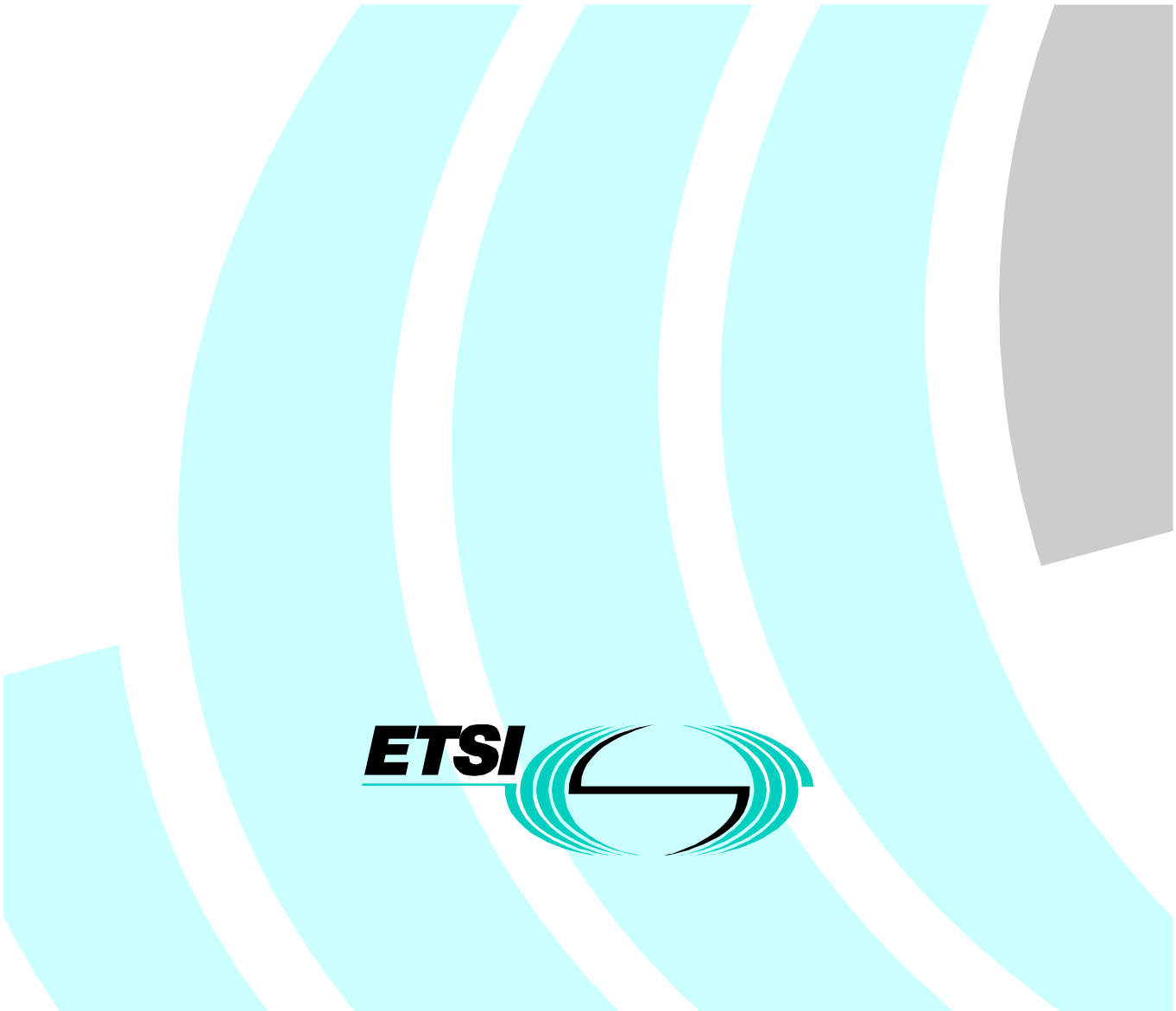
EN 300 477 V1.2.2 (1999-05)

European Standard (Telecommunications series)

Universal Personal Telecommunication (UPT); UPT phase 2; Functional specification of the interface of a UPT Integrated Circuit Card (ICC) and Card Accepting Devices (CAD); UPT card accepting Dual Tone Multiple Frequency (DTMF) device



Reference
REN/NA-064012 (4f000ipc.PDF)

Keywords
card, DTMF, UPT

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

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

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Technical Committee Network Aspects (NA).

National transposition dates	
Date of adoption of this EN:	23 April 1999
Date of latest announcement of this EN (doa):	31 July 1999
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 January 2000
Date of withdrawal of any conflicting National Standard (dow):	31 January 2000

1 Scope

The present document defines the interface between the Universal Personal Telecommunication (UPT) card and the Card Accepting Device (CAD) for the operational phase. It also defines those aspects of the internal organization of the UPT card which are related to the operational phase. This is to ensure interoperability between a UPT card and a CAD independently to the respective manufacturers and UPT service provider.

The present document only defines the interface between a UPT card and a card reading Dual Tone Multiple Frequency (DTMF) device (I-ETS 300 380 [1]).

NOTE: Other types of CADs are under study.

The present document defines:

- the requirements for the physical characteristics of the UPT card, the electrical signals and the transmission protocol;
- the model which shall be used as a basis for the design of the logical structure of the UPT card;
- the security features;
- the interface functions;
- the commands for operating the interface functions;
- the contents of the files required for the UPT application;
- the service set to be supported in the UPT card;
- the application protocol (security, services, etc.);
- the Implementation Conformance Statement (ICS) proformas.

