3GPP TSG-T (Terminals) Meeting #12
Stockholm, Sweden, 13 - 15 June 2001

Tdoc TP-010107

Source: T3

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

Document for: Approval

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

T3 Doc	Spec	CR	Rv	Rel	Subject
T3-010327	31.102	079		R99	Alignment of Status Words for AUTHENTICATE with TS 102 221
T3-010328	31.102	080		rel-4	Alignment of Status Words for AUTHENTICATE with TS 102 221
T3-010356	31.102	081		R99	Correction of EF(ECC) (note: R99 only)
T3-010385	31.102	082		rel-4	Addition of Operators Preferences file for GPRS service usage
T3-010390	31.102	083		R99	Correction to EF(HPLMNwACT) access condition
T3-010391	31.102	084		rel-4	Correction to EF(HPLMNwACT) access condition
T3-010412	31.102	085	1	R99	General corrections
T3-010387	31.102	086		rel-4	General corrections
T3-010426	31.102	087	1	R99	Clarification of the Authenticate command description
T3-010404	31.102	088		R99	Clarification of the type 3 links of the phonebook
T3-010405	31.102	089		rel-4	Clarification of the type 3 links of the phonebook
T3-010406	31.102	090		R99	Correction of compact Edge files
T3-010437	31.102	091		R99	Clarification of OCT/ICT files
T3-010438	31.102	092		rel-4	Clarification of OCT/ICT files
T3-010439	31.102	093		rel-4	Clarification of the Authenticate command description
T3-010440	31.102	094		rel-4	Correction of compact Edge files
T3-010450	31.102	095		rel-4	New implementation of SPN to align with SA1 specifications

3GPP T3 meeting #19
St. John, 8 - 11 May, 2001

Tdoc T3-010327
(revised from Tdoc T3-0103285)

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **079** ⌘ rev ⌘ Current version: **3.5.0** ⌘

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

Title:	⌘	Correction of status words for AUTHENTICATE
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	2001-05-09
Category:	⌘	**F**
Release:	⌘	*R99 (Release 1999)*

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 status words currently specified are not completely in line with the status word definitions in ETS 102 221.
Summary of change:	⌘	This CR aligns the status word definitions with the latest version of ETS 102 221. The status word list of ETS 102 221 v3.2.0 is replacing the existent status word list and has been expanded by the following status word: '98 64'
Consequences if not approved:	⌘	Potential inconsistencies in implementations, depending on the specification being used.

Clauses affected:	⌘	7.3.2		
Other specs Affected:	⌘	[ ] Other core specifications [X] Test specifications [ ] O&M Specifications	⌘	31.121
Other comments:	⌘			

7.3.2 Status Words of the Commands

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

Commands and status words

AUTHENTICATE	
	90 00
	91 XX
*	9F XX
	61XX#
	93 00
	92 0X
*	65 81
	94 00
	94 02
	94 04
*	94 08
	98 02
*	69 82
	98 08
	98 10
	98 40
	98 50
*	98 62
*	98 64
*	67 XX
*	6B XX
	6D XX
*	6E XX
*	6F XX
	62 81
	62 83
	62 82
	62 84
	62 00
	63 CX
	69 81
*	69 84
*	69 85
	69 86
	6A 81
	6A 82
	6A 83
	6A 84
	6A 85
*	6A 86
	6A 87
*	6A 88
	6C XX

Status Words	AUTHENTICATE
90 00	*
91 XX	*
93 00	
98 50	
98 62	*
98 64	*
62 00	*
62 81	
62 82	
62 83	
63 CX	
64 00	*
65 00	*
65 81	*
67 00	*
67 XX – (see note)	*
68 00	*
68 81	*
68 82	*
69 81	
69 82	*
69 83	
69 84	*
69 85	*
69 86	
6A 80	
6A 81	*
6A 82	
6A 83	
6A 86	*
6A 87	
6A 88	*
6B 00	*
6E 00	*
6F 00	*
6F XX – (see note)	*
NOTE: Except SW2 = '00'.	

3GPP T3 meeting #19
St. John, 8 - 11 May, 2001

Tdoc T3-010328

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **080** ⌘ rev ⌘ Current version: **4.0.0** ⌘

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

Title:	⌘	Correction of status words for AUTHENTICATE
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	2001-05-09
Category:	⌘	**F**
Release:	⌘	*REL-4*

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 status words currently specified are not completely in line with the status word definitions in ETS 102 221.
Summary of change:	⌘	This CR aligns the status word definitions with the latest version of ETS 102 221. The status word list of ETS 102 221 v4.1.0 is replacing the existent status word list and has been expanded by the following status word: '98 64'
Consequences if not approved:	⌘	Potential inconsistencies in implementations, depending on the specification being used.

Clauses affected:	⌘	7.3.2		
Other specs Affected:	⌘	[ ] Other core specifications [X] Test specifications [ ] O&M Specifications	⌘	31.121
Other comments:	⌘			

7.3.2 Status Words of the Commands

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

Commands and status words

AUTHENTICATE	
	90 00
	91 XX
*	9F XX
	61XX#
	93 00
	92 0X
*	65 81
	94 00
	94 02
	94 04
*	94 08
	98 02
*	69 82
	98 08
	98 10
	98 40
	98 50
*	98 62
*	98 64
*	67 XX
*	6B XX
	6D XX
*	6E XX
*	6F XX
	62 81
	62 83
	62 82
	62 84
	62 00
	63 CX
	69 81
*	69 84
*	69 85
	69 86
	6A 81
	6A 82
	6A 83
	6A 84
	6A 85
*	6A 86
	6A 87
*	6A 88
	6C XX

Status Words	AUTHENTICATE
90 00	*
91 XX	*
93 00	
98 50	
98 62	*
98 64	*
62 00	*
62 81	
62 82	
62 83	
63 CX	
64 00	*
65 00	*
65 81	*
67 00	*
67 XX – (see note)	*
68 00	*
68 81	*
68 82	*
69 81	
69 82	*
69 83	
69 84	*
69 85	*
69 86	
6A 80	
6A 81	*
6A 82	
6A 83	
6A 86	*
6A 87	
6A 88	*
6B 00	*
6E 00	*
6F 00	*
6F XX – (see note)	*
NOTE: Except SW2 = '00'.	

3GPP T3 meeting #19
St. John, 8 - 11 May, 2001

Tdoc T3-010356
(revised version of T3-010342)

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **081** ⌘ rev ⌘ Current version: **3.5.0** ⌘

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

Title:	⌘	Correction of EF_ECC (note: R99 only)
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	2001-05-09
Category:	⌘	**F**
Release:	⌘	*R99 (Release 1999)*

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:	⌘	CR071 introduced a change to the EF_ECC based on Rel-4 of 24.008. In R99 of 24.008 these service categories are not defined, thus they cannot be referred to in 31.102 R99.
Summary of change:	⌘	The Emergency Service Category bits are set to RFU and a corresponding note, defining the behaviour of the ME, is added.
Consequences if not approved:	⌘	31.102 R99 is not compliant to 24.008 R99.

Clauses affected:	⌘	4.2.21		
Other specs Affected:	⌘	[ ] Other core specifications [X] Test specifications [ ] O&M Specifications	⌘	31.121
Other comments:	⌘			

4.2.21 EF_{ECC} (Emergency Call Codes)

This EF contains emergency call codes.

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

Access Conditions:

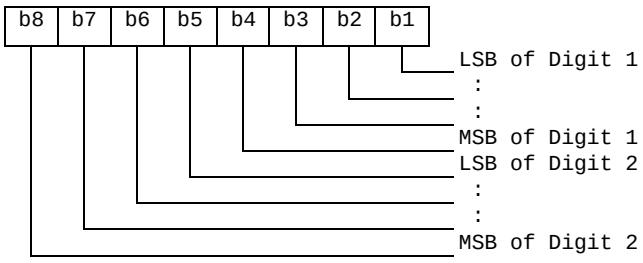
READ	ALW
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

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

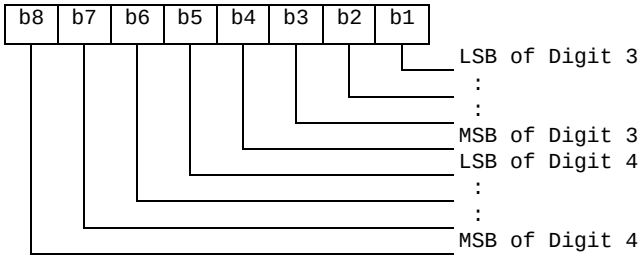
- Emergency Call Code.
  Contents:
  - Emergency Call Code.

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

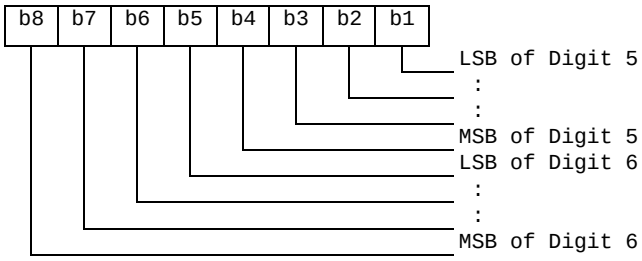
Byte 1:



Byte 2:



Byte 3:



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

  Or
  - one of the UCS2 coded options as defined in the annex of 3G TS 31.101 [11].
- Emergency Service Category.
  Contents:
  ~~Information to be sent to the network indicating the category of the emergency call.~~
  In future versions this information will be used to be sent to the network indicating the category of the emergency call. In the present release this feature is not defined.

  Coding:
  ~~Coding according to 24.008 [9].~~

  The coding is not defined in R99 and therefore this byte is set to RFU. A R99 terminal shall not interpret the Emergency Service Category byte.

3GPP T3 (USIM) Meeting #19, 8-11 May 01
St John, USVI

Tdoc T3-010385
(revised version of T3-010244)

CR-Form-v3

CHANGE REQUEST

⌘ **TS 31.102** **CR** **082** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Addition of Operators Preferences file for GPRS service usage
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	10/05/01
Category:	⌘	B
Release:	⌘	*REL-4*

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 addition of a GPRS configuration file that defines the default settings for GPRS service when an application does not fully specify the GPRS settings.
Summary of change:	⌘	At present there are no defined settings of key parameters for GPRS connections. Therefore this field being optional has one change in the USIM service table for the addition of the optional feature. Secondly the addition of the GPRS Operator Preferences TLV encoded transparent file, describing the parameters. Finally the addition of the procedure
Consequences if not approved:	⌘	Indeterminate behaviour of GPRS services dependant on the Terminal manufacturer.

