-book between an external entity and the UICC (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 organisation of files in t~~T~~he application specific phone-book ~~is a copy of the file structure of~~ follows the same rules as the one specified for the public phone book under $DF_{TELECOM}$. The application specific phonebook may contain a different set of files than the one in the public area under $DF_{TELECOM}$.

4.4.2.1 EF_{PBR} (Phone Book Reference file)

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

4.4.2.12.1 EF_{UID} (Unique Identifier)

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

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

Structure of EF_{UID}

Identifier: '4F21'	Structure: linear fixed	Conditional (see Note)
SFI: 'XX'		
Record length: 2 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

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

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

- Unique Identifier of Phone Book Entry.

  Content:

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

  Coding:

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

4.4.2.12.2 EF_{PSC} (Phone book Synchronisation Counter)

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

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

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

Structure of EF_{PSC}

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

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

- PSC: Unique synchronisation counter of Phone Book.

  Content:

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

  Coding:

  hexadecimal value.

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

- For a phone book residing in DF-telecom:

  - ~~Phone book identifier~~PBID = ICCid (10bytes) "fixed part" + 4 bytes (in EF_{PSC}) "variable part".

- For a phone book residing in an USIM application:

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

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

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

    - If UID = 'FF FF' then.

      {Increment **PSC** mod 'FF FF FF FF'; all the UIDs shall be regenerated}.

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

    If CC = 'FF FF' then.

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

3GPP TSG-T3 (USIM) Meeting #16
Seoul, SK, 13-15 November 2000

***Document* T3-000619**
supersedes Tdocs T3-000534, T3-000535, T3-000536, T3-000540, T3-000582, T3-000598,

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	056	Current Version:	V3.3.0

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

For submission to:	TSG-T #10	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: *(at least one should be marked with an X)* (U)SIM [X] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T3 **Date:** 15/11/2000

Subject: Miscellaneous clarifications and minor corrections

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 4	

Reason for change:

Collection of clarifications, editorial and minor corrections :

- The update activity of the EF(START-HFN) is changed to "high"
- Clarification of the description of the EF(GRP)
- Renaming of DF GSM to DF GSM-ACCESS to avoid confusions.
– Clarification of hidden information if EF(PBC)
– Location Information : the "memory problem" status code is corrected
- The File Identifier of the EF-ARR and EF-CCP2 in the Annex are incorrect.

Clauses affected: 4.2.51, 4.4.2.5, 4.4.2.6, 4.4.3, 4.7, 5.2.5, Annex H

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.

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

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

Identifier: '6F5B'	Structure: transparent	Mandatory
SFI: '0F'		
File size: 6 bytes	Update activity: ~~low~~high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

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

4.4.2.5 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 $EF_{P\sout{CB}BC}$ and EF_{ADN}).

Structure of control file EF_{PBC}

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

Access Conditions:

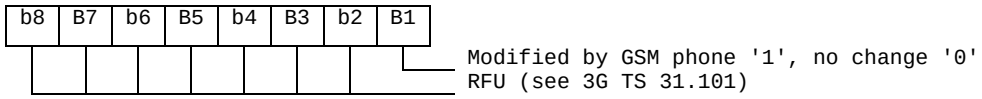
READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

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

  Coding:



- Hidden Information.
  Contents:
  indicates to which USIM~~/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~~. If the secret code is not verified, then the phone book entry is hidden.
  Coding:
  '00' – the phone book entry is not hidden;
  'xx' – the phone book entry is hidden. 'xx' is the record number in EF_{DIR} of the associated USIM application.

4.4.2.6 EF_{GRP} (Grouping file)

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

Structure of grouping file EF_{GRP}

Identifier: '4FXX'	Structure: linear fixed	Conditional (see Note)
SFI: 'XX'		
Record Length: X bytes (1 ≤ X ≤10)	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Group Name Identifier 1	M	1 byte
2	Group Name Identifier 2	O	1 byte
X	Group Name Identifier X	O	1 byte

NOTE: This file is mandatory if and only if EF_{GAS} is present.

- Group Name Identifier x.

  Content:

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

  Coding:

  - '00' – ~~the phone book entry is not part of a group~~ no group indicated;
  - 'XX' – record number in EF_{GAS} containing the alpha string naming the group of which the phone book entry is a member.

.