The present document does not specify any aspects related to the administrative management phase. Any internal technical realization of either the UPT card or the CAD are only specified where these reflect over the interface. The present document does not specify any of the security algorithms which may be used.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] I-ETS 300 380: "Universal Personal Telecommunication (UPT); Access devices Dual Tone Multi Frequency (DTMF) sender for acoustical coupling to the microphone of a handset telephone".

[2] ETS 300 391-1: "Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT phase 1; Part 1: Specification".

[3] I-ETS 300 045 (1992): "European digital cellular telecommunication system (Phase 1); Subscriber Identity Module - Mobile Equipment (SIM-ME) interface specification (GSM 11.11)".

[4] CCITT Recommendation T.50 (1988): "International alphabet No 5 "(ISO 646: 1983, Information processing - ISO 7-bits coded characters set for information interchange)".

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

[6] ISO 7810 (1985): "Identification cards - Physical characteristics".

[7] ISO 7811-1 (1985): "Identification cards - Recording technique - Part 1: Embossing".

[8] ISO 7811-3 (1985): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards".

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

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

[11] ISO/IEC 7816-3 (1990): "Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols".

[12] ISO/IEC 7816-4: "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange".

[13] ISO 8859-1 (1987): "Information processing - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1".

[14] EN 726-3 (1994): "Terminal Equipment (TE); Requirements for IC cards and terminals for telecommunication use Part 3: Application independent card requirements".

[15] EN 726-6 (1994): "Terminal Equipment (TE); Requirements for IC cards and terminals for telecommunication use - Part 6: Telecommunication features".

[16] ENV 1375-1: "Identification card systems - Intersector integrated circuit(s) card additional formats - Part 1: ID-000 card size and physical characteristics".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

access conditions: set of security attributes associated with a file

ADM: access condition to an EF which is under the control of the authority which creates this file

administrative phase: part of the card life between the manufacturing phase and the usage phase

application: application consists of a set of security mechanisms, files, data and protocols (excluding transmission protocols) which are located and used in the Integrated Circuit (IC) card and outside the IC card (external application)

application protocol: set of procedures required by the application

CAD_{UPT}: card accepting device for UPT. All type of telecommunication terminals with a card reader accepting a UPT card

card holder verification: authentication of the user to the UPT card

card session: link between the card and the external world starting with the Answer To Reset (ATR) and ending with a subsequent reset or a de-activation of the card

CHV1: CHV; access condition used by the PIM for the verification of the identity of the user

current directory: latest Master File (MF) or Dedicated File (DF) selected

current Elementary File (EF): latest EF selected

current file: latest MF, DF or EF selected

Dedicated File (DF): file containing access conditions and, optionally, EFs or other DFs

device holder verification: authentication of the user to the UPT access device

directory: general term for MF or DF

Elementary File (EF): file containing access conditions and data and no other files

file: directory or an organized set of bytes or records in the PIM

file identifier: 2 bytes which address a file in the UPT card

ID-1 UPT card: UPT card having the format of an ID-1 card (see ISO/IEC 7816-1 [9])

Local Personal Identification Number (LPIN): used for card holder verification

Master File (MF): unique mandatory DF representing the root

padding: one or more bits appended to a message in order to cause the message to contain the required number of bits or bytes

PIM: data, functions and procedures residing in an IC card needed to gain access to UPT. It can be implemented as part of a multi-application card or as a UPT dedicated card

plug-in UPT card: second format of UPT card (see clause 4)

record: string of bytes within an EF handled as a single entity (see clause 6)

record number: number which identifies a record within an EF

record pointer: record pointer is used to address one record in an EF

Special Local Personal Identification Number (SLPIN): used to unblock the CHV1

UPT card application: set of security mechanisms, files, data and protocols which are located and used in the UPT card for the UPT service

UPT card session: link between the UPT card and the CAD_{UPT} starting with the ATR and ending with the subsequent reset or deactivation of the card

3.2 Symbols

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

Vcc	Supply voltage
Vpp	Programming voltage
'0' to '9' and 'A' to 'F'	The sixteen hexadecimal digits
V_{OH}	High level output voltage
V_{OL}	Low level output voltage
V_{IH}	High level input voltage
V_{IL}	Low level input voltage
Icc	Supply current at Vcc
I_{OH}	High level output current
I_{OL}	Low level output current
I_{IH}	High level input current
I_{IL}	Low level input current
t_R	Risetime from 10 % to 90 % of signal amplitude
t_F	Falltime from 90 % to 10 % of signal amplitude

C_{out}	Output capacitance
C_{in}	Input capacitance

3.3 Abbreviations

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

AC	Authentication Code
ADN	Abbreviated Dialling Number
APDU	Application Protocol Data Unit
ATR	Answer To Reset
BCD	Binary Coded Decimal
CAD	Card Accepting Device
CHV	Card Holder Verification information
DF	Dedicated File
DTMF	Dual Tone Multiple Frequency
EF	Elementary File
etu	elementary time unit
IC	Integrated Circuit
ICC	Integrated Circuit(s) Card
ID	Identifier
lgth	the (specific) length of a data unit
LND	Last Number Dialled
LPIN	Local Personal Identification Number
LSB	Least Significant Bit
MF	Master File
MMI	Man Machine Interface
MSB	Most Significant Bit
n_s	16 least significant bits of sequence number
NPI	Numbering Plan Identifier
PIM	Personal Identification Module
PIN	Personal Identification Number
PTS	Protocol Type Select (response to the ATR)
PUI	Personal User Identity
RFU	Reserved for Future Use
SLPIN	Special Local Personal Identification Number
SW1	Status Word 1
SW2	Status Word 2
TON	Type Of Number
UPT	Universal Personal Telecommunication

4 Physical characteristics

Two physical types of UPT card are specified. These are the "ID-1 card" (see ISO 7810 [6]) and the "plug-in card" (see ENV 1375-1 [16]).