Clauses affected:	⌘	4.2.8, 4.4, 4.7, 5.3.2x, Annex A, Annex D, Annex E
Other specs Affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

4.2.8 EF_{UST} (USIM Service Table)

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

Identifier: '6F38'	Structure: transparent	Mandatory
SFI: '04'		
File size: X bytes, X >= 1	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Services n°1 to n°8	M	1 byte
2	Services n°9 to n°16	O	1 byte
3	Services n°17 to n°24	O	1 byte
4	Services n°25 to n°32	O	1 byte
etc.			
X	Services n°(8X-7) to n°(8X)	O	1 byte

-Services

Contents:

Service n°1 : Local Phone Book
Service n°2 : Fixed Dialling Numbers (FDN)
Service n°3 : Extension 2
Service n°4 : Service Dialling Numbers (SDN)
Service n°5 : Extension3
Service n°6 : Barred Dialling Numbers (BDN)
Service n°7 : Extension4
Service n°8 : Outgoing Call Information (OCI and OCT)
Service n°9 : Incoming Call Information (ICI and ICT)
Service n°10: Short Message Storage (SMS)
Service n°11: Short Message Status Reports (SMSR)
Service n°12: Short Message Service Parameters (SMSP)
Service n°13: Advice of Charge (AoC)
Service n°14: Capability Configuration Parameters (CCP)
Service n°15: Cell Broadcast Message Identifier
Service n°16: Cell Broadcast Message Identifier Ranges
Service n°17: Group Identifier Level 1
Service n°18: Group Identifier Level 2
Service n°19: Service Provider Name
Service n°20: User controlled PLMN selector with Access Technology
Service n°21: MSISDN
Service n°22: Image (IMG)
Service n°23: Not used (reserved for SoLSA)
Service n°24: Enhanced Multi-Level Precedence and Pre-emption Service
Service n°25: Automatic Answer for Emlpp
Service n°26: RFU
Service n°27: GSM Access
Service n°28: Data download via SMS-PP
Service n°29: Data download via SMS-CB
Service n°30: Call Control by USIM
Service n°31: MO-SMS Control by USIM
Service n°32: RUN AT COMMAND command
Service n°33: Packet Switched Domain
Service n°34: Enabled Services Table
Service n°35: APN Control List (ACL)
Service n°36: Depersonalisation Control Keys
Service n°37: Co-operative Network List
Service n°38: GSM security context
Service n°39 CPBCCH Information
Service n°40 Investigation Scan
Service n°41 MExE
Service n°42 Operator controlled PLMN selector with Access Technology
Service n°43 HPLMN selector with Access Technology
Service n° XX GPRS Operator Preferences

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

Coding:

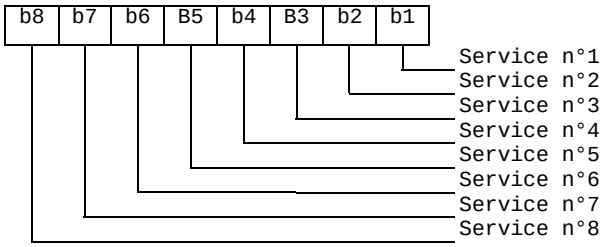
1 bit is used to code each service:

bit = 1: service available;

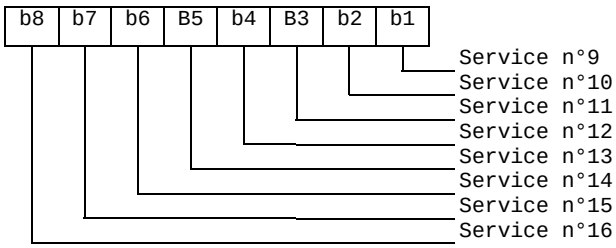
bit = 0: service not available.

- Service available means that the USIM has the capability to support the service and that the service is available for the user of the USIM unless the service is identified as "disabled" in EF_{EST}.
  Service not available means that the service shall not be used by the USIM user, even if the USIM has the capability to support the service.

First byte:



Second byte:



etc.

4.4.x $EF_{GPRSOperPrefs}$ (GPRS Operator Preferences)

This EF contains the Operators preferences for the use of the GPRS service.

Identifier: '6Fxx'	Structure: transparent	Optional
SFI :'xx'		
File size: X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 – X	TLV object(s) containing GPRS operator preferences information	M	

- $EF_{OperPrefs}$ Cell Information tags

Tag Value	**Tag Description**
'Ax'	GPRS operator preferences Tag
'80'	GPRS Class A Attachment preferences in Home PLMN tag
'81'	GPRS Class A Detachment preferences in Home PLMN tag
'82'	GPRS Class A Attachment preferences in Roaming PLMN tag
'83'	GPRS Class A Detachment preferences in Roaming PLMN tag

After the constructed 'Ax' Tag object the TLVs thereafter define preferences for the terminal settings for a particular Class of terminal. These preferences cannot be repeated i.e. the tag value cannot be repeated.

- GPRS Attachment Preferences for Class A in home PLMN TLV

Contents

This TLV defines the Operators Class A terminal GPRS Attachment Preferences when in the Home PLMN.

Coding

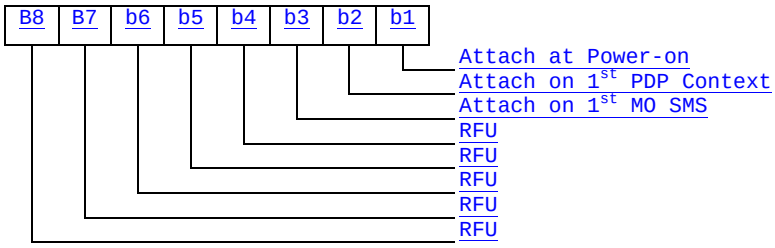
Description	**M/O**	**Length**
GPRS Class A Attachment Preferences in Home PLMN Tag	M	1
Length	M	1
Class A Attachment Terminal Preferences	M	1

- Class A Attachment Terminal Preferences

Contents

The operators GPRS Attachment Preferences in home PLMN for GPRS Class A terminal operation

Coding



- bit = 1: rule selected;
- bit = 0: rule not selected.

If bits b1 to b8 are not selected then this specifically means that the ME attachment rules take preference.

- GPRS Class A terminal Detachment Preferences in home PLMN TLV

Contents

This TLV details the Operator Preferences for GPRS detachment when in the Home PLMN

Coding

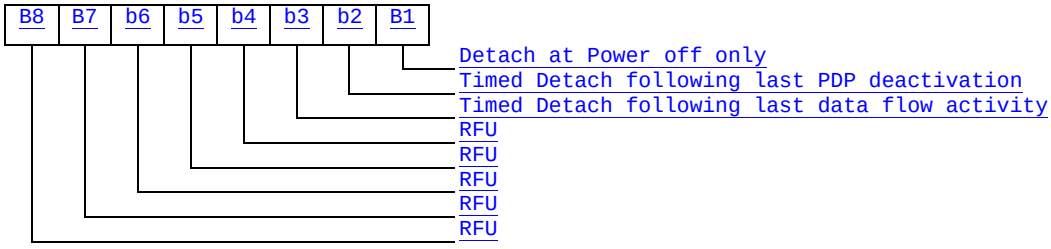
Description	**M/O**	**Length**
GPRS Detachment Class A Preferences in home PLMN Tag	M	1
Length	M	1
Terminal Detachment Preferences	M	1
Detachment Timer Value	M	2

-Terminal Detachment Preferences

Contents

The operators GPRS Detachment Preferences in home PLMN for GPRS Class A terminal operation

Coding



- bit = 1: activation rule selected;
- bit = 0: activation rule not selected.

If bit b1 is selected then bits b2 to b8 are ignored.

If bit b2 is selected bit b3 is ignored.

If bit b3 is selected bit b2 is ignored.

If bits b1 to b8 are not selected then this specifically means that the ME detachment rules take preference.

- Detachment Timer Value

Contents

The timer value for the Operator Preferences for timed GPRS detachment for Class A operation in home PLMN for use when bit b2 or b3 is set.

Coding

Value in minutes coded on two bytes: 0 to 65535 ('FFFF')

Value of '0000' means timer expires immediately.

Value of 'FFFF' means timer never expires.

- GPRS Class A Terminal Attachment Preferences in Roaming PLMN TLV

Contents

This TLV details the Operator Preferences for GPRS Attachment when in the Roaming PLMN

Coding

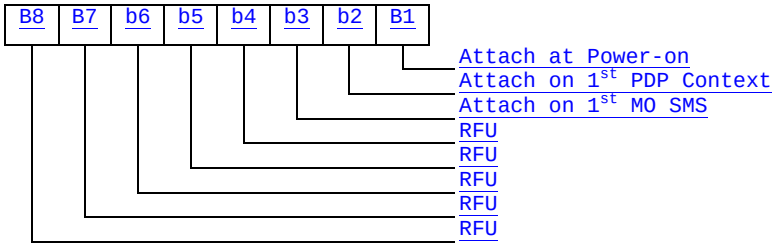
Description	**M/O**	**Length**
GPRS Class A Attachment Preferences in Roaming PLMN Tag	M	1
Length	M	1
Class A Attachment Terminal Preferences	M	1

- Class A Attachment Terminal Preferences

Contents

The operators GPRS Attachment Preferences in Roaming PLMN for GPRS Class A terminal operation

Coding



- bit = 1: rule selected;
- bit = 0: rule not selected.

If bits b1 to b8 are not selected then this specifically means that the ME attachment rules take preference.

- GPRS Class A Terminal Detachment Preferences in Roaming PLMN TLV

Contents

This TLV details the Operator Preferences for GPRS detachment when in the Roaming PLMN

Coding

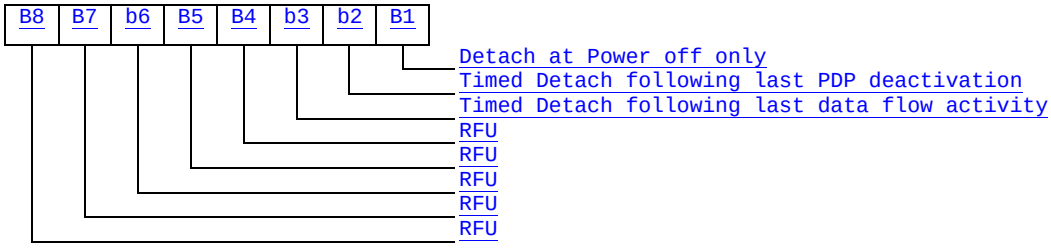
Description	M/O	Length
GPRS Detachment Class A Preferences in Roaming PLMN Tag	M	1
Length	M	1
Terminal Detachment Preferences	M	1
Detachment Timer Value	M	2

- Terminal Detachment Preferences

Contents

The operators GPRS Detachment Preferences in home PLMN for GPRS Class A terminal operation

Coding



- bit = 1: activation rule selected;
- bit = 0: activation rule not selected.

If bit b1 is selected then bits b2 to b8 are ignored.

If bit b2 is selected bit b3 is ignored.

If bit b3 is selected bit b2 is ignored.

If bits b1 to b8 are not selected then this specifically means that the ME detachment rules take preference.

- Detachment Timer Value

Contents

The timer value for the Operator preferences for timed GPRS detachment for Class A terminal operation in Roaming PLMN for use when either bit b2 or b3 is set.

Coding

Value in minutes coded on two bytes: 0 to 65535 (‘FFFF’)

Value of ‘0000’ means timer expires immediately.

Value of ‘FFFF’ means timer never expires.

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}.