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

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

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

Figure 4.1: File identifiers and directory structures of UICC

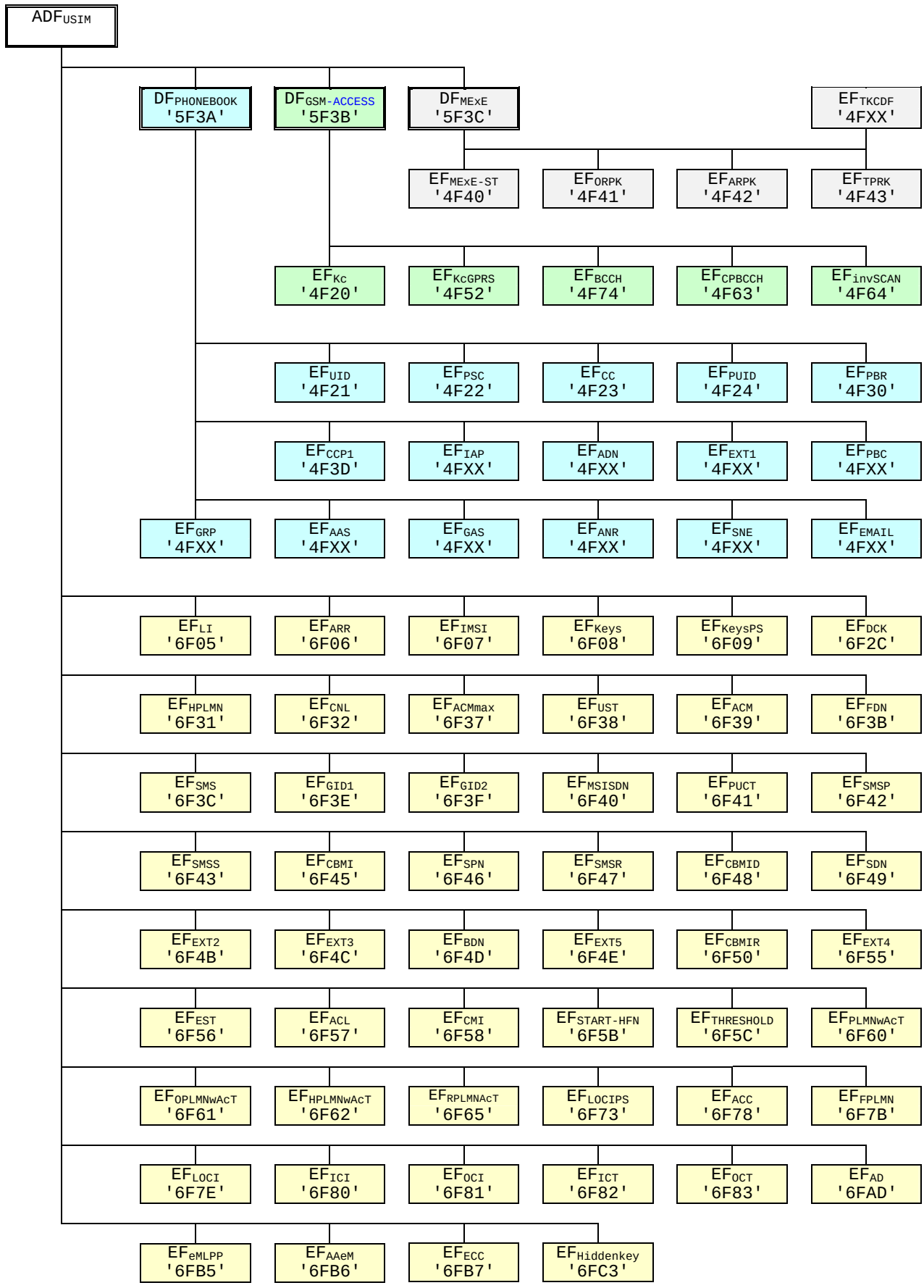


Figure 4.2: File identifiers and directory structures of USIM

5.2.5 Location information

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

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

In the case when updating EF_{LOCI} with data containing the TMSI value and the card reports the error '~~92 40~~65 81' (Memory Problem), the ME shall terminate 3G operation.

Annex H (normative): List of SFI Values

This annex lists SFI values assigned in this specification.

H.1 List of SFI Values at the USIM ADF Level

File Identification	SFI	Description
'6FB7'	'01'	Emergency call codes
'6F05'	'02'	Language indication
'6FAD'	'03'	Administrative data
'6F38'	'04'	USIM service table
'6F56'	'05'	Enabled services table
'6F78'	'06'	Access control class
'6F07'	'07'	IMSI
'6F08'	'08'	Ciphering and integrity keys
'6F09'	'09'	Ciphering and integrity keys for packet switched domain
'6F60'	'0A'	User PLMN selector
'6F7E	'0B'	Location information
'6F73'	'0C'	Packet switched location information
'6F7B'	'0D'	Forbidden PLMNs
'6F48'	'0E'	CBMID
'6F5B'	'0F'	Hyperframe number
'6F5C'	'10'	Maximum value of hyperframe number
'6F61'	'11'	Operator PLMN selector
'6F31'	'12'	HPLMN search period
'6F62'	'13'	Preferred HPLMN access technology
'6F80'	'14'	Incoming call information
'6F81'	'15'	Outgoing call information
'6F4F~~39~~'	'16'	Capability configuration parameters 2
'6F064F~~'~~'	'17'	Access Rule Reference
'6F65'	'18'	RPLMN last used Access Technology

All other SFI values are reserved for future use.

H.2 List of SFI Values at the DF GSM-ACCESS Level

File Identification	SFI	Description
'4F20'	'01'	GSM Ciphering Key Kc
'4F52'	'02'	GPRS Ciphering Key KcGPRS
'4F74'	'03'	Broadcast Control Channel BCCH

All other SFI values are reserved for future use.