The physical characteristics of both types of UPT card shall be in accordance with ISO/IEC 7816-1 [9] and ISO/IEC 7816-2 [10] unless otherwise specified. The following additional requirements shall be applied to ensure proper operation in the UPT environment.

4.1 Format and layout

The identification number as defined in EF_{ID} (see clause 10) shall be present on the outside of the ID-1 card. The information on the outside of the plug-in card shall include at least the individual account identifier and the check digit of the IC card identification.

4.1.1 ID-1 size

Format and layout of the ID-1 card shall be in accordance with ISO/IEC 7816-1 [9] and ISO/IEC 7816-2 [10].

The card should have a polarization mark which indicates how the user should insert the card into the CAD_{UPT}.

The CAD_{UPT} shall accept embossed ID-1 cards. The embossing shall be in accordance with ISO 7811-1 [7] and ISO 7811-3 [8]. The contacts of the ID-1 card shall be located on the front (embossed face, see ISO 7810 [6]) of the card.

4.1.2 Plug-in size

The plug-in card has a width of 25 mm, a height of 15 mm, a thickness the same as an ID-1 card and a feature for orientation. See annex A for details of the dimensions of the card and the dimensions and location of the contacts.

Clauses A.1 and A.2 of ISO/IEC 7816-1 [9] do not apply to the plug-in UPT card.

Annex A of ISO/IEC 7816-2 [10] applies with the location of the reference points adapted to the smaller size. The three reference points P1, P2 and P3 measure 7,5 mm, 3,3 mm and 20,8 mm, respectively, from 0 with the values in table A.1 of ISO/IEC 7816-2 [10] replaced by the corresponding values of figure A.1.

4.2 Temperature range for card operation

The temperature range for full operational use shall be between -25°C and +70°C with occasional peaks of up to +85°C. "Occasional" means not more than 4 hours each time and not more than 100 times during the life time of the card.

4.3 Contacts

The provision of contacts shall be in accordance with ISO/IEC 7816-2 [10].

4.3.1 Provision of contacts

CAD_{UPT}: There need not be any contacting elements in positions C4 and C8.

Contact C6 need not be provided.

UPT card: Contacts C4 and C8 need not be provided by the UPT card.

Contact C6 shall not be bonded in the UPT card.

4.3.2 Activation and deactivation

The CAD_{UPT} shall connect, activate and deactivate the UPT card in accordance with the operating procedures specified in ISO/IEC 7816-3 [11].

For any voltage level, monitored during the activation sequence, or during the deactivation sequence, the order of the contact activation/deactivation shall be respected.

NOTE 1: It is recommended that whenever possible the deactivation sequence defined in ISO/IEC 7816-3 [11] should be followed by the CAD_{UPT} on all occasions when the CAD_{UPT} is powered down.

NOTE 2: The voltage level of Vcc used by UPT differs from that specified in ISO/IEC 7816-3 [11]. Vcc is powered when it has a value between 4,5 V and 5,5 V.

4.3.3 Contact pressure

The contact pressure shall be large enough to ensure reliable and continuous contact (e.g. to overcome oxidization and to prevent interruption caused by vibration). The radius of any curvature of the contacting elements shall be greater than or equal to 0,8 mm over the contact area.

Under no circumstances may a contact force be greater than 0,5 N per contact.

4.4 Precedence

For a CAD_{UPT} which accepts both an ID-1 PIM and a plug-in PIM, the ID-1 PIM shall take precedence over the plug-in PIM.

5 Electronic signals and transmission protocols

Electronic signals and transmission protocols shall be in accordance with ISO/IEC 7816-3 [11] unless otherwise specified. The following additional requirements shall be applied to ensure proper operation in the UPT environment.

The choice of the transmission protocol(s), to be used to communicate between the PIM and the CAD_{UPT}, shall at least include that specified and denoted by T = 0 in ISO/IEC 7816-3 [11].

The values given in the tables hereafter are derived from ISO/IEC 7816-3 [11], subclause 4.2 with the following considerations:

- V_{OH} and V_{OL} always refer to the device (CAD_{UPT} or PIM) which is driving the interface. V_{IH} and V_{IL} always refer to the device (CAD_{UPT} or PIM) which is operating as a receiver on the interface;
- this convention is different to the one used in ISO/IEC 7816-3 [11], which specifically defines an ICC for which its current conventions apply. The following clauses define the specific core requirements for the PIM, which provide also the basis for Type Approval. For each state (V_{OH}, V_{IH}, V_{IL} and V_{OL}) a positive current is defined as flowing out of the entity (CAD_{UPT} or PIM) in that state;
- the high current options of ISO/IEC 7816-3 [11] for V_{IH} and V_{OH} are not specified for the PIM as they apply to NMOS technology requirements. No realization of the PIM using NMOS is foreseen.