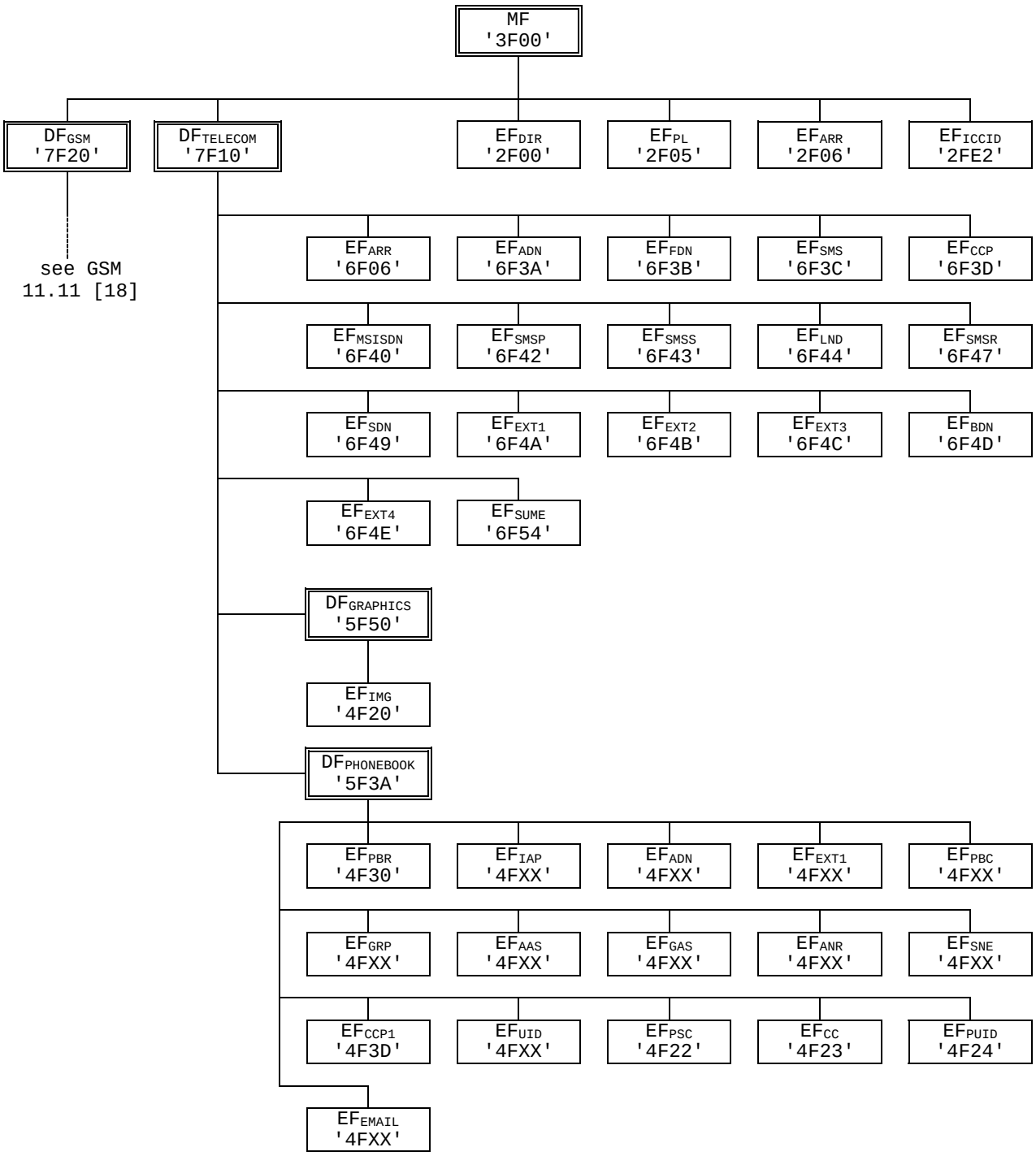
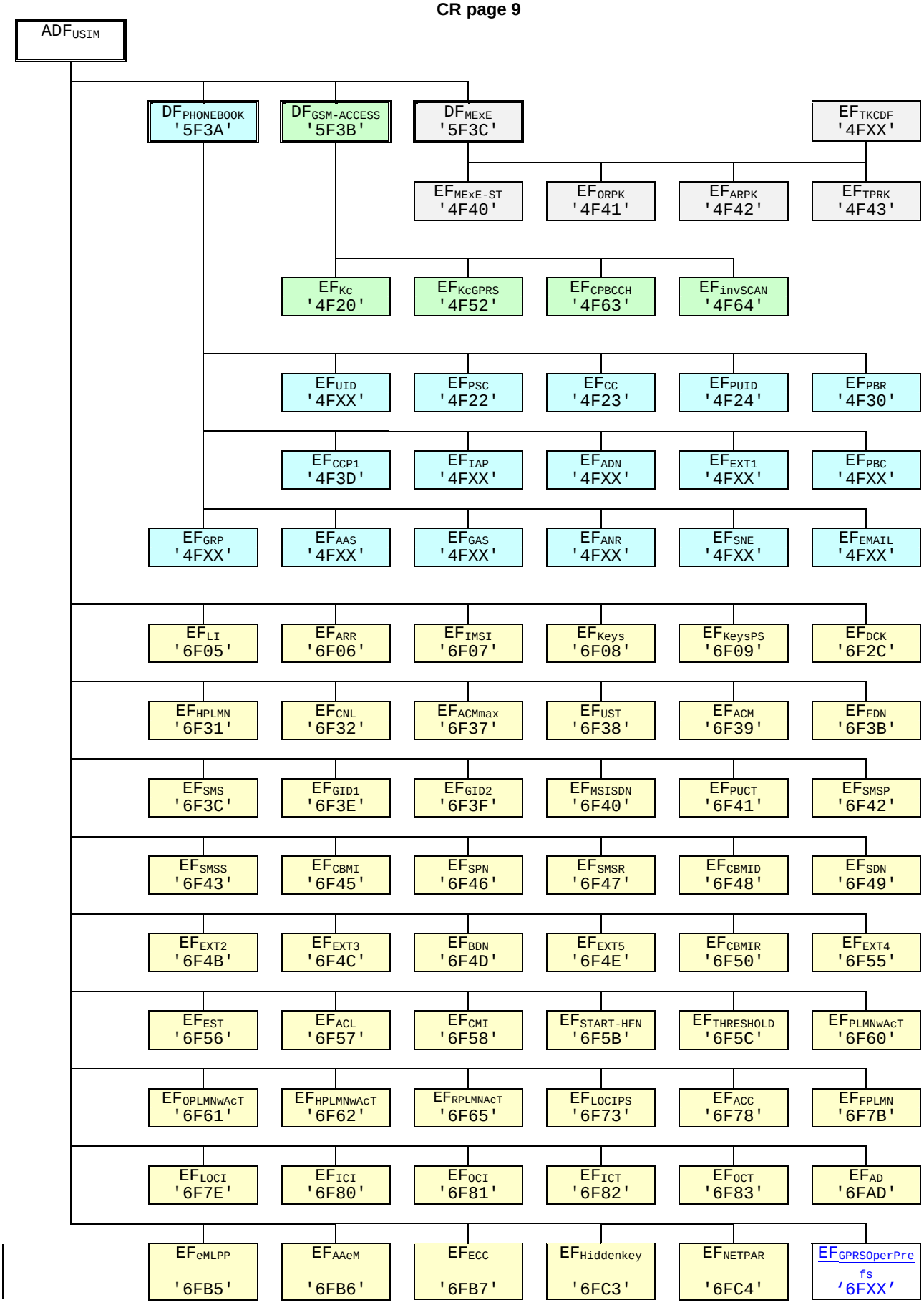


Figure 4.1: File identifiers and directory structures of UICC


ADF USIM
DF PHONEBOOK '5F3A'
DF GSM-ACCESS '5F3B'
DF MExE '5F3C'
EF TKCDF '4FXX'
EF MExE-ST '4F40'
EF ORPK '4F41'
EF ARPK '4F42'
EF TPRK '4F43'
EF Kc '4F20'
EF KcGPRS '4F52'
EF CPBCCH '4F63'
EF invSCAN '4F64'
EF UID '4FXX'
EF PSC '4F22'
EF CC '4F23'
EF PUID '4F24'
EF PBR '4F30'
EF CCP1 '4F3D'
EF IAP '4FXX'
EF ADN '4FXX'
EF EXT1 '4FXX'
EF PBC '4FXX'
EF GRP '4FXX'
EF AAS '4FXX'
EF GAS '4FXX'
EF ANR '4FXX'
EF SNE '4FXX'
EF EMAIL '4FXX'
EF LI '6F05'
EF ARR '6F06'
EF IMSI '6F07'
EF Keys '6F08'
EF KeysPS '6F09'
EF DCK '6F2C'
EF HPLMN '6F31'
EF CNL '6F32'
EF ACMmax '6F37'
EF UST '6F38'
EF ACM '6F39'
EF FDN '6F3B'
EF SMS '6F3C'
EF GID1 '6F3E'
EF GID2 '6F3F'
EF MSISDN '6F40'
EF PUCT '6F41'
EF SMSP '6F42'
EF SMSS '6F43'
EF CBMI '6F45'
EF SPN '6F46'
EF SMSR '6F47'
EF CBMID '6F48'
EF SDN '6F49'
EF EXT2 '6F4B'
EF EXT3 '6F4C'
EF BDN '6F4D'
EF EXT5 '6F4E'
EF CBMIR '6F50'
EF EXT4 '6F55'
EF EST '6F56'
EF ACL '6F57'
EF CMI '6F58'
EF START-HFN '6F5B'
EF THRESHOLD '6F5C'
EF PLMNwAcT '6F60'
EF OPLMNwAcT '6F61'
EF HPLMNwAcT '6F62'
EF RPLMNAcT '6F65'
EF LOCIPS '6F73'
EF ACC '6F78'
EF FPLMN '6F7B'
EF LOCI '6F7E'
EF ICI '6F80'
EF OCI '6F81'
EF ICT '6F82'
EF OCT '6F83'
EF AD '6FAD'
EF eMLPP '6FB5'
EF AAeM '6FB6'
EF ECC '6FB7'
EF Hiddenkey '6FC3'
EF NETPAR '6FC4'
EF GPRSOperPrefs '6FXX'

5.3.2x

Requirement: Service n° XX Present

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

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

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

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

Continued….

File identification	Description	Change advised
'6F40'	MSISDN storage	Yes
'6F41'	PUCT	Yes
'6F42'	SMS parameters	Yes
'6F43'	SMS status	Yes
'6F44'	Last number dialled	Yes
'6F45'	CBMI	Caution
'6F46'	Service provider name	Yes
'6F47'	Short message status reports	Yes
'6F48'	CBMID	Yes
'6F49'	Service Dialling Numbers	Yes
'6F4B'	Extension 2	Yes
'6F4C'	Extension 3	Yes
'6F4D'	Barred dialling numbers	Yes
'6F4E'	Extension 5	Yes
'6F4F'	Capability configuration parameters 2	Yes
'6F50'	CBMIR	Yes
'6F52'	GPRS Ciphering key KcGPRS	No
'6F54'	SetUp Menu Elements	Yes
'6F56'	Enabled services table	
'6F57'	Access point name control list	
'6F58'	Comparison method information	
'6F5B'	Initialisation value for Hyperframe number	Caution
'6F5C'	Maximum value of START	Yes
'6F60'	User controlled PLMN selector with Access Technology	No
'6F61'	Operator controlled PLMN selector with Access Technology	Caution
'6F62'	HPLMN selector with Access Technology	Caution
'6F63'	RPLMN last used Access Technology	Caution
'6F73'	Packet switched location information	Caution
'6F78'	Access control class	Caution
'6F7B'	Forbidden PLMNs	Caution
'6F7E'	Location information	No (Note 1)
'6F80'	Incoming call information	Yes
'6F81'	Outgoing call information	Yes
'6F82'	Incoming call timer	Yes
'6F83'	Outgoing call timer	Yes
'6FAD'	Administrative data	Caution
'6FB5'	Enhanced Multi Level Pre-emption and Priority	Yes
'6FB6'	Automatic Answer for eMLPP Service	Yes
'6FB7'	Emergency Call Codes	Caution
'6FC2'	Group identity	No
'6FC3'	Key for hidden phone book entries	
'6FC4'	Network Parameters	No
'6Fxx'	GPRS Operator Preferences	Caution

NOTE1: If EF_{IMSI} is changed, the UICC should issue REFRESH as defined in TS 31.111 and update EF_{LOCI} accordingly.