3GPP TSG-T3 (USIM) Meeting #16
Seoul, SK, 13-15 November 2000

Document T3-000620
Supersedes Tdocs T3-000599

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**	**057**	Current Version:	V3.3.0

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

For submission to: TSG-T #10 *list expected approval meeting # here ↑*

for approval [X] 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 [X] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T3 **Date:** 15/11/2000

Subject: file-id of EFs of the phonebook

Work item: T.E.I.

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

F	Correction	[X]
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	[X]
Release 4	[ ]

Reason for change: The file-id of the EF(ADN) and EF(UID) cannot be fixed, as there might be several instances of these files (in the case where a phonebook holds more than 254 entries).

Clauses affected: 4.4.2.3, 4.4.2.12.1, 4.5.1, 4.5.2, 4.7, Annex A, Annex E

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.

4.4.2.3 EF_{ADN} (Abbreviated dialling numbers)

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

Identifier: '4F~~3A~~XX'	Structure: linear fixed	Conditional (see Note)
SFI: 'XX'		
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

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: '4F~~21~~XX'	Structure: linear fixed	Conditional (see Note)
SFI: 'XX'		
Record length: 2 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

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

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

- Unique Identifier of Phone Book Entry.

  Content:

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

  Coding:

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

4.5 Contents of EFs at the TELECOM level

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

4.5.1 EF_{ADN} (Abbreviated dialling numbers)

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

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

4.5.2 EF_{EXT1} (Extension1)

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

4.7 Files of USIM

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

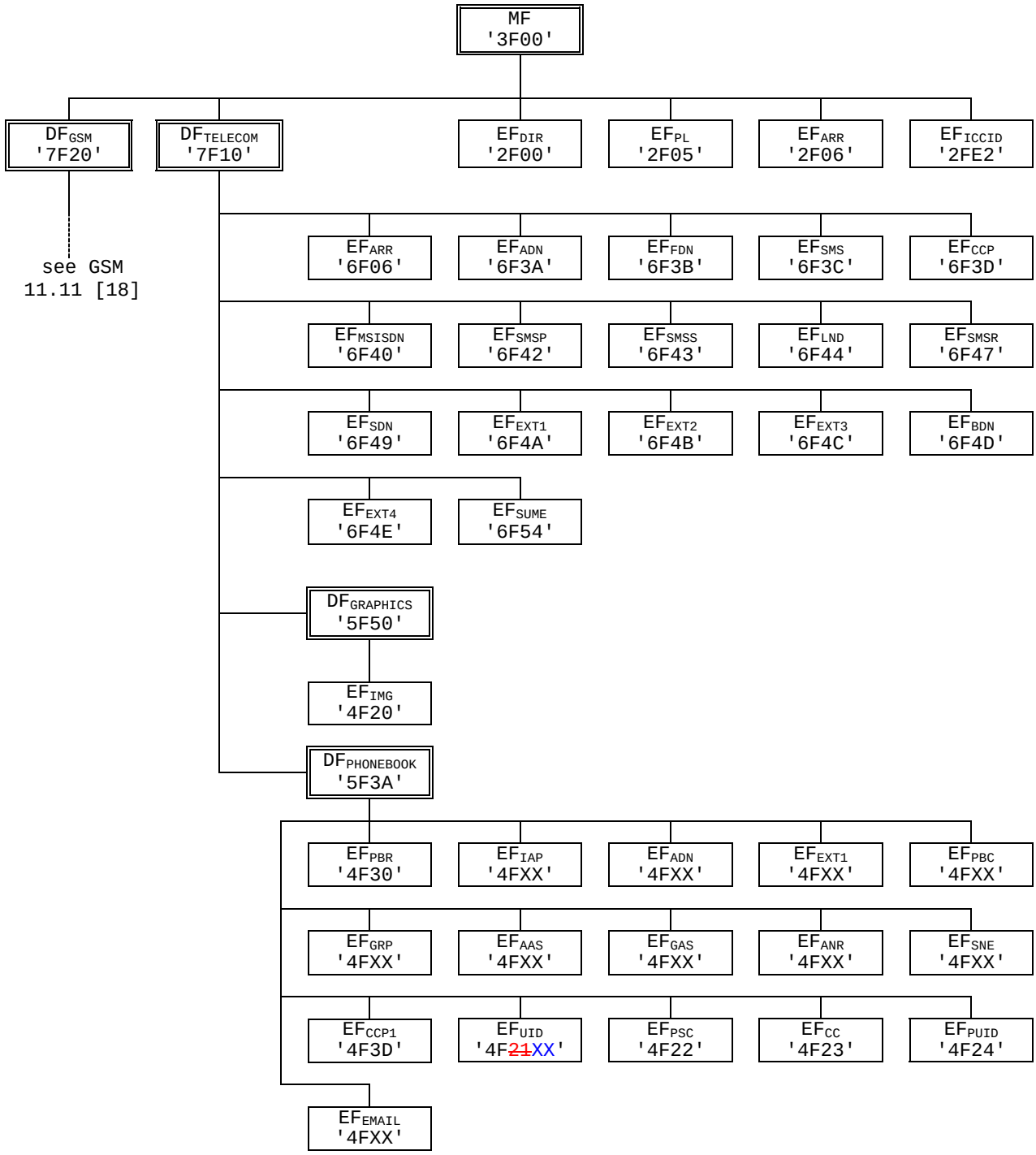


Figure 4.1: File identifiers and directory structures of UICC

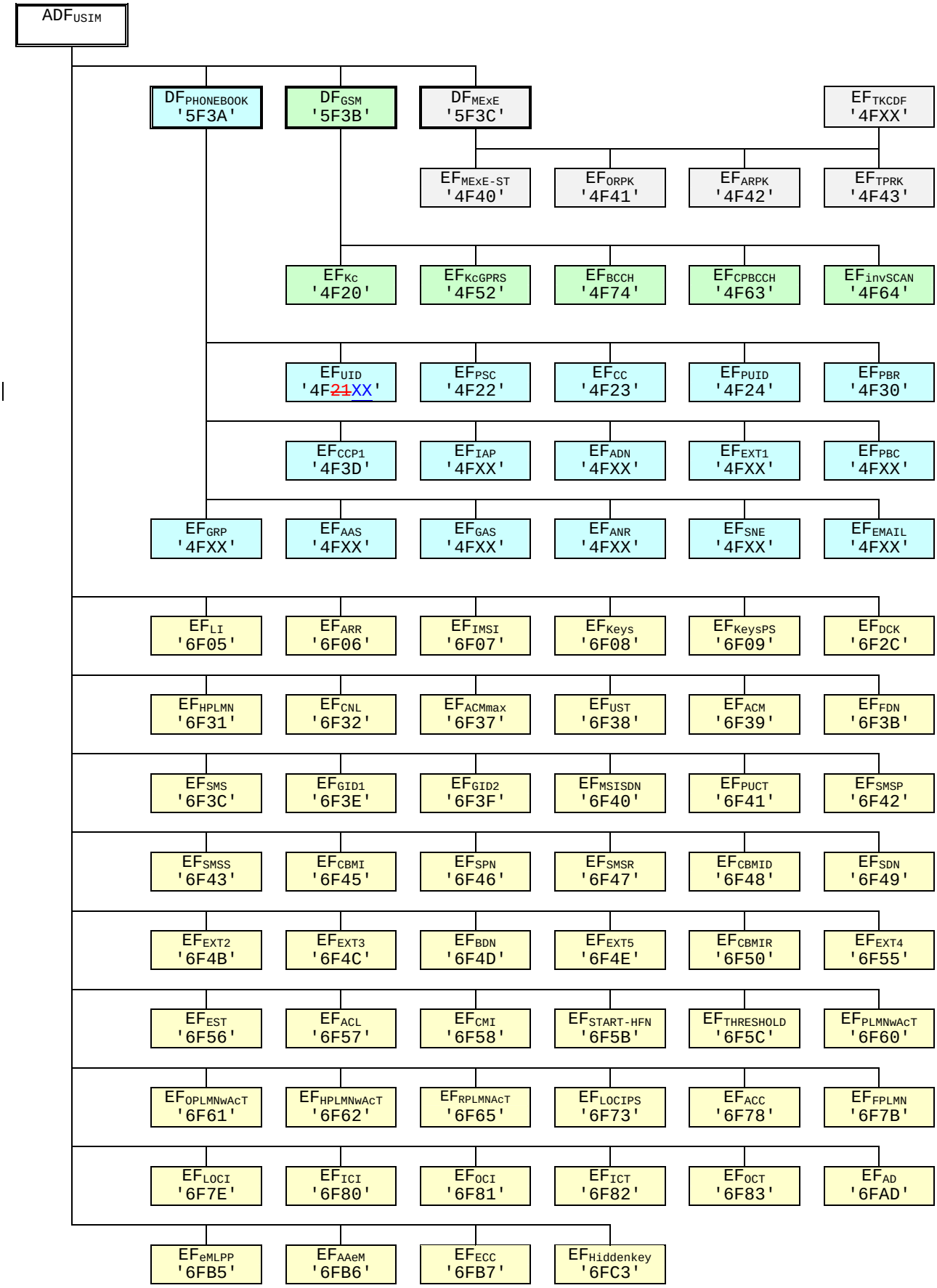


Figure 4.2: File identifiers and directory structures of USIM

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

Annex A (informative): EF changes via Data Download or USAT applications

This annex defines if changing the content of an EF by the network (e.g. by sending an SMS), or by a USAT Application, is advisable. Updating of certain EFs "over the air" such as EF_{ACC} could result in unpredictable behaviour of the UE; these are marked "Caution" in the table below. Certain EFs are marked "No"; under no circumstances should "over the air" changes of these EFs be considered.