5.1 Supply voltage

The PIM shall be operated within the following limits:

Table 1: Electrical characteristics of VCC under normal operating conditions

Symbol	Minimum	Maximum	Unit
Vcc	4,5	5,5	V
Icc		10	mA

The current consumption of the PIM shall not exceed the value given in table 1 at any frequency and voltage accepted by the PIM.

When the PIM is in idle state (see below) the current consumption of the card shall not exceed 200 µA at 1 MHz and 25°C.

The CAD_{UPT} shall support the current as required above. It shall also be able to counteract spikes in the current consumption of the card up to a maximum charge of 40 nAs with no more than 400 ns duration and a maximum amplitude of 200 mA, ensuring that the supply voltage stays in the specified range.

NOTE: A possible solution would be to place a capacitor (e.g. 100 nF, ceramic) as close as possible to the contacting elements.

5.2 Reset (RST) (contact C2)

The CAD_{UPT} shall operate the PIM within the following limits shown in table 2.

Table 2: Electrical characteristics of RST under normal operating conditions

Symbol	Conditions	Minimum	Maximum
V_{OH}	I_{OHmax} = +20 µA	Vcc - 0,7	Vcc (note)
V_{OL}	I_{OLmax} = -200 µA	0 V (note)	0,6 V
t_R t_F	$C_{out} = C_{in}$ = 30 pF		400 µs
NOTE: To allow for overshoot the voltage on RST shall remain between -0,3 V and Vcc + 0,3 V during dynamic operation.			

5.3 Programming voltage

The CAD_{UPT} need not provide contact C6. If the CAD_{UPT} provides contact C6, then contact C6 shall not be connected.

5.4 Clock (CLK)

The PIM shall operate with a clock frequency between 1 MHz and 5 MHz. The clock shall be supplied by the CAD_{UPT}. No "internal clock" PIMs shall be used.

The duty cycle shall be between 40 % and 60 % of the period during stable operation.

The CAD_{UPT} shall operate the PIM within the following limits:

Table 3: Electrical characteristics of CLK under normal operating conditions

Symbol	Conditions	Minimum	Maximum
V_{OH}	I_{OHmax} = +20 µA	0,7 x Vcc	Vcc (note)
V_{OL}	I_{OLmax} = -200 µA	0 V (note)	0,5 V
t_R t_F	$C_{out} = C_{in}$ = 30 pF		9 % of period with a maximum of 0,5 µs
NOTE: To allow for overshoot the voltage on CLK shall remain between -0,3 V and Vcc + 0,3 V during dynamic operation.			

5.5 I/O (contact C7)

Table 4 defines the electrical characteristics of the I/O (contact C7). The values given in the table have the effect of defining the values of the pull-up resistor in the CAD_{UPT} and the impedances of the drivers and receivers in the CAD_{UPT} and PIM.

Table 4: Electrical characteristics of I/O under normal operating conditions

Symbol	Conditions	Minimum	Maximum
V_{IH}	I_{IHmax} = ± 20 µA (note 2)	0,7 x Vcc	Vcc + 0,3 V
V_{IL}	I_{ILmax} = +1 mA	-0,3 V	0,8 V
V_{OH} (note 1)	I_{OHmax} = +20 µA	3,8 V	Vcc (note 3)
V_{OL}	I_{OLmax} = -1 mA	0 V (note 3)	0,4 V
t_R t_F	C_{out} = C_{in} = 30 pF		1µs
NOTE 1: It is assumed that a pull-up resistor is used in the interface device(recommended value: 20 kΩ). NOTE 2: During static conditions (idle state) only the positive value can apply. Under dynamic operating conditions (transmission) short term voltage spikes on the I/O line may cause a current reversal. NOTE 3: To allow for overshoot the voltage on I/O shall remain between -0,3 V and Vcc + 0,3 V during dynamic operation.			

5.6 States

There are two states for the PIM while the power supply is on:

- the PIM is in operating state when it executes a command. This state also includes transmission from and to the CAD_{UPT};
- the PIM is in idle state at any other time. It shall retain all pertinent data during this state.

The PIM may support a clockstop mode. The clock shall only be switched off subject to the conditions specified in the SELECT response to the MF.

Clockstop mode: A CAD_{UPT} shall wait at least five (5) elementary time units (etu's) after having received the last bit of the response before it switches off the clock (if it is allowed to do so). It shall wait at least two (2) etu's before it sends the first command after having started the clock.

5.7 Baud rate

The baud rate for all communications shall be: $\frac{(\text{clock frequency})}{372}$.

5.8 ATR

The ATR is information presented by the PIM to the CAD_{UPT} at the beginning of the card session and gives operational requirements.

5.8.1 Structure and contents

Table 5 gives an explanation of the characters specified in ISO/IEC 7816-3 [11] and the requirements for their use in UPT. The ATR consists of at most 33 characters. The CAD_{UPT} shall be able to receive interface characters for transmission protocols other than T = 0, historical characters and a check byte, even if only T = 0 is used by the CAD_{UPT}.