Annex D (informative): Tags defined in 31.102

Tag	Name of Data Element	Usage
'A0'	GSM cell information The following are encapsulated under 'A0': '80' GSM Camping Frequency data object '81' GSM Neighbour Frequency Information data object	Network Parameters (EF_{NETPAR})
'A1'	FDD cell information The following are encapsulated under 'A1': '80' FDD Intra Frequency data object '81' FDD Inter Frequency Information data object	Network Parameters (EF_{NETPAR})
'A2'	TDD cell information The following are encapsulated under 'A2': '80' TDD Intra Frequency data object '81' TDD Inter Frequency Information data object	Network Parameters (EF_{NETPAR})
'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})
'AX'	GPRS Operator Preferences: The following are encapsulated under 'AX': '80' GPRS Class A Attachment Preferences in Home PLMN data object '81' GPRS Class A Detachment Preferences in Home PLMN data object '82' GPRS Class A Attachment Preferences in Roaming PLMN data object '83' GPRS Class A Detachment Preferences in Roaming PLMN data object	

Annex E (informative):

Suggested contents of the EFs at pre-personalization
If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

File Identification	Description	Value
'2F00'	Application directory	Card issuer/operator dependant
'2F05'	Preferred languages	'FF…FF'
'2F06'	Access rule reference	Card issuer/operator dependant
'2FE2'	ICC identification	operator dependant
'4F20'	Image data	'00FF...FF'
'4FXX'	Image instance data files	'FF…FF'
'4FXX'	Unique identifier	'0000'
'4F22'	Phone book synchronisation counter	'00000000'
'4F23'	Change counter	'0000'
'4F24'	Previous unique identifier	'0000'
'4F30'	Phone book reference file	Operator dependant
'4FXX'	Capability configuration parameters 1	'FF…FF'
'4F63'	CPBCCH Information	'FF..FF'
'4F64'	Investigation PLMN scan	'00'
'4FXX'	E-mail addresses	'FF…FF'
'4FXX'	Additional number alpha string	'FF…FF'
'4FXX'	Second name entry	'FF…FF'
'4FXX'	Abbreviated dialling numbers	'FF...FF'
'4FXX'	Grouping file	'00…00'
'4FXX'	Grouping information alpha string	'FF…FF'
'4FXX'	Phone book control	'0000'
'4FXX'	Index administration phone book	'FF…FF'
'4FXX'	Additional number	'FF…FF'
'4FXX'	Extension 1	'00FF...FF'
'6F05'	Language indication	'FF…FF'
'6F07'	IMSI	Operator dependant
'6F08'	Ciphering and integrity keys	'07FF…FF'
'6F09'	Ciphering and integrity keys for packet switched domain	'07FF…FF'
'6F20'	Ciphering key Kc	'FF...FF07'
'6F2C'	De-personalization control keys	'FF…FF'
'6F31'	HPLMN search period	'FF'
'6F32'	Co-operative network list	'FF…FF'
'6F37'	ACM maximum value	'000000' (see note 1)
'6F38'	USIM service table	Operator dependant
'6F39'	Accumulated call meter	'000000'
'6F3B'	Fixed dialling numbers	'FF...FF'
'6F3C'	Short messages	'00FF...FF'
'6F3E'	Group identifier level 1	Operator dependant
'6F3F'	Group identifier level 2	Operator dependant
'6F40'	MSISDN storage	'FF...FF'
'6F41'	PUCT	'FFFFFF0000'
'6F42'	SMS parameters	'FF...FF'
'6F43'	SMS status	'FF...FF'
'6F45'	CBMI	'FF...FF'
'6F46'	Service provider name	Operator dependant
'6F47'	Short message status reports	'00FF…FF'
'6F48'	CBMID	'FF...FF'
'6F49'	Service Dialling Numbers	'FF...FF'
'6F4B'	Extension 2	'00FF...FF'
'6F4C'	Extension 3	'00FF...FF'

Continued....

File Identification	Description	Value
'6F4D'	Barred Dialling Numbers	'FF...FF'
'6F4E'	Extension 5	'00FF...FF'
'6F4F'	Capability configuration parameters 2	'FF...FF'
'6F50'	CBMIR	'FF...FF'
'6F52'	GPRS Ciphering key KcGPRS	'FF...FF07'
'6F54'	SetUp Menu Elements	Operator dependant
'6F55'	Extension 4	'FF...FF'
'6F56'	Enabled services table	Operator dependant
'6F57'	Access point name control list	'00FF…FF'
'6F58'	Comparison method information	'FF…FF'
'6F5B'	Initialisation value for Hyperframe number	'00…00'
'6F5C'	Maximum value of START	Operator dependant
'6F60'	User controlled PLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F61'	Operator controlled PLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F62'	HPLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F65'	RPLMN last used Access Technology	'0000'
'6F73'	Packet switched location information	'FFFFFFFF FFFFFF xxxxxx 0000 FF 01' (see note 2)
'6F78'	Access control class	Operator dependant
'6F7B'	Forbidden PLMNs	'FF...FF'
'6F7E	Location information	'FFFFFFFF xxxxxx 0000 FF 01' (see note 2)
'6F80'	Incoming call information	'FF…FF 000000 00 01FFFF'
'6F81'	Outgoing call information	'FF…FF 000000 01FFFF'
'6F82'	Incoming call timer	'000000'
'6F83'	Outgoing call timer	'000000'
'6FAD'	Administrative data	Operator dependant
'6FB5'	EMLPP	Operator dependant
'6FB6'	AaeM	'00'
'6FB7'	Emergency call codes	Operator dependant
'6FC2'	Group identity	'FFFFFFFF'
'6FC3'	Key for hidden phone book entries	'FF…FF'
‘6FC4'	Network Parameters	'FF…FF'
‘xxxx’	GPRS Operator Preferences	Operator dependant

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

NOTE 2: xxxxxx stands for any valid MCC and MNC, coded according to 3G TS 24.008 [9].

3GPP TSG-T3 Meeting #19
St. John, US VI, 8-11 May 2001

Tdoc T3-010390

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **083** ⌘ rev **-** ⌘ Current version: **3.5.0** ⌘

*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:	⌘	Correction of EF $HPLMN_{wAcT}$ Access Condition
Source:	⌘	T3
Work item code:	⌘	***Date:*** ⌘ 2001-05-11
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 Access Condition of the EF $HPLMN_{wAcT}$ update is currently set to PIN. As this EF is under Operator control, the Access Condition should be “ADM”
Summary of change:	⌘	Access Condition of the EF $HPLMN_{wAcT}$ is changed to “ADM”
Consequences if not approved:	⌘	The UPDATE of the EF HPLMNwACT is not under operator control.

Clauses affected:	⌘	4.2.54
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

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

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

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

Access Conditions:

READ	PIN
UPDATE	~~PIN~~ADM
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

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

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

3GPP TSG-T3 Meeting #19
St. John, US VI, 8-11 May 2001

Tdoc T3-010391

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **084** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

*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:	⌘	Correction of EF $HPLMN_{wAcT}$ Access Condition
Source:	⌘	T3
Work item code:	⌘	***Date:*** ⌘ 2001-05-11
Category:	⌘ **A**	***Release:*** ⌘ Rel-4

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 Access Condition of the EF $HPLMN_{wAcT}$ update is currently set to PIN. As this EF is under Operator control, the Access Condition should be “ADM”
Summary of change:	⌘	Access Condition of the EF $HPLMN_{wAcT}$ is changed to “ADM”
Consequences if not approved:	⌘	The UPDATE of the EF HPLMNwACT is not under operator control.

Clauses affected:	⌘	4.2.54
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

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

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

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

Access Conditions:

READ	PIN
UPDATE	~~PIN~~ADM
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

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

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

3GPP T3 (USIM) Meeting #19
St John, US VI, 8-11 May, 2001

Tdoc T3-010412
(revised version of T3-010386)

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **085 rev1** ⌘ rev **-** ⌘ Current version: **3.5.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	General Corrections
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11.05.2001
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:	⌘	
Summary of change:	⌘	
Consequences if not approved:	⌘	TS 31.102 will contain inconsistencies

Clauses affected:	⌘	4.4.2.1; 4.4.2.2; 5.3.2; 5.3.5; 6.4		
Other specs affected:	⌘	[ ] Other core specifications	⌘	
		[X] Test specifications		31.121
		[ ] O&M Specifications		
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 record identifier within a record.

Table 4.1: Phone Book Reference file Constructed Tags

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

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

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

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

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

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

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

4.4.2.2 EF_{IAP} (Index Administration Phone book)

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

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

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

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

Index administration file EF_{IAP} structure

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

Bytes	Description	M/O	Length
1	Record number of the first object indicated after Tag '~~Đ~~A9'	M	1 byte
2	Record number of the second object indicated after Tag '~~Đ~~A9'	M	1 byte
X	Record number of the x^{th} object indicated after Tag '~~Đ~~A9'	M	1 byte

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

5.3.2 Dialling numbers

Requirements:

- Service n°1 "available" for ADN located under the local phonebook
- Presence of EF_{ADN} in EF_{PBR} for ADN located under the global phonebook
- Presence of EF_{ANR} in EF_{PBR} for ANR.
- Service n°2 "available" for FDN.

- Service n°21 "available" for MSISDN.
- Service n°4 "available" for SDN.
- Service n°6 "available" for BDN.
- Service n°8 "available" for EF_{OCI}
- Service n°9 "available" for EF_{ICI}

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

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

~~Requirement: Service n°1 "available".~~

~~Service n°2 for FDN.~~

~~Service n°21 for MSISDN.~~

~~Service n°4 for SDN.~~

~~Service n°6 for BDN.~~

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

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

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

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

  ~~Requirement:~~

  ~~Service n°1 "available".~~

  ~~Service n°2 for FDN.~~

  ~~Service n°4 for SDN.~~

  ~~Service n°6 for BDN.~~

- The ME seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the ME runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted.
- The first 20 "digits" are stored in the dialling number/SSC string. The value of the length of BCD number/SSC contents is set to the maximum value, which is 11. The Extension1 record identifier is coded with the associated record number in the EF_{EXT1}. The remaining digits are stored in the selected Extension1 record where the type of the record is set to "additional data". The first byte of the Extension1 record is set with the number of bytes of the remaining additional data. The number of bytes containing digit information is the sum of the length of BCD number/SSC contents of EF_{ADN} and byte 2 of all associated chained Extension1 records containing additional data.

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

~~Requirement:~~

~~Service n°1 "available".~~

~~- Service n°2 for FDN.~~

~~- Service n°4 for SDN.~~

~~- Service n°6 for BDN.~~

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

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

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

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

Request: The ME sends the identification of the information to be read. The ME shall analyse the data of EF_{ADN} to ascertain, whether additional data is associated in EF_{EXT1} or EF_{CCP1}. If necessary, then the ME performs the reading procedure on these EFs to assemble the complete ADN/SSC.

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

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

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

FDN capability request. The ME shall check the state of service n°2, i.e. if FDN is "enabled" or "disabled". If FDN is enabled, the ME shall only allow outgoing calls as defined in the fixed number dialling description in TS 22.101 [24]. To ascertain the state of FDN, the ME shall check in EF_{UST} and EF_{EST} if FDN is enabled (service activated and available). In all other cases service n°2 is disabled.

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

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

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

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

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

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

5.3.5 Capability configuration parameters

- Requirement: Service n°14 "available".

- Request: The ME performs the reading procedure with EF_{CCP2}.

- Update: The ME performs the updating procedure with EF_{CCP2}.

- Erasure: The ME sends the identification of the requested information to be erased. The content of the identified record in EF_{CCP2} is marked as "free".

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].

Disabling of PIN2 is allowed. This is, however, not the case if PIN2 is mapped to the CHV2 of a GSM application.

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].

3GPP T3 (USIM) Meeting #19
St John, US VI, 8-11 May, 2001

Tdoc T3-010387
(revised version of T3-010330)

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **086** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	General Corrections
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11.05.2001
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:	⌘	
Summary of change:	⌘	
Consequences if not approved:	⌘	TS 31.102 will contain inconsistencies

Clauses affected:	⌘	4.4.2.1; 4.4.2.2; 5.3.2; 5.3.5; 6.4		
Other specs affected:	⌘	[ ] Other core specifications	⌘	
		[X] Test specifications		31.121
		[ ] O&M Specifications		
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 record identifier within a record.

Table 4.1: Phone Book Reference file Constructed Tags

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

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

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

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

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

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

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

4.4.2.2 EF_{IAP} (Index Administration Phone book)

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

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

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

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

Index administration file EF_{IAP} structure

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

Bytes	Description	M/O	Length
1	Record number of the first object indicated after Tag '~~Đ~~A9'	M	1 byte
2	Record number of the second object indicated after Tag '~~Đ~~A9'	M	1 byte
X	Record number of the x^{th} object indicated after Tag '~~Đ~~A9'	M	1 byte

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

5.3.2 Dialling numbers

Requirements:

- Service n°1 "available" for ADN located under the local phonebook
- Presence of EF_{ADN} in EF_{PBR} for ADN located under the global phonebook
- Presence of EF_{ANR} in EF_{PBR} for ANR.
- Service n°2 "available" for FDN.