File identification	Description	Change advised
'2F00'	Application directory	
'2F05'	Preferred languages	Yes
'2F06'	Access rule reference	
'2FE2'	ICC identification	No
'4F20'	Image data	Yes
'4FXX'	Image Instance data Files	Yes
'4F~~21~~xx'	Unique identifier	Yes
'4F22'	Phone book synchronisation counter	Yes
'4F23'	Change counter	Yes
'4F24'	Previous unique identifier	Yes
'4F30'	Phone book reference file	Yes
'4F3D'	Capability configuration parameters 1	Yes
'4F75'	CPBCCH Information	No
'4F76	Investigation Scan	Caution
'4FXX'	Additional number alpha string	Yes
'4FXX'	Additional number	Yes
'4FXX'	Second name entry	Yes
'4FXX'	Grouping information alpha string	Yes
'4FXX'	Phone book control	Yes
'4FXX'	E-mail addresses	Yes
'4FXX'	Index administration phone book	Yes
'4FXX'	Extension 1	Yes
'4FXX'	Abbreviated dialling numbers	Yes
'4FXX'	Grouping file	Yes
'6F05'	Language indication	Yes
'6F07'	IMSI	Caution (Note 1)
'6F08'	Ciphering and integrity keys	No
'6F09'	Ciphering and integrity keys for packet switched domain	No
'6F20'	Ciphering key Kc	No
'6F2C'	De-personalization Control Keys	Caution
'6F31'	HPLMN search period	Caution
'6F32'	Co-operative network list	Caution
'6F37'	ACM maximum value	Yes
'6F38'	USIM service table	Caution
'6F39'	Accumulated call meter	Yes
'6F3B'	Fixed dialling numbers	Yes
'6F3C'	Short messages	Yes
'6F3D'	Capability configuration parameters	Yes
'6F3E'	Group identifier level 1	Yes
'6F3F'	Group identifier level 2	Yes

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

If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

File Identification	Description	Value
'2F00'	Application directory	Card issuer/operator dependant
'2F05'	Preferred languages	'FF…FF'
'2F06'	Access rule reference	Card issuer/operator dependant
'2FE2'	ICC identification	operator dependant
'4F20'	Image data	'00FF...FF'
'4FXX'	Image instance data files	'FF…FF'
'4F~~21~~xx'	Unique identifier	'0000'
'4F22'	Phone book synchronisation counter	'00000000'
'4F23'	Change counter	'0000'
'4F24'	Previous unique identifier	'0000'
'4F30'	Phone book reference file	Operator dependant
'4F3D'	Capability configuration parameters 1	'FF…FF'
'4F63'	CPBCCH Information	'FF..FF'
'4F64'	Investigation PLMN scan	'00'
'4FXX'	E-mail addresses	'FF…FF'
'4FXX'	Additional number alpha string	'FF…FF'
'4FXX'	Second name entry	'FF…FF'
'4FXX'	Abbreviated dialling numbers	'FF...FF'
'4FXX'	Grouping file	'00…00'
'4FXX'	Grouping information alpha string	'FF…FF'
'4FXX'	Phone book control	'0000'
'4FXX'	Index administration phone book	'FF…FF'
'4FXX'	Additional number	'FF…FF'
'4FXX'	Extension 1	'00FF...FF'
'6F05'	Language indication	'FF…FF'
'6F07'	IMSI	Operator dependant
'6F08'	Ciphering and integrity keys	'07FF…FF'
'6F09'	Ciphering and integrity keys for packet switched domain	'07FF…FF'
'6F20'	Ciphering key Kc	'FF...FF07'
'6F2C'	De-personalization control keys	'FF…FF'
'6F31'	HPLMN search period	'FF'
'6F32'	Co-operative network list	'FF…FF'
'6F37'	ACM maximum value	'000000' (see note 1)
'6F38'	USIM service table	Operator dependant
'6F39'	Accumulated call meter	'000000'
'6F3B'	Fixed dialling numbers	'FF...FF'
'6F3C'	Short messages	'00FF...FF'
'6F3E'	Group identifier level 1	Operator dependant

3GPP TSG-T3 (USIM) Meeting #16
Seoul, SK, 13-15 November 2000

Document T3-000621
supersedes Tdoc T3-000600

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**	**058**	Current Version:	V3.3.0

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

For submission to:	TSG-T #10	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: *(at least one should be marked with an X)* (U)SIM [X] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T3 **Date:** 15/11/2000

Subject: correction of the phonebook example

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 4	

Reason for change:
Some mistakes lie within the phonebook example in annex G :
- GRP files are linked 1:1 with ADN, therefore their file-ID should be present in EF(PBR), after the 'D8' tag.
– The EXT1 file referred to from Rec2 of PBR has a file-id equal to '4F25'

Clauses affected: 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.