Table 5: ATR

	Character	Contents	sent by the card	a) evaluation by the CAD_{UPT} b) reaction by the CAD_{UPT}
1	Initial character TS	coding convention for all subsequent characters (direct or inverse convention)	always	a) always b) using appropriate convention
2	Format character T0	subsequent interface characters, number of historical characters	always	a) always b) identifying the subsequent characters accordingly
3	Interface character (global) TA1	parameters to calculate the work etu	optional	a) always if present b) if TA1 is not '11', Protocol Type Select (PTS) procedure shall be used (see subclause 5.7.2)
4	Interface character (global) TB1	parameters to calculate the programming voltage and current	optional	a) always if present b) if PI1 is not 0, then reject the UPT card in accordance with subclause 5.9
5	Interface character (global) TC1	parameters to calculate the extra guardtime requested by the card; no extra guardtime is used to send characters from the card to the CAD_{UPT}	optional	a) always if present b) if TC1 is not 0 or 255, then reject the UPT card in accordance with subclause 5.9 (note)
6	Interface character TD1	protocol type; indicator for the presence of interface characters, specifying rules to be used for transmissions with the given protocol type	optional	a) always if present b) identifying the subsequent characters accordingly
7	Interface character (specific) TA2	not used for protocol T = 0	optional	a) optional b) --------
8	Interface character (global) TB2	parameter to calculate the programming voltage	never	the allowed value of TB1 above defines that an external programming voltage is not applicable
9	Interface character (specific) TC2	parameters to calculate the work waiting time	optional	a) always if present b) using the work waiting time accordingly
10	Interface character TDi (i > 1)	protocol type; indicator for the presence of interface characters, specifying rules to be used for transmissions with the given protocol type	optional	a) always if present b) identifying the subsequent characters accordingly
11	Interface character TAi, TBi TCi (i > 2)	characters which contain interface characters for other transmission protocols	optional	a) optional b) --------

	Character	Contents	sent by the card	a) evaluation by the CAD_{UPT} b) reaction by the CAD_{UPT}
12	Historical characters T1,...,TK	specified by ISO/IEC 7816-4 [12]	optional	a) optional b) --------
13	Check character TCK	check byte (exclusive -ORing)	not sent if only T = 0 is indicated in the ATR; in all other cases TCK shall be sent	a) optional b) --------
NOTE: According to ISO/IEC 7816-3 [11], N = 255 indicates that the minimum delay is 12 etu's for the asynchronous half duplex character transmission protocol.				

5.8.2 PTS procedure

Specifically related to the present document the PTS procedure according to ISO/IEC 7816-3 [11], clause 7, is applied, in case of T = 0 and if TA1 is not equal to '11', as follows:

The following PTS procedure applies to T = 0:

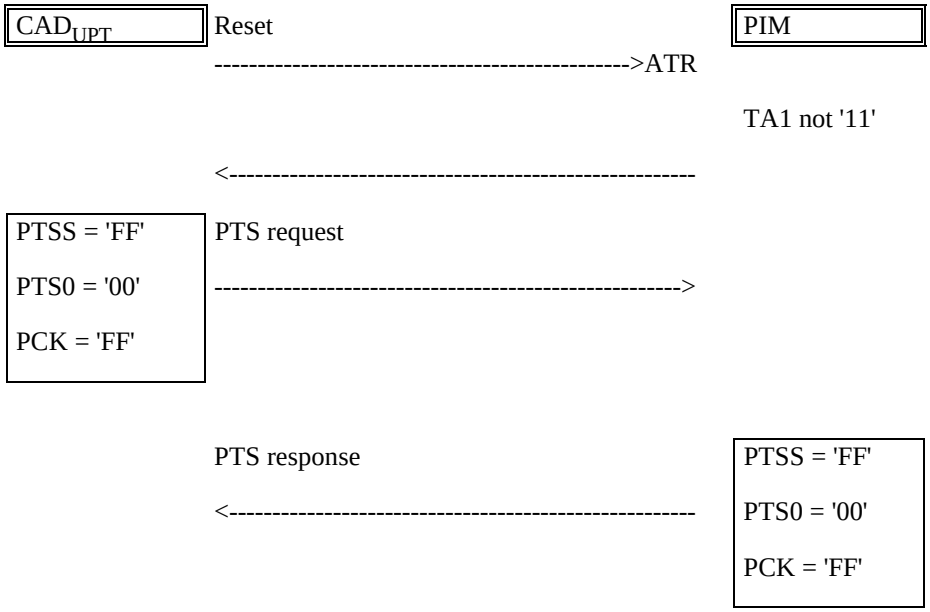


Figure 1: PTS procedure

PTS Request and PTS Response consist of the three (3) characters PTSS, PTS0 and PCK of which PTSS is sent first.

After this procedure the protocol T = 0 and the parameters F = 372, D = 1 and N = 0 will be used.

5.9 Error handling

Following receipt of a wrong ATR, the CAD_{UPT} shall perform a Reset. The CAD_{UPT} shall not reject the PIM until at least three consecutive wrong ATRs are received.

During the transmission of the ATR and the protocol type selection, the error detection and character repetition procedure specified in ISO/IEC 7816-3 [11], subclause 6.1.3, is optional for the CAD_{UPT}. For the subsequent transmission on the basis of T = 0 this procedure is mandatory for the CAD_{UPT}.

For the PIM, the error detection and character repetition procedure is mandatory for all communications.

6 Logical model

This clause describes the logical structure for the memory of a PIM, the code associated with it, and the structure of files used.

6.1 General model

Figure 2 shows the general structural relationship between files. The files are organized in a hierarchical structure. They may be either administrative or application specific. The operating system handles the access to the data stored in different files.