- Service n°21 "available" for MSISDN.
- Service n°4 "available" for SDN.
- Service n°6 "available" for BDN.
- Service n°8 "available" for EF_{OCI}
- Service n°9 "available" for EF_{ICI}

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

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

~~Requirement: Service n°1 "available".~~

~~Service n°2 for FDN.~~

~~Service n°21 for MSISDN.~~

~~Service n°4 for SDN.~~

~~Service n°6 for BDN.~~

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

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

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

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

  ~~Requirement:~~

  ~~Service n°1 "available".~~

  ~~Service n°2 for FDN.~~

  ~~Service n°4 for SDN.~~

  ~~Service n°6 for BDN.~~

- The ME seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the ME runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted.
- The first 20 "digits" are stored in the dialling number/SSC string. The value of the length of BCD number/SSC contents is set to the maximum value, which is 11. The Extension1 record identifier is coded with the associated record number in the EF_{EXT1}. The remaining digits are stored in the selected Extension1 record where the type of the record is set to "additional data". The first byte of the Extension1 record is set with the number of bytes of the remaining additional data. The number of bytes containing digit information is the sum of the length of BCD number/SSC contents of EF_{ADN} and byte 2 of all associated chained Extension1 records containing additional data.

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

~~Requirement:~~

~~Service n°1 "available".~~

~~— Service n°2 for FDN.~~

~~— Service n°4 for SDN.~~

~~— Service n°6 for BDN.~~

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

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

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

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

Request: The ME sends the identification of the information to be read. The ME shall analyse the data of EF_{ADN} to ascertain, whether additional data is associated in EF_{EXT1} or EF_{CCP1}. If necessary, then the ME performs the reading procedure on these EFs to assemble the complete ADN/SSC.

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

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

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

FDN capability request. The ME shall check the state of service n°2, i.e. if FDN is "enabled" or "disabled". If FDN is enabled, the ME shall only allow outgoing calls as defined in the fixed number dialling description in TS 22.101 [24]. To ascertain the state of FDN, the ME shall check in EF_{UST} and EF_{EST} if FDN is enabled (service activated and available). In all other cases service n°2 is disabled.

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

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

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

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

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

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

5.3.5 Capability configuration parameters

- Requirement: Service n°14 "available".

- Request: The ME performs the reading procedure with EF_{CCP2}.

- Update: The ME performs the updating procedure with EF_{CCP2}.

- Erasure: The ME sends the identification of the requested information to be erased. The content of the identified record in EF_{CCP2} is marked as "free".

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].

Disabling of PIN2 is allowed. This is, however, not the case if PIN2 is mapped to the CHV2 of a GSM application.

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].

3GPP TSG-T3 (USIM) Meeting #19
St John, USA, 8-11 May 2001

Tdoc T3-010426
(supersedes T3-010398)

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **087** ⌘ rev **1** ⌘ Current version: **3.5.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarification of the Authenticate command description
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	10/05/2001
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:	⌘c	Prerequisites on when the Authenticate command can be executed, can be interpreted differently
Summary of change:	⌘	Clarification which directory has to be selected for the execution of the Authenticate command,
Consequences if not approved:	⌘	Different interpretations may lead to wrong implementations.

Clauses affected:	⌘	5.2, 7.1.1		
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.

5.2.1 Authentication algorithms computation

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

After a Successful AUTHENTICATE command, the ME shall perform Cipher and Integrity key update procedure.

[…]

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 application has been selected and activated, and the current directory is the USIM ADF or any subdirectory under this ADF, and a successful PIN verification procedure has been performed (see clause 5).

The function can be used in two different contexts:

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

3GPP T3 (USIM) Meeting #19
St John, US Virgin Island, 8-11 May, 2001

Tdoc T3-010404
(revised from T3-010389)

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **88** ⌘ rev **-** ⌘ Current version: **3.5.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarification of the type 3 links of the phonebook
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11-05-2001
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)*

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:	⌘	There's a limitation for files referenced by type 3 links that must be explicitely stated : 2 files of the same kind (such as EF_{EXT1}) cannot be referred to by a type 3 link.
Summary of change:	⌘	The restriction on files referred by type 3 links is added. The word "kind" is used as appropriate.
Consequences if not approved:	⌘	Inconsistencies within the specification.

Clauses affected:	⌘	Section 4.4.2.1, 4.4.2.14
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	Equivalent CR for the REL-4 specification : see CR 31.102-89

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

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

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

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

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

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

Table 4.1: Phone Book Reference file Constructed Tags

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

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

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

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

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

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

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

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

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

- Length = '02' Value: 'FID (2 bytes)'
- Length = '03' Value: 'FID (2 bytes)', 'SFI (1 byte)'

Table 4.2: Tag definitions for the phone book ~~type~~kind 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 kind of 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

4.4.2.14 Phonebook restrictions

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

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

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

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

- an EF_{PBR} record shall not contain more than one occurence of a given kind of file indicated in tag 'AA' (type 3 link). For instance, an EF_{PBR} record may only contain one reference to an EF_{EXT1}.

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

3GPP T3 (USIM) Meeting #19
St John, US Virgin Island, 8-11 May, 2001

Tdoc T3-010405

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **89** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarification of the type 3 links of the phonebook
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11-05-2001
Category:	⌘	**F**
Release:	⌘	REL-4

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)*

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:	⌘	There's a limitation for files referenced by type 3 links that must be explicitely stated : 2 files of the same kind (such as EF_{EXT1}) cannot be referred to by a type 3 link.
Summary of change:	⌘	The restriction on files referred by type 3 links is added. The word "kind" is used as appropriate.
Consequences if not approved:	⌘	Inconsistencies within the specification.

Clauses affected:	⌘	Section 4.4.2.1, 4.4.2.14
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	Equivalent CR for the R99 specification : see CR 31.102-88

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

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

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

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

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

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

Table 4.1: Phone Book Reference file Constructed Tags

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

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

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

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

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

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

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

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

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

- Length = '02' Value: 'FID (2 bytes)'
- Length = '03' Value: 'FID (2 bytes)', 'SFI (1 byte)'

Table 4.2: Tag definitions for the phone book ~~type~~kind 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 kind of 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

4.4.2.14 Phonebook restrictions

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

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

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

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

- an EF_{PBR} record shall not contain more than one occurence of a given kind of file indicated in tag 'AA' (type 3 link). For instance, an EF_{PBR} record may only contain one reference to an EF_{EXT1}.

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

3GPP T3 Meeting #19
St John, US VI, 8 - 11 May, 2001

Tdoc T3-010406
(revised from T3-010395)

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **90** ⌘ rev **-** ⌘ Current version: **3.4.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Correction of GSM Compact files
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11-05-2001
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)*

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 files are only used by GSM Compact mobiles, and therefore need not to be used by mobiles not supporting this radio access technology.
Summary of change:	⌘	It is clarified that GSM Compact files under DF(GSM-access) are optional. In particular $EF_{RPMLNAcT}$ is changed from 'mandatory' to 'optional'. Related procedures are updated. Clarified the status for other files needed for GSM access: EF_{Kc} and EF_{KcGPRS}
Consequences if not approved:	⌘	Inconsistency of the specification with RAN requirements.

Clauses affected:	⌘	Section 4.2.8, 4.2.56, 4.4.3, 4.4.3.1, 4.4.3.2, 5.1.1.3, 5.1.2.1, 5.1.2.2, 5.2.10, 5.2.11, 5.3.22		
Other specs affected:	⌘	[ ] Other core specifications [ ] Test specifications [ ] O&M Specifications	⌘	
Other comments:	⌘	An equivalent CR is needed for the REL-4 version of the specification		

4.2.8 EF_{UST} (USIM Service Table)

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

Identifier: '6F38'	Structure: transparent	Mandatory
SFI: '04'		
File size: X bytes, X >= 1	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Services n°1 to n°8	M	1 byte
2	Services n°9 to n°16	O	1 byte
3	Services n°17 to n°24	O	1 byte
4	Services n°25 to n°32	O	1 byte
etc.			
X	Services n°(8X-7) to n°(8X)	O	1 byte

-Services

Contents:	Service n°1 :	Local Phone Book
	Service n°2 :	Fixed Dialling Numbers (FDN)
	Service n°3 :	Extension 2
	Service n°4 :	Service Dialling Numbers (SDN)
	Service n°5 :	Extension3
	Service n°6 :	Barred Dialling Numbers (BDN)
	Service n°7 :	Extension4
	Service n°8 :	Outgoing Call Information (OCI and OCT)
	Service n°9 :	Incoming Call Information (ICI and ICT)
	Service n°10:	Short Message Storage (SMS)
	Service n°11:	Short Message Status Reports (SMSR)
	Service n°12:	Short Message Service Parameters (SMSP)
	Service n°13:	Advice of Charge (AoC)
	Service n°14:	Capability Configuration Parameters (CCP)
	Service n°15:	Cell Broadcast Message Identifier
	Service n°16:	Cell Broadcast Message Identifier Ranges
	Service n°17:	Group Identifier Level 1
	Service n°18:	Group Identifier Level 2
	Service n°19:	Service Provider Name
	Service n°20:	User controlled PLMN selector with Access Technology
	Service n°21:	MSISDN
	Service n°22:	Image (IMG)
	Service n°23:	Not used (reserved for SoLSA)
	Service n°24:	Enhanced Multi-Level Precedence and Pre-emption Service
	Service n°25:	Automatic Answer for eMLPP
	Service n°26:	RFU
	Service n°27:	GSM Access
	Service n°28:	Data download via SMS-PP
	Service n°29:	Data download via SMS-CB
	Service n°30:	Call Control by USIM
	Service n°31:	MO-SMS Control by USIM
	Service n°32:	RUN AT COMMAND command
	Service n°33:	shall be set to '1'
	Service n°34:	Enabled Services Table
	Service n°35:	APN Control List (ACL)
	Service n°36:	Depersonalisation Control Keys
	Service n°37:	Co-operative Network List
	Service n°38:	GSM security context
	Service n°39:	CPBCCH Information
	Service n°40:	Investigation Scan
	Service n°41:	MExE
	Service n°42:	Operator controlled PLMN selector with Access Technology
	Service n°43:	HPLMN selector with Access Technology
	Service n°44:	Extension 5
	Service n°xx:	RPLMN Last used Access Technology

4.2.56 $EF_{RPLMNA\sout{C}cT}$ (RPLMN Last used Access Technology)

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

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

Identifier: '6F65'	Structure: transparent	~~Mandatory~~ Optional
SFI: '18'		
File size: 2+X bytes	Update activity: High	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 2	Access Technology of RPLMN	M	2 bytes
3 to 2+X	RFU	O	X bytes

- Access Technology

  Coding:

  - See $EF_{PLMN\sout{sel}wA\sout{C}cT}$ for coding.

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

4.4.3.1 EF_{Kc} (GSM Ciphering key Kc)

This EF contains the ciphering key Kc and the ciphering key sequence number n for enciphering in a GSM access network. If the GSM access service is available on the USIM, then this file is mandatory.

Identifier: '4F20'	Structure: transparent	Optional
SFI: '01'		
File size: 9 bytes	Update activity: high	

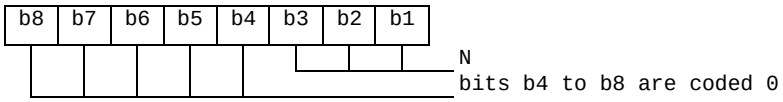
Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

- Ciphering key sequence number n
  Coding:



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

4.4.3.2 EF_{KcGPRS} (GPRS Ciphering key KcGPRS)

This EF contains the ciphering key KcGPRS and the ciphering key sequence number n for GPRS (see 3G TS 23.060 [7]). If the GSM access service is available on the USIM, then this file is mandatory.

Identifier: '4F52'	Structure: transparent	Optional
SFI: '02'		
File size: 9 bytes	Update activity: high	

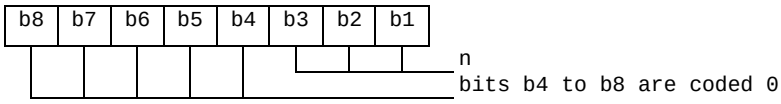
Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

- Ciphering key sequence number n for GPRS.
  Coding:



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

5.1.1.3 GSM related initialisation procedures

If GSM access is enabled the following procedures shall be performed if the applicable service is enabled~~.~~ and if the ME supports the GSM compact access technology.