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 $DF_{PHONEBOOK}$

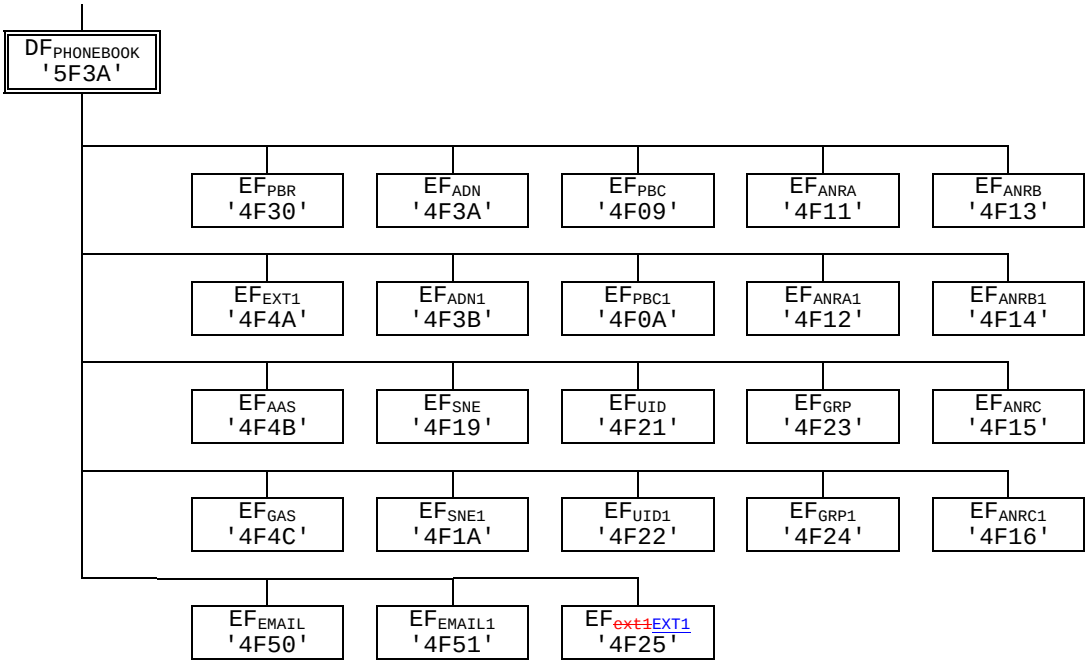


Table G.2: Contents of EF_{PBR}

Rec 1	Tag'D8'	L='226'	Tag'C0'	L='03'	'4F3A'	'01'	Tag'C5'	L='03'	'4F09'	'02'	Tag'C6'	L='02'	'4F23'	
	Tag'C4'	L='02'	'4F11'	Tag'C4'										
	L='02'	'4F13'	Tag'C4'	L='02'	'4F15'	Tag'C3'	L='02'	'4F19'	Tag'C9'	L='02'	'4F21'	Tag'CA'	L='02'	'4F50'
	Tag'DA'	L='0C'	Tag'C2'	L='02'	'4F4A'	Tag'C7'	L='02'	'4F4B'	Tag'C8'	L='02'	'4F4C'	'FF'		
Rec 2	Tag'D8'	L='204'	Tag'C0'	L='02'	'4F3B'	Tag'C5'	L='02'	'4F0A'	Tag'C6'	L='02'	'4F24'			
	Tag'C4'	L='02'	'4F12'	Tag'C4'	L='02'	'4F14'								
	Tag'C4'	L='02'	'4F16'	Tag'C3'	L='02'	'4F1A'	Tag'C9'	L='02'	'4F22'	Tag'CA'	L='02'	'4F51'	Tag'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 '4F4A25'	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													

3GPP TSG-T3 Meeting #16
Seoul, Korea, 13-15 November 2000

Tdoc T3-000625

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **059** ⌘ rev ⌘ Current version: **3.3.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Alignments with 3G TS 33.102 V 3.6.0
Source:	⌘	T3
Work item code:	⌘	***Date:*** ⌘ 13.11.00
Category:	⌘	**F** ***Release:*** ⌘ R99

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

Use one of the following releases:

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

Reason for change:	⌘	Some corrections to 3G TS 33.102 that were approved by SA#9 require alignment of 3G TS 31.102
Summary of change:	⌘	In clauses 6.2 and 7.1.1.1 a new function f5* is introduced to allow a modified computation of the anonymity key AK in re-synchronisation procedures. In clause 7.1.1.1 the length of the list of the last used sequence numbers is reduced to 32. In clause 7.1.1 the wording is changed to mention "VLR/SGSN" instead of "MSC/VLR or SGSN" Annex C (which actually was a copy of Annex C.2 of TS 33.102) is deleted. Accordingly, the reference in clause 7.1.1.1 is changed to TS 33.102
Consequences if not approved:	⌘	Inconsistencies between TS 31.102 and TS 33.102

Clauses affected:	⌘	6.2, 7.1.1, 7.1.1.1, Annex C
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

6.2 Cryptographic Functions

The names and parameters of the cryptographic functions supported by the USIM are defined in 3G TS 33.102 [13]. These are:

- f1: a message authentication function for network authentication used to compute XMAC;
- f1*: a message authentication function for support to re-synchronisation with the property that no valuable information can be inferred from the function values of f1* about those of f1, ... , f5, f5* and vice versa;
- f2: a message authentication function for user authentication used to compute SRES;
- f3: a key generating function to compute the cipher key CK;
- f4: a key generating function to compute the integrity key IK;
- f5: a key generating function to compute the anonymity key AK (optional);
- f5*: a key generating function to compute AK in re-synchronisation procedures with the property that no valuable information can be inferred from the function values of f5* about those of f1, f1*, f2, ... , f5 and vice versa.

These cryptographic functions may exist either discretely or combined within the USIM.

7 USIM Commands

7.1 AUTHENTICATE

7.1.1 Command description

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

The function is related to a particular USIM and shall not be executable unless the USIM or any sub-directory has been selected as the Current Directory and a successful PIN verification procedure has been performed (see clause 5).

The function can be used in two different contexts:

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

7.1.1.1 3G security context

The USIM first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ 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~~ 32 sequence numbers generated. A possible verification method is described in ~~annex C~~TS 33.102 [13].