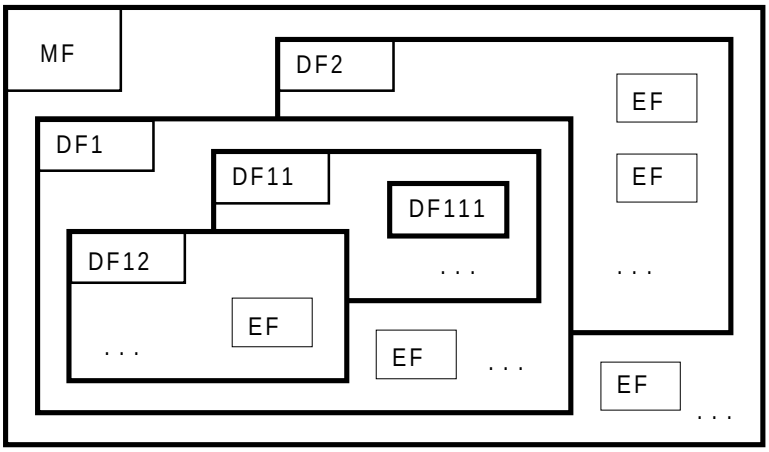


Figure 2: General structure of files in the PIM

Files are composed of a header, which is internally managed by the PIM, and optionally a body part. The information in the header is related to the structure and attributes of the file and may be obtained by using the response of the command SELECT. This information is fixed during the administrative phase. The body part contains the data of the file.

6.2 File identifier

A file ID is used to address or identify each specific file. The file ID consists of two bytes and shall be coded in hexadecimal notation.

The first byte identifies the type of file. For the PIM, the following values are specified:

'3F' MF (coded '3F00');

'7F' DF;

'2F' EF under the MF;

'00', '01' EF, specified in EN 726-3 [14];

'6F' EF under a DF.

File IDs shall be subject to the following conditions:

- the file ID shall be assigned at the time of the creation of the file concerned;
- no two files under the same parent shall have the same ID;
- a child and its parent shall never have the same file ID;
- a child and its grandparent shall never have the same file ID;
- a child and its grandparent's child (if it is a DF) shall never have the same file ID.

In this way, each file is uniquely identified. The file IDs are specified in clause 10.

6.3 MF

The MF is the DF (see subclause 6.4) representing the root of the file structure.

6.4 Dedicated Files

A DF is a functional grouping of files. It may be the parent of DFs and/or EFs.

A DF consists of a header and allocated memory for all files within this DF.

The following DFs are defined for the PIM: DF_{UPT} and $DF_{TELECOM}$:

- DF_{UPT} contains the UPT application and can be placed at any level;
- $DF_{TELECOM}$ contains the information about telecom features (e.g. abbreviated dialling, Last Number Dialled (LND) and other information used in the UPT features). It can be placed at any level.

NOTE: In a multiapplication card providing a UPT and a GSM application, $DF_{TELECOM}$ may be shared between both applications. In this case, the file identifier for $DF_{TELECOM}$ should be '7F10', and $DF_{TELECOM}$ be a direct child of the masterfile.

6.5 EFs

An EF is composed of a header and a body part. The following two structures of an EF can be used by the PIM.

6.5.1 Transparent EF

The PIM shall always be able to handle transparent EFs. The body part of a transparent EF consists of a sequence of bytes (figure 3). When reading or updating, the sequence of bytes to be acted upon is referenced by a relative address (offset) that indicates the start position (in bytes) and the number of bytes to be read or updated. The first byte of the body of a transparent EF has the relative address '0000'. The total data length of the body of the EF is indicated in the header of the EF.

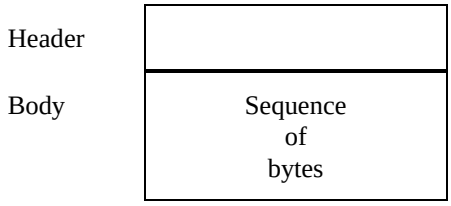


Figure 3: Structure of a transparent EF

6.5.2 Linear fixed EF

The PIM need only be able to handle linear fixed EFs if $DF_{TELECOM}$ is present. The body of an EF with linear fixed structure consists of a sequence of records all having the same (fixed) length. The first record is Record 1, the last record is Record n (figure 4).

The length of a record as well as this value multiplied by the number of records are indicated in the header of the EF.

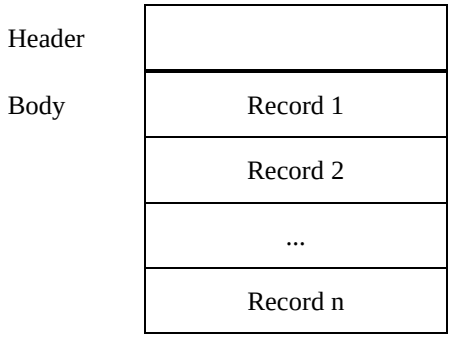


Figure 4: Structure of a linear fixed EF

There are several methods to access records within an EF of this type:

- absolutely, using the record number;
- when the record pointer is not set, it shall be possible to perform an action on the first or the last record;
- when the record pointer is set, it shall be possible to perform an action on this record, the next record (unless the record pointer is set to the last record), or the previous record (unless the record pointer is set to the first record);
- by identifying a record using pattern seek starting:
  - forwards from the beginning of the file;
  - forwards from the record following the one at which the record pointer is set (unless the record pointer is set to the last record);
  - backwards from the end of the file;
  - backwards from the record preceding the one at which the record pointer is set (unless the record pointer is set to the first record).