- Investigation Scan request.
- CPBCCH information request.

5.1.2 Session termination

5.1.2.1 3G session termination

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

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

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

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

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

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

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

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

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

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

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

5.1.2.2 GSM termination procedures

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

- CPBCCH information update (if the ME supports the GSM compact access technology).
- RPLMN last used Access Technology update (if the ME supports the GSM compact access technology).

5.2.10 GSM Cipher key

Requirement: Service n°27 "available".

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

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

5.2.11 GPRS Cipher key

Requirement: Service n°27 "available".

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

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

5.3.22 RPLMN last used Access Technology

Requirement: Service n°xx "available".

Request: The ME performs the reading procedure with EF_{RPLMN}~~act~~AcT

Update: The ME performs the updating procedure with EF_{RLMN}~~act~~AcT.

3GPP T3 (USIM) Meeting #19
St John, US VI, 8-11 May, 2001

Tdoc T3-010437
Revision of T3-010431

CR-Form-v3

CHANGE REQUEST

⌘ **31.102 CR 91** ⌘ rev **-** ⌘ Current version: **3.5.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarification of OCT/ICT files.
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11/05/01
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:	⌘	It is not clearly specified that both OCI(ICI) and OCT(ICT) files shall be present when service n°8(9) is available. OCT and ICT files do need to have more than one entry.
Summary of change:	⌘	If service N°8 is available, both OCI and OCT files shall be present. If service N°9 is available, both ICI and ICT files shall be present. Addition of a note indicating that OCT and ICT files should have only one entry. Editorial change.
Consequences if not approved:	⌘	Inconsistencies.

Clauses affected:	⌘	4.2.33-4.2.36
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

4.2.33 EF_{ICI} (Incoming Call Information)

If service n°9 is "available", this file shall be present.

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

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

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

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

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

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

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

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

Structure of EF_{ICI}

Identifier: '6F80'	Structure: Cyclic	Optional
SFI: '14'		
Record length: X+28 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

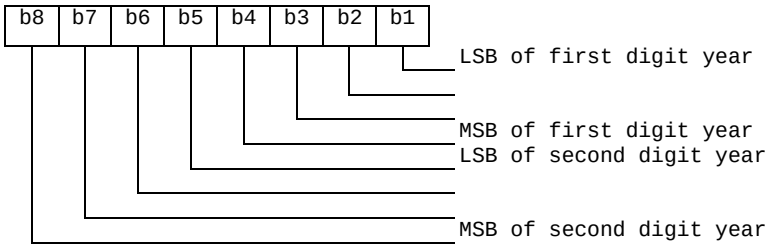
Detail 1 Coding of date and time.

Content:

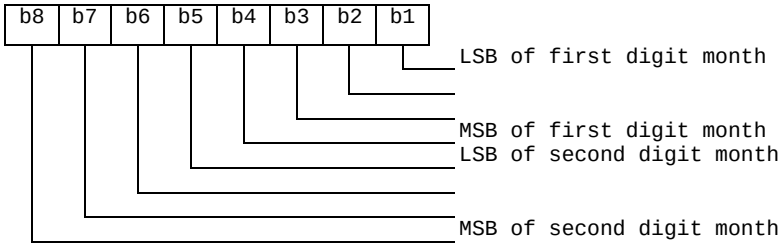
the date and time are defined by the ME.

Coding:

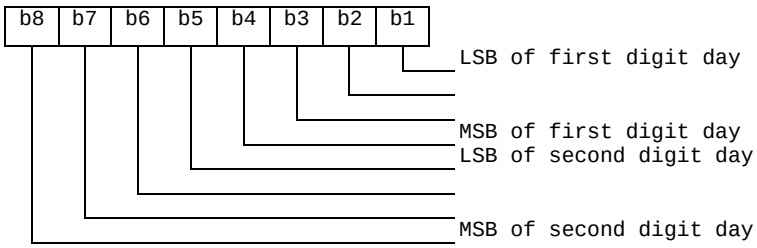
it is according to the extended BCD coding from Byte1 to Byte 7. The first 3 bytes show year, month and day (yy.mm.dd). The next 3 bytes show hour, minute and second (hh.mm.ss). The last Byte 7 is Time Zone. The Time Zone indicates the difference, expressed in quarters of an hour, between the local time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



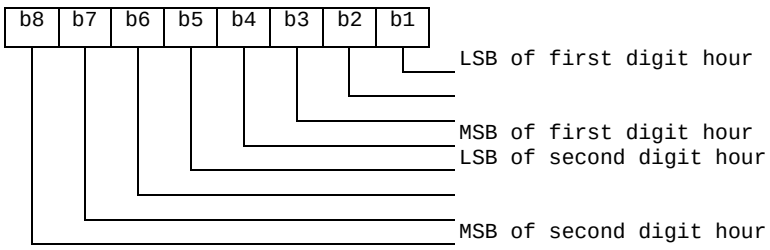
Byte X+16: Month



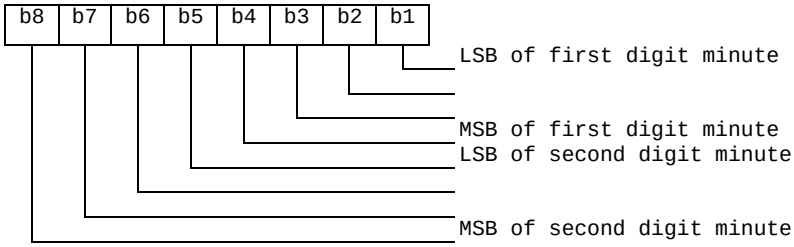
Byte X+17: Day



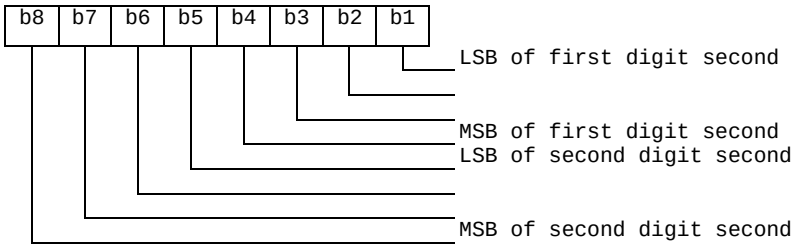
Byte X+18: Hour



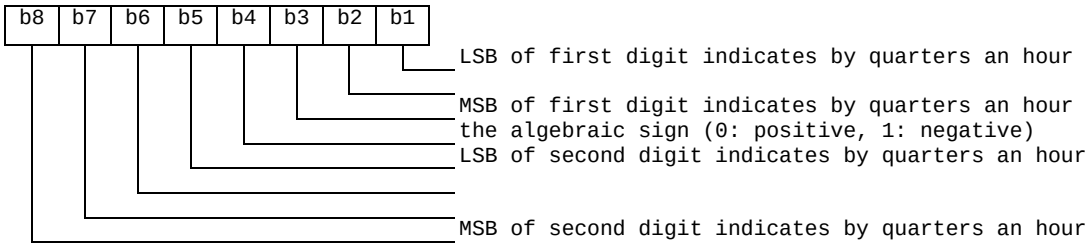
Byte X+19: Minute



Byte X+20: Second



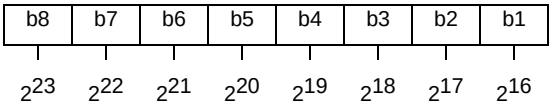
Byte X+21: Time Zone



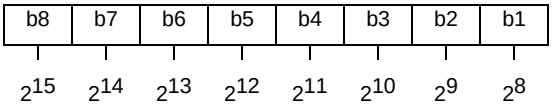
Detail 2 Coding of call duration.

Call duration is indicated by second.

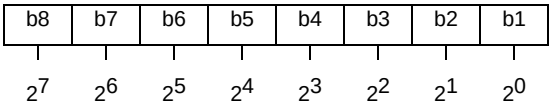
Byte X+22:



Byte X+23:



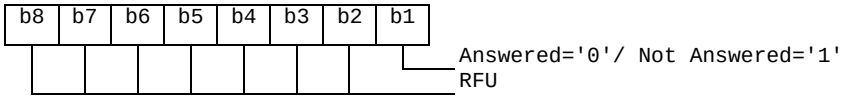
Byte X+24:



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

Detail 3 Coding of Call status.

Byte X+25:

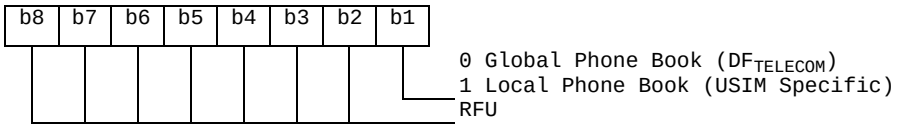


Detail 4 Link to phone book entry

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

Phone book reference.

Byte X+26:



EF_{PBR} record number:

- Byte X+27: Hexadecimal value.

EF_{ADN} record number:

- Byte X+28: Hexadecimal value.

4.2.34 EF_{OCI} (Outgoing Call Information)

If service n°8 is "available", this file shall be present.

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

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

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

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

Coding scheme is according to EF_{ICI}.

Structure of EF_{OCI}

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

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

4.2.35 EF_{ICT} (Incoming Call Timer)

If service n°9 is "available", this file shall be present.

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

NOTE: This file should have only one entry.

Structure of EF_{ICT}

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

Access Conditions:

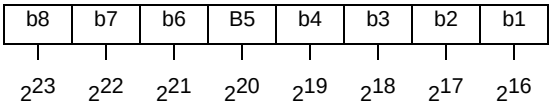
READ	PIN
UPDATE	PIN/PIN2 (fixed during administrative management)
INCREASE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

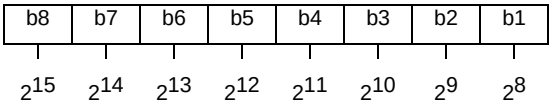
Coding:

Accumulated call timer value is indicated by second.

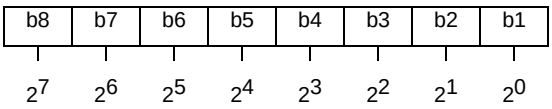
Byte 1:



Byte 2:



Byte 3:



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

4.2.36 EF_{OCT} (Outgoing Call Timer)

If service n°8 is "available", this file shall be present.

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

NOTE: This file should have only one entry.

Structure of EF_{OCT}

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

Access Conditions:

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

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

3GPP T3 (USIM) Meeting #19
St John, US VI, 8-11 May, 2001

Tdoc T3-010438

CR-Form-v3

CHANGE REQUEST

⌘ **31.102 CR 92** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarification of OCT/ICT files.
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11/05/01
Category:	⌘	**F**
Release:	⌘	REL-4

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:	⌘	It is not clearly specified that both OCI(ICI) and OCT(ICT) files shall be present when service n°8(9) is available. OCT and ICT files do need to have more than one entry.
Summary of change:	⌘	If service N°8 is available, both OCI and OCT files shall be present. If service N°9 is available, both ICI and ICT files shall be present. Addition of a note indicating that OCT and ICT files should have only one entry. Editorial change.
Consequences if not approved:	⌘	Inconsistencies.

Clauses affected:	⌘	4.2.33-4.2.36
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

4.2.33 EF_{ICI} (Incoming Call Information)

If service n°9 is "available", this file shall be present.

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

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

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

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

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

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

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

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

Structure of EF_{ICI}

Identifier: '6F80'	Structure: Cyclic	Optional
SFI: '14'		
Record length: X+28 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

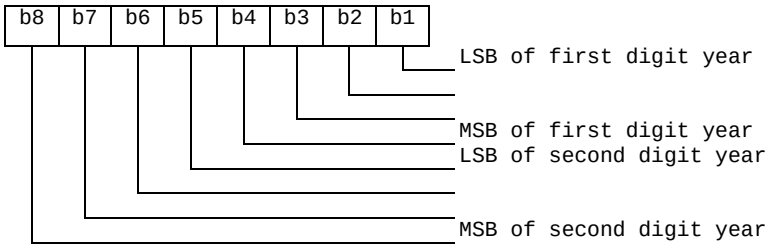
Detail 1 Coding of date and time.