NOTE: This implies that the USIM has to keep a list of the last used sequence numbers and the length of the list is at least ~~50~~ 32 entries.

If the USIM detects the sequence numbers to be invalid, this is considered as a synchronisation failure and the USIM abandons the function. In this case the command response is AUTS, where:
AUTS = Conc(SQN_{MS}) || MACS;
Conc(SQN_{MS}) = SQN_{MS} ⊕ $f5^*_K$(~~MACS || 0...0~~RAND) is the concealed value of the counter SQN_{MS} in the USIM; and.
MACS = $f1^*_K$(SQN_{MS} || RAND || AMF) where:
RAND is the random value received in the current user authentication request;
the AMF assumes a dummy value of all zeroes so that it does not need to be transmitted in clear in the resynchronisation message.

If the sequence number is considered in the correct range, the USIM computes RES = $f2_K$ (RAND), the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND) and includes these in the command response. Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND.

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

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

Input:

- RAND, AUTN (AUTN := SQN ⊕ 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 (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 50 entries.

3GPP TSG-T3 (USIM) Meeting #16
Seoul, SK, 13-15 November 2000

***Document* T3-000595**
Supersedes Tdoc T3-000542

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	062	Current Version:	V3.3.0

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

For submission to:	TSG-T #10	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: *(at least one should be marked with an X)* (U)SIM [X] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: T3 **Date:** 15/11/2000

Subject: phonebook correction on CCPs –solution 2

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 4	

Reason for change:
The use of the CCPs need to be clarified. It is proposed to have a simple approach :
- CCP1 is a file of the phonebook, and referred to from ADN and ANR, using a type 3 link
– CCP2 is a file under the USIM ADF, indicating the Capability/Configuration of a number within the FDN, SDN, BDN, MSISDN, ICI, OCI
– ECCP is a file under the DF TELECOM which may be provided when a SIM application is present on the UICC
Furthermore, the EF(CCP1) must be corrected in order to be able to store a 3G CCP.

Clauses affected: 4.4.2.1, 4.4.2.3, 4.4.2.9, 4.4.2.11, 4.5.3, 4.6.3, Annexes A, D, E

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.

4.4.2.1 EF_{PBR} (Phone Book Reference file)

[...]

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

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

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

Table 4.3: Presence of files as type

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

4.4.2.3 EF_{ADN} (Abbreviated dialling numbers)

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

Identifier: '4F3A	Structure: linear fixed	Conditional (see Note)
SFI: 'XX'		
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

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

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

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

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

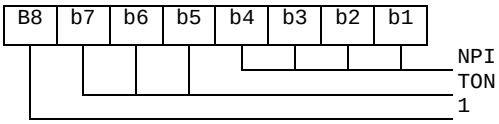
- Length of BCD number/SSC contents.
  Contents:
  - this byte gives the number of bytes of the following two data items containing actual BCD number/SSC information. This means that the maximum value is 11, even when the actual ADN/SSC information length is greater than 11. When an ADN/SSC has extension,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

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

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

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

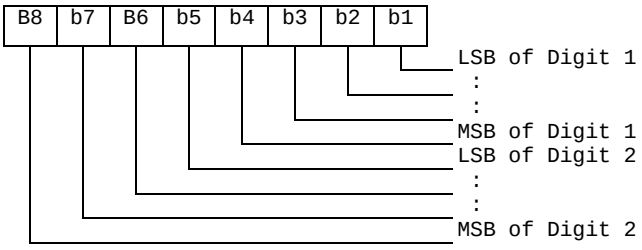
NOTE 2: If a dialling number is absent, no TON/NPI byte is transmitted over the radio interface (see 3G TS 24.008 [9]). Accordingly, the ME should not interpret the value 'FF' and not send it over the radio interface.



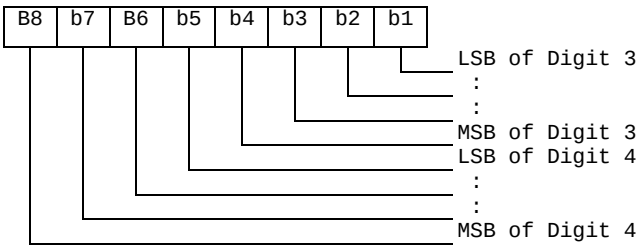
- Dialling Number/SSC String
  Contents:
  - up to 20 digits of the telephone number and/or SSC information.

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

Byte X+3



Byte X+4:



etc.

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

  Coding:
  - binary.

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: 'XX'		
Record length: 12 or 14 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/Configuration1 Identifier	M	1 byte
13	ADN file SFI	C	1 byte
14	ADN file Record Identifier	C	1 byte

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

- Additional Number Identifier

  Content:

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

  Coding:

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

- Additional number

  Content:

  - additional phone number linked to the phone book entry.

  Coding:

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

- Capability/Configuration1 Identifier.

  Contents:

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

  Coding:

  - binary.

- ADN file SFI.