If an action following the selection of a record is aborted, then the record pointer shall remain set at the record at which it was set prior to the action. If the record pointer was not set prior to the action it shall remain undefined.

NOTE 1: It is not possible, at present, to have more than 255 records in a file of this type.

NOTE 2: It is not possible, at present, to have more than 255 bytes in one record.

6.5.3 Cyclic EF

The PIM need only be able to handle cyclic EFs if EF_{LND} is present. Cyclic files are used for storing records in chronological order. When all records have been used for storage, then the next storage of data shall overwrite the oldest information.

An EF with a cyclic structure consists of a fixed number of records with the same (fixed) length. In this file structure there is a link between the last record (n) and the first record. When the record pointer is set to the last record n, then the next record is record 1. Similarly, when the record pointer is set to record 1, then the previous record is record n. The last updated record containing the newest data is record number 1, and the oldest data is held in record number n.

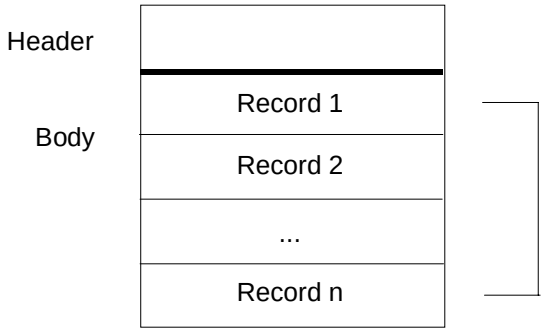


Figure 5: Structure of a cyclic file

For update operations only PREVIOUS record shall be used. For reading operations, the methods of addressing are Next, Previous, Current and Record Number.

After selection of a cyclic file (for either operation), the record pointer shall address the record updated or increased last. If an action following selection of a record is aborted, then the record pointer shall remain set at the record at which it was set prior to the action.

NOTE: It is not possible, at present, to have more than 255 records in a file of this type, and each record cannot be greater than 255 bytes.

6.6 Methods for selecting a file

Each file may be selected by using the SELECT function in accordance with the following rules:

1) selecting a DF or the MF sets the current directory. After such a selection, there is no current EF;

2) selecting an EF sets the current EF, and the current directory becomes the DF or MF that is the parent of this EF. The current EF is always a child of the current directory.

The following files may be selected:

- any file that is an immediate child of the current directory;
- any DF that is an immediate child of the parent of the current directory (this covers also the reselection of the current directory if there is a current EF);
- the parent of the current directory;
- the MF.

This means in particular that a DF shall be selected prior to the selection of any of its EFs. All selections are made using the file ID.

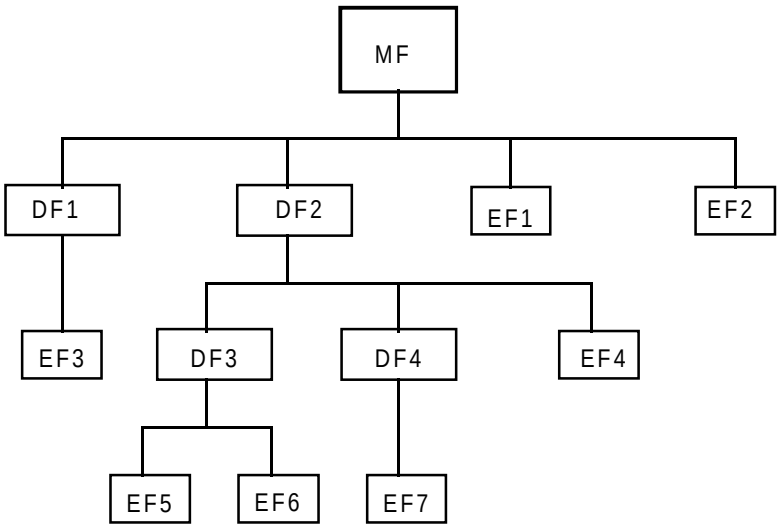


Figure 6: Logical file structure

Table 6 gives the valid selections according to the logical structure shown in figure 6. Reselection of the current file is also allowed, but not explicitly indicated in table 6.

Table 6: Valid file selections

current file	valid selections
MF	DF1, DF2, EF1, EF2
DF1	MF, DF2, EF3
DF2	MF, DF1, DF3, DF4, EF4
DF3	MF, DF2, DF4, EF5, EF6
DF4	MF, DF2, DF3, EF7
EF1	MF, DF1, DF2, EF2
EF2	MF, DF1, DF2, EF1
EF3	MF, DF1, DF2
EF4	MF, DF1, DF2, DF3, DF4
EF5	MF, DF2, DF3, DF4, EF6
EF6	MF, DF2, DF3, DF4, EF5
EF7	MF, DF2, DF3, DF4

6.7 Reservation of file IDs

In addition to the identifiers used for the files specified in the present document, the following IDs under DF_{UPT} are reserved for future UPT standardization:

- DFs: '7F1X';
- EFs: '6FXX'.

In addition the following file IDs are reserved for UPT administrative purposes (e.g. administrative files specified by card issuers or UPT providers) under DF_{UPT}:

- DFs: '7F4X';
- EFs: '2FXX'.