Content:

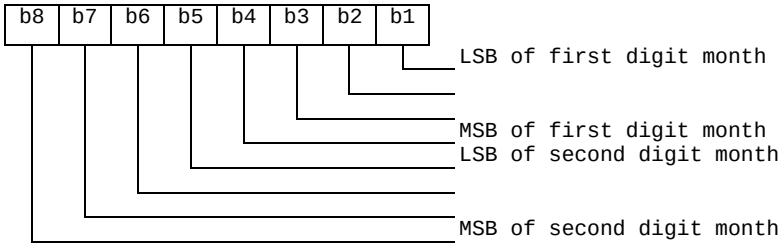
the date and time are defined by the ME.

Coding:

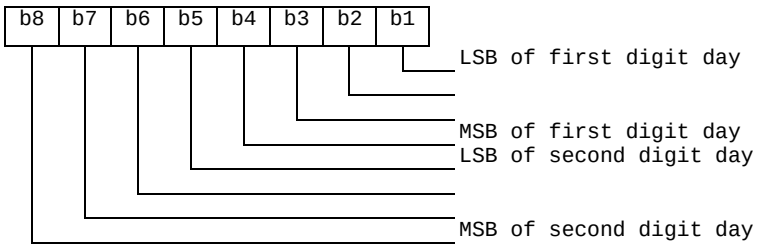
it is according to the extended BCD coding from Byte1 to Byte 7. The first 3 bytes show year, month and day (yy.mm.dd). The next 3 bytes show hour, minute and second (hh.mm.ss). The last Byte 7 is Time Zone. The Time Zone indicates the difference, expressed in quarters of an hour, between the local time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



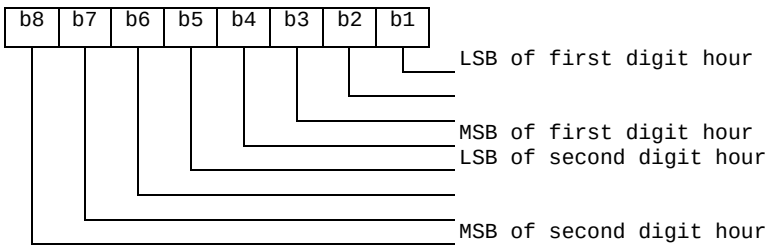
Byte X+16: Month



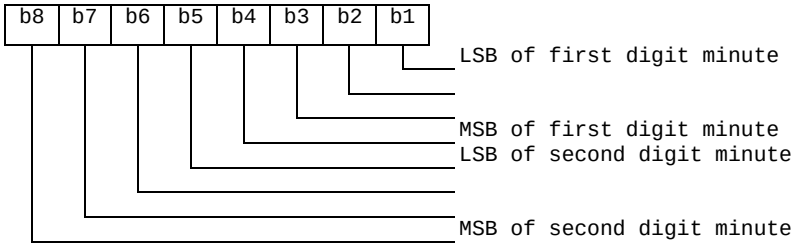
Byte X+17: Day



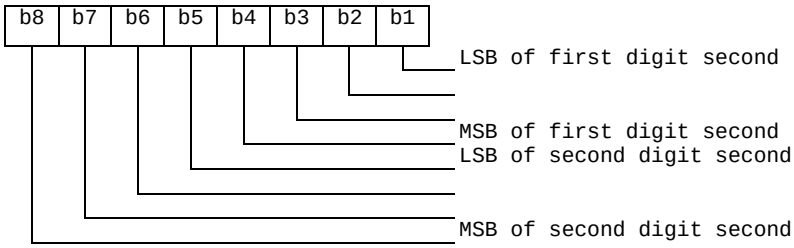
Byte X+18: Hour



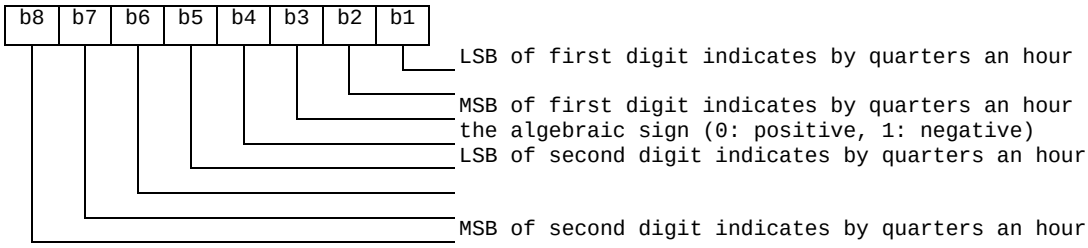
Byte X+19: Minute



Byte X+20: Second



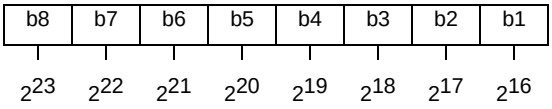
Byte X+21: Time Zone



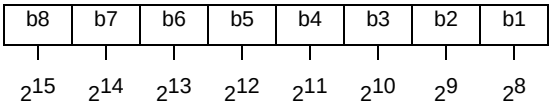
Detail 2 Coding of call duration.

Call duration is indicated by second.

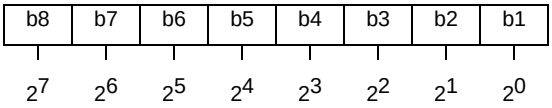
Byte X+22:



Byte X+23:



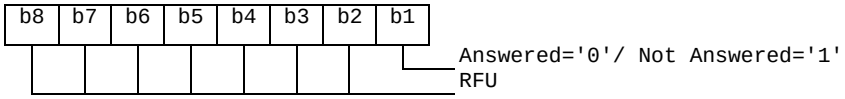
Byte X+24:



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

Detail 3 Coding of Call status.

Byte X+25:

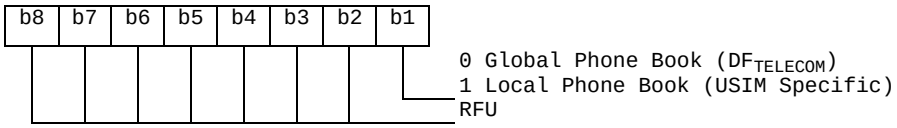


Detail 4 Link to phone book entry

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

Phone book reference.

Byte X+26:



EF_{PBR} record number:

- Byte X+27: Hexadecimal value.

EF_{ADN} record number:

- Byte X+28: Hexadecimal value.

4.2.34 EF_{OCI} (Outgoing Call Information)

If service n°8 is "available", this file shall be present.

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

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

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

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

Coding scheme is according to EF_{ICI}.

Structure of EF_{OCI}

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

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

4.2.35 EF_{ICT} (Incoming Call Timer)

If service n°9 is "available", this file shall be present.

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

NOTE: This file should have only one entry.

Structure of EF_{ICT}

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

Access Conditions:

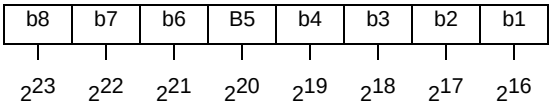
READ	PIN
UPDATE	PIN/PIN2 (fixed during administrative management)
INCREASE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

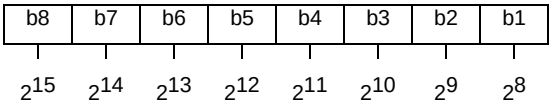
Coding:

Accumulated call timer value is indicated by second.

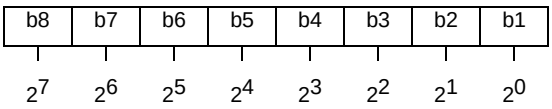
Byte 1:



Byte 2:



Byte 3:



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

4.2.36 EF_{OCT} (Outgoing Call Timer)

If service n°8 is "available", this file shall be present.

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

NOTE: This file should have only one entry.

Structure of EF_{OCT}

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

Access Conditions:

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

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

3GPP TSG-T3 (USIM) Meeting #19
St John, USVI, 8-11 May 2001

Tdoc T3-010439

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **093** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarification of the Authenticate command description
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	10/05/2001
Category:	⌘	**A**
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:	⌘c	Prerequisites on when the Authenticate command can be executed, can be interpreted differently
Summary of change:	⌘	Clarification which directory has to be selected for the execution of the Authenticate command,
Consequences if not approved:	⌘	Different interpretations may lead to wrong implementations.

Clauses affected:	⌘	5.2, 7.1.1		
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.

5.2.1 Authentication algorithms computation

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

After a Successful AUTHENTICATE command, the ME shall perform Cipher and Integrity key update procedure.

[…]

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 application has been selected and activated, and the current directory is the USIM ADF or any subdirectory under this ADF, ~~or any sub-directory has been selected as the Current Directory~~ and a successful PIN verification procedure has been performed (see clause 5).

The function can be used in two different contexts:

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

3GPP T3 Meeting #19
St John, US VI, 8 - 11 May, 2001

Tdoc T3-010440

CR-Form-v3

CHANGE REQUEST

⌘ **31.102** **CR** **94** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Correction of GSM Compact files
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11-05-2001
Category:	⌘	**F**
Release:	⌘	REL-4

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)*

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 files are only used by GSM Compact mobiles, and therefore need not to be used by mobiles not supporting this radio access technology.
Summary of change:	⌘	It is clarified that GSM Compact files under DF(GSM-access) are optional. In particular $EF_{RPMLNAcT}$ is changed from 'mandatory' to 'optional'. Related procedures are updated. Clarified the status for other files needed for GSM access: EF_{Kc} and EF_{KcGPRS}
Consequences if not approved:	⌘	Inconsistency of the specification with RAN requirements.

Clauses affected:	⌘	Section 4.2.8, 4.2.56, 4.4.3, 4.4.3.1, 4.4.3.2, 5.1.1.3, 5.1.2.1, 5.1.2.2, 5.2.10, 5.2.11, 5.3.22		
Other specs affected:	⌘	[ ] Other core specifications [ ] Test specifications [ ] O&M Specifications	⌘	
Other comments:	⌘	Equivalent to CR 31.102-90 (R99).		

4.2.8 EF_{UST} (USIM Service Table)

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

Identifier: '6F38'	Structure: transparent	Mandatory
SFI: '04'		
File size: X bytes, X >= 1	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Services n°1 to n°8	M	1 byte
2	Services n°9 to n°16	O	1 byte
3	Services n°17 to n°24	O	1 byte
4	Services n°25 to n°32	O	1 byte
etc.			
X	Services n°(8X-7) to n°(8X)	O	1 byte

-Services

Contents:	Service n°1 :	Local Phone Book
	Service n°2 :	Fixed Dialling Numbers (FDN)
	Service n°3 :	Extension 2
	Service n°4 :	Service Dialling Numbers (SDN)
	Service n°5 :	Extension3
	Service n°6 :	Barred Dialling Numbers (BDN)
	Service n°7 :	Extension4
	Service n°8 :	Outgoing Call Information (OCI and OCT)
	Service n°9 :	Incoming Call Information (ICI and ICT)
	Service n°10:	Short Message Storage (SMS)
	Service n°11:	Short Message Status Reports (SMSR)
	Service n°12:	Short Message Service Parameters (SMSP)
	Service n°13:	Advice of Charge (AoC)
	Service n°14:	Capability Configuration Parameters (CCP)
	Service n°15:	Cell Broadcast Message Identifier
	Service n°16:	Cell Broadcast Message Identifier Ranges
	Service n°17:	Group Identifier Level 1
	Service n°18:	Group Identifier Level 2
	Service n°19:	Service Provider Name
	Service n°20:	User controlled PLMN selector with Access Technology
	Service n°21:	MSISDN
	Service n°22:	Image (IMG)
	Service n°23:	Not used (reserved for SoLSA)
	Service n°24:	Enhanced Multi-Level Precedence and Pre-emption Service
	Service n°25:	Automatic Answer for eMLPP
	Service n°26:	RFU
	Service n°27:	GSM Access
	Service n°28:	Data download via SMS-PP
	Service n°29:	Data download via SMS-CB
	Service n°30:	Call Control by USIM
	Service n°31:	MO-SMS Control by USIM
	Service n°32:	RUN AT COMMAND command
	Service n°33:	shall be set to '1'
	Service n°34:	Enabled Services Table
	Service n°35:	APN Control List (ACL)
	Service n°36:	Depersonalisation Control Keys
	Service n°37:	Co-operative Network List
	Service n°38:	GSM security context
	Service n°39:	CPBCCH Information
	Service n°40:	Investigation Scan
	Service n°41:	MExE
	Service n°42:	Operator controlled PLMN selector with Access Technology
	Service n°43:	HPLMN selector with Access Technology
	Service n°44:	Extension 5
	Service n°45:	PLMN Network Name
	Service n°46:	Operator PLMN List
	Service n°47:	Mailbox Dialling Numbers
	Service n°48:	Message Waiting Indication Status
	Service n°49:	Call Forwarding Indication Status
	Service n°xx:	RPLMN Last used Access Technology

4.2.56 $EF_{RPLMNA\sout{C}cT}$ (RPLMN Last used Access Technology)

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

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

Identifier: '6F65'	Structure: transparent	~~Mandatory~~ Optional
SFI: '18'		
File size: 2+X bytes	Update activity: High	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 2	Access Technology of RPLMN	M	2 bytes
3 to 2+X	RFU	O	X bytes

- Access Technology

  Coding:

  - See $EF_{PLMN\sout{sel}wA\sout{C}cT}$ for coding.