  Content:

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: '4F~~3D~~XX'	Structure: linear fixed	Optional
SFI: 'XX'		
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 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.~~

- unused bytes are filled with 'FF'

4.5.3 EF_{ECCP} (Extended Capability Configuration Parameter)

In case of a present GSM application on the UICC the first EF_{CCP1} (i.e. reflected by the first record in EF_{PBR}) of the $DF_{PHONEBOOK}$ is mapped (with an identifier equal to '6F4F') to $DF_{TELECOM}$ to ensure backwards compatibility. There shall not be any EF_{CCP} (with a file-id of '6F3D') under $DF_{TELECOM}$ because otherwise a GSM terminal could create inconsistencies within the phonebook.

4.6.3 EF_{CCP} (Capability Configuration Parameters)

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

Identifier: '4F3D'	Structure: linear fixed	Optional
SFI: optional		
Record length: 14 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

- Bearer capability information element

  Contents and Coding:

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

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

Annex A (informative): EF changes via Data Download or USAT applications

This annex defines if changing the content of an EF by the network (e.g. by sending an SMS), or by a USAT Application, is advisable. Updating of certain EFs "over the air" such as EF_{ACC} could result in unpredictable behaviour of the UE; these are marked "Caution" in the table below. Certain EFs are marked "No"; under no circumstances should "over the air" changes of these EFs be considered.

File identification	Description	Change advised
'2F00'	Application directory	
'2F05'	Preferred languages	Yes
'2F06'	Access rule reference	
'2FE2'	ICC identification	No
'4F20'	Image data	Yes
'4FXX'	Image Instance data Files	Yes
'4F21'	Unique identifier	Yes
'4F22'	Phone book synchronisation counter	Yes
'4F23'	Change counter	Yes
'4F24'	Previous unique identifier	Yes
'4F30'	Phone book reference file	Yes
'4F~~3D~~XX'	Capability configuration parameters 1	Yes
'4F75'	CPBCCH Information	No
'4F76	Investigation Scan	Caution
'4FXX'	Additional number alpha string	Yes
'4FXX'	Additional number	Yes
'4FXX'	Second name entry	Yes
'4FXX'	Grouping information alpha string	Yes
'4FXX'	Phone book control	Yes
'4FXX'	E-mail addresses	Yes
'4FXX'	Index administration phone book	Yes
'4FXX'	Extension 1	Yes
'4FXX'	Abbreviated dialling numbers	Yes
'4FXX'	Grouping file	Yes
'6F05'	Language indication	Yes
'6F07'	IMSI	Caution (Note 1)
'6F08'	Ciphering and integrity keys	No
'6F09'	Ciphering and integrity keys for packet switched domain	No
'6F20'	Ciphering key Kc	No
'6F2C'	De-personalization Control Keys	Caution
'6F31'	HPLMN search period	Caution
'6F32'	Co-operative network list	Caution
'6F37'	ACM maximum value	Yes
'6F38'	USIM service table	Caution
'6F39'	Accumulated call meter	Yes

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 'CA' EF_{EMAIL} data object 'CB' EF_{CCP1} data object	Phone Book Reference File (EF_{PBR})
'DB'	Successful 3G authentication	Response to AUTHENTICATE
'DC'	Synchronisation failure	Response to AUTHENTICATE
'DD'	Access Point Name	APN Control List (EF_{ACL})

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

If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

File Identification	Description	Value
'2F00'	Application directory	Card issuer/operator dependant
'2F05'	Preferred languages	'FF…FF'
'2F06'	Access rule reference	Card issuer/operator dependant
'2FE2'	ICC identification	operator dependant
'4F20'	Image data	'00FF...FF'
'4FXX'	Image instance data files	'FF…FF'
'4F21'	Unique identifier	'0000'
'4F22'	Phone book synchronisation counter	'00000000'
'4F23'	Change counter	'0000'
'4F24'	Previous unique identifier	'0000'
'4F30'	Phone book reference file	Operator dependant
'4F~~3D~~XX'	Capability configuration parameters 1	'FF…FF'
'4F63'	CPBCCH Information	'FF..FF'
'4F64'	Investigation PLMN scan	'00'
'4FXX'	E-mail addresses	'FF…FF'
'4FXX'	Additional number alpha string	'FF…FF'
'4FXX'	Second name entry	'FF…FF'
'4FXX'	Abbreviated dialling numbers	'FF...FF'
'4FXX'	Grouping file	'00…00'
'4FXX'	Grouping information alpha string	'FF…FF'
'4FXX'	Phone book control	'0000'
'4FXX'	Index administration phone book	'FF…FF'
'4FXX'	Additional number	'FF…FF'
'4FXX'	Extension 1	'00FF...FF'
'6F05'	Language indication	'FF…FF'
'6F07'	IMSI	Operator dependant
'6F08'	Ciphering and integrity keys	'07FF…FF'
'6F09'	Ciphering and integrity keys for packet switched domain	'07FF…FF'
'6F20'	Ciphering key Kc	'FF...FF07'
'6F2C'	De-personalization control keys	'FF…FF'
'6F31'	HPLMN search period	'FF'
'6F32'	Co-operative network list	'FF…FF'
'6F37'	ACM maximum value	'000000' (see note 1)
'6F38'	USIM service table	Operator dependant
'6F39'	Accumulated call meter	'000000'
'6F3B'	Fixed dialling numbers	'FF...FF'