In the above mentioned file IDs, X ranges from '0' to 'F'. The value 'FF FF' shall not be used.

NOTE: When choosing file IDs, care should be taken to avoid conflicts with IDs already used in other standards concerning IC cards for telecommunication use.

7 Security services and facilities

The security services and facilities specified in the present document follows the architecture for UPT as specified in ETS 300 391-1 [2].

This clause considers those aspects which are relevant to the PIM.

The PIM can be used by UPT subscribers and UPT users. No distinguishment between these two is made in the present document. From the PIM's point of view they are both users.

The CAD_{UPT} interacts with the PIM and the user when performing the following security services and facilities:

- authentication of the user to the PIM (card holder verification);
- authentication of a CAD_{UPT} to the authenticating entity (strong authentication as defined in ETS 300 391-1 [2]);
- access control to the files in the PIM.

NOTE: The procedure used for authentication of the user to the card is called card holder verification and corresponds to device holder verification as described in ETS 300 391-1 [2].

7.1 Authentication key

For every Personal User Identity (PUI) there is a corresponding authentication key, K. K is used in the authentication algorithm for authenticating the PIM to the authenticating entity. The key has a length of 128 bits and it is stored in the PIM at personalization time.

7.2 Algorithms and processes

The possible authentication algorithms are identified in ETS 300 391-1 [2]. An LPIN, stored in the PIM is used for card holder verification.

A PIM shall be used for strong authentication as defined in ETS 300 391-1 [2].

The PIM needs to be connected to the CAD_{UPT} during the entire strong authentication procedure, see clause 11 for further details.

7.2.1 Card Holder Verification

Card holder verification is used to authenticate the UPT user to the PIM. A LPIN stored in the PIM is used for card holder verification, which is divided into two steps:

step 1: the user gives his LPIN to the CAD_{UPT};

step 2: the CAD_{UPT} sends the LPIN to the PIM in a VERIFY CHV command.

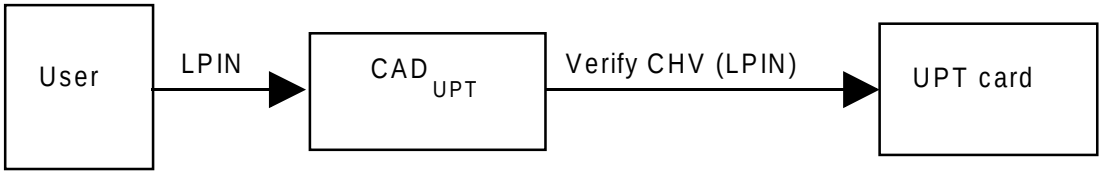


Figure 7: Card holder verification

The LPIN can be changed by using the CHANGE CHV command.

In case of 3 consecutive false CHV1 presentations the CHV1 shall be blocked. The access rights are lost and the UPT application cannot be accessed. It is not possible to perform a successful card holder verification until the CHV1 has been unblocked.

For the UPT application, the relevant CHV1 value is the LPIN, and the relevant UNBLOCK CHV1 value is the SLPIN (as defined in ETS 300 391-1 [2]).

It shall never be possible to disable the relevant CHV1 for the UPT application. That means if the relevant EF_{CHV1} resides under a parent directory, where it is requested to support the DISABLE CHV function, then a separate EF_{CHV1} whose relevant CHV1 cannot be disabled needs to reside under DF_{UPT}.

NOTE: There may exist more than one CHV1 in the PIM.

7.2.2 Strong authentication

The one pass strong authentication process works as follows:

1) a successful card holder verification is performed;
2) a timer is started in the CAD_{UPT}. If a time-out occurs the PIM shall be RESET by the CAD_{UPT}. No further authentication attempts can be made until a new card holder verification has been performed;
3) the authentication procedure is activated by the user (if the time-out has not been reached), whereby the following steps take place;
4) the PUI and the sequence number (n) are obtained from the PIM;
5) the sequence number is given to the PIM, which calculates an Authentication Code (AC) and returns it to the CAD_{UPT};
6) the sequence number (n) is incremented and stored in the PIM;
7) the CAD_{UPT} sends the PUI, n_s and AC to the authenticating entity;
8) if the authentication fails steps 3 to 7 can be repeated, as long as the time-out has not been reached.

7.3 File access conditions

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

The access conditions for the commands READ and SEEK are identical.

It is always possible to perform the command SELECT, since no access conditions are defined for this command.

The meaning of access conditions is as follows:

ALWAYS: the action can take place without any restriction;

CHV1: the action shall only be possible if one of the following conditions are fulfilled:

- a correct CHV1 value has already been presented to the PIM during the current session;
- UNBLOCK CHV1 has successfully been performed during the current session.

The CHV1 value of the relevant EF_{CHV1} shall be used. This means that EF_{CHV1} is a child of the current directory. If there is no such EF, then the relevant CHV1 of the parent directory shall be used.

NEVER: the action can not be performed over the PIM interface;

ADM: the action is the responsibility of the authority responsible for the creation of the file.

Access conditions are not hierarchical. An access condition which has been satisfied remains valid until the end of the PIM session as long as the corresponding CHV1 remains unblocked, i.e. only after three consecutive wrong attempts, not necessarily in the same PIM session, the access rights previously granted by this CHV1 are lost immediately.

7.4 Function access condition

It shall not be possible to