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

4.4.3.1 EF_{Kc} (GSM Ciphering key Kc)

This EF contains the ciphering key Kc and the ciphering key sequence number n for enciphering in a GSM access network. If the GSM access service is available on the USIM, then this file is mandatory.

Identifier: '4F20'	Structure: transparent	Optional
SFI: '01'		
File size: 9 bytes	Update activity: high	

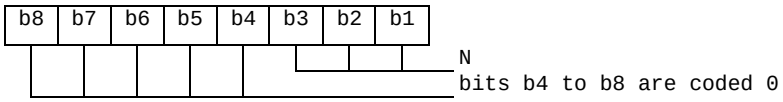
Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

- Ciphering key sequence number n
  Coding:



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

4.4.3.2 EF_{KcGPRS} (GPRS Ciphering key KcGPRS)

This EF contains the ciphering key KcGPRS and the ciphering key sequence number n for GPRS (see 3G TS 23.060 [7]). If the GSM access service is available on the USIM, then this file is mandatory.

Identifier: '4F52'	Structure: transparent	Optional
SFI: '02'		
File size: 9 bytes	Update activity: high	

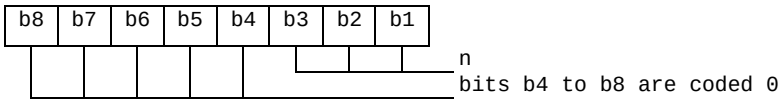
Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

- Ciphering key sequence number n for GPRS.
  Coding:



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

5.1.1.3 GSM related initialisation procedures

If GSM access is enabled the following procedures shall be performed if the applicable service is enabled~~.~~ and if the ME supports the GSM compact access technology.

- Investigation Scan request.
- CPBCCH information request.

5.1.2 Session termination

5.1.2.1 3G session termination

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

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

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

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

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

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

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

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

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

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

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

5.1.2.2 GSM termination procedures

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

- CPBCCH information update (if the ME supports the GSM compact access technology).
- RPLMN last used Access Technology update (if the ME supports the GSM compact access technology).

5.2.10 GSM Cipher key

Requirement: Service n°27 "available".

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

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

5.2.11 GPRS Cipher key

Requirement: Service n°27 "available".

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

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

5.3.22 RPLMN last used Access Technology

Requirement: Service n°xx "available".

Request: The ME performs the reading procedure with EF_{RPLMN}~~act~~AcT

Update: The ME performs the updating procedure with EF_{RLMN}~~act~~AcT.

3GPP T3 (USIM) Meeting #19
St John, US VI, 8-11 May, 2001

Tdoc T3-010450
(updated version of T3-010436)

CR-Form-v3

CHANGE REQUEST

⌘ **TS 31.102** **CR** **095** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	New implementation of SPN
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11/05/01
Category:	⌘	B
Release:	⌘	*REL-4*

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:	⌘	In its meeting of Cape Town in February 2001, S1 introduced a new implementation of the Service Provider Name for REL-4 (See 22.101 CR 068).
Summary of change:	⌘	• Add a new file, EF_{SPDI} to store the Service provider display information • Modify EF_{SPN} in order to store the new display conditions
Consequences if not approved:	⌘	Inconsistencies between S1 and T3 specifications.

Clauses affected:	⌘	4.2.8, 4.2.12, 4.2.X, 5.3.X
Other specs Affected:	⌘	[ ] Other core specifications [ ] Test specifications [ ] O&M Specifications
	⌘	
Other comments:	⌘	

4.2.8 EF_{UST} (USIM Service Table)

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

Identifier: '6F38'	Structure: transparent	Mandatory
SFI: '04'		
File size: X bytes, X >= 1	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Services n°1 to n°8	M	1 byte
2	Services n°9 to n°16	O	1 byte
3	Services n°17 to n°24	O	1 byte
4	Services n°25 to n°32	O	1 byte
etc.			
X	Services n°(8X-7) to n°(8X)	O	1 byte

-Services

Contents:		
	Service n°1 :	Local Phone Book
	Service n°2 :	Fixed Dialling Numbers (FDN)
	Service n°3 :	Extension 2
	Service n°4 :	Service Dialling Numbers (SDN)
	Service n°5 :	Extension3
	Service n°6 :	Barred Dialling Numbers (BDN)
	Service n°7 :	Extension4
	Service n°8 :	Outgoing Call Information (OCI and OCT)
	Service n°9 :	Incoming Call Information (ICI and ICT)
	Service n°10:	Short Message Storage (SMS)
	Service n°11:	Short Message Status Reports (SMSR)
	Service n°12:	Short Message Service Parameters (SMSP)
	Service n°13:	Advice of Charge (AoC)
	Service n°14:	Capability Configuration Parameters (CCP)
	Service n°15:	Cell Broadcast Message Identifier
	Service n°16:	Cell Broadcast Message Identifier Ranges
	Service n°17:	Group Identifier Level 1
	Service n°18:	Group Identifier Level 2
	Service n°19:	Service Provider Name
	Service n°20:	User controlled PLMN selector with Access Technology
	Service n°21:	MSISDN
	Service n°22:	Image (IMG)
	Service n°23:	Not used (reserved for SoLSA)
	Service n°24:	Enhanced Multi-Level Precedence and Pre-emption Service
	Service n°25:	Automatic Answer for Emlpp
	Service n°26:	RFU
	Service n°27:	GSM Access
	Service n°28:	Data download via SMS-PP
	Service n°29:	Data download via SMS-CB
	Service n°30:	Call Control by USIM
	Service n°31:	MO-SMS Control by USIM
	Service n°32:	RUN AT COMMAND command
	Service n°33:	Packet Switched Domain
	Service n°34:	Enabled Services Table
	Service n°35:	APN Control List (ACL)
	Service n°36:	Depersonalisation Control Keys
	Service n°37:	Co-operative Network List
	Service n°38:	GSM security context
	Service n°39	CPBCCH Information
	Service n°40	Investigation Scan
	Service n°41	MExE
	Service n°42	Operator controlled PLMN selector with Access Technology
	Service n°43	HPLMN selector with Access Technology
	Service n°xx	Service Provider Display Information

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

Coding:

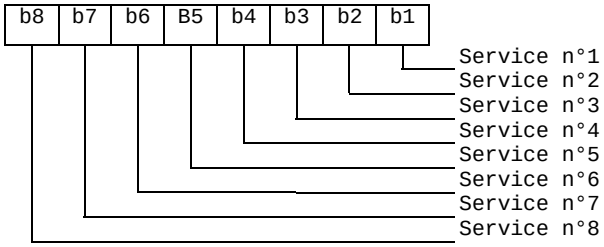
1 bit is used to code each service:

bit = 1: service available;

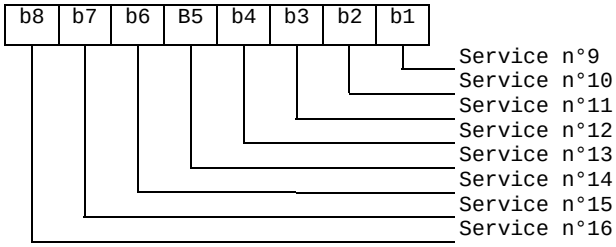
bit = 0: service not available.

- Service available means that the USIM has the capability to support the service and that the service is available for the user of the USIM unless the service is identified as "disabled" in EF_{EST}.
  Service not available means that the service shall not be used by the USIM user, even if the USIM has the capability to support the service.

First byte:



Second byte:



etc.

4.2.12 EF_{SPN} (Service Provider Name)

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

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

Access Conditions:

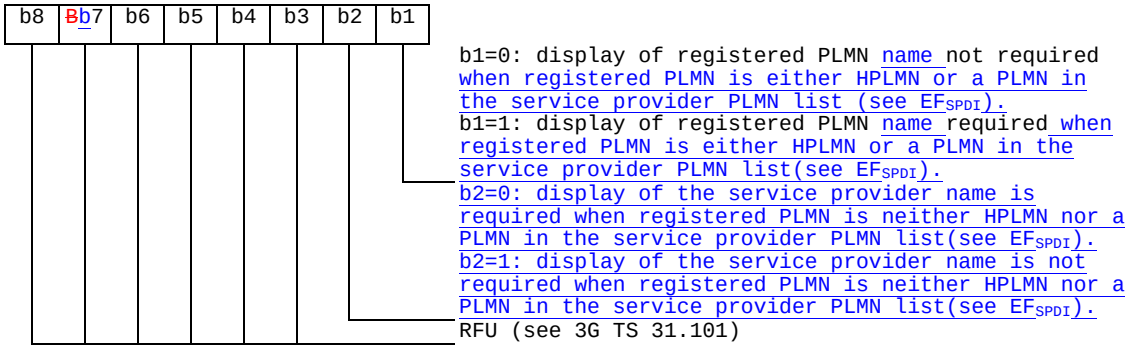
READ	ALWAYS
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

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

- Display Condition

  Contents: display condition for the service provider name in respect to the registered PLMN (see 3GPP TS 22.101[24] ~~GSM 02.07 [17]~~).

  Coding:



- Service Provider Name

  Contents:

  service provider string ~~to be displayed~~

  Coding:

  the string shall use:

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

4.2.X EF_{SPDI} (Service Provider Display Information)

This EF contains information regarding the service provider display i.e. the service provider PLMN list.

Identifier: 'XX'	Structure: transparent	Optional
SFI: 'XX'		
File size: 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) containing Service Provider information	M	x bytes

Tag Value	**Tag Description**
'Ax'	Service provider display information Tag
'80'	Service provider PLMN list tag

The service provider display information object is a constructed TLV.

- Service provider PLMN list

  Contents:

  This TLV contains a list of n PLMNs in which the Service Provider Name shall be displayed, as defined in subclause 4.2.12 (EF_{SPN}).

  Coding:

Description	**M/O**	**Length**
Service provider PLMN list tag	M	1 byte
Length (see note)	M	x bytes
1st PLMN entry	M	3 bytes
2nd PLMN entry	O	3 bytes
3rd PLMN entry	O	3 bytes
...		
nth PLMN entry	O	3 bytes
Note: the length is 3*n bytes, where n denotes the number of PLMN entries. The length can be coded on one or more bytes.		

  Each PLMN is coded as follows:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC) according to 3G TS 24.008 [9]. In case a PLMN entry is not used, it shall be set to 'FF FF FF'.

5.3.X Service Provider Display Information

Requirement: Service n°19 and xx are "available".

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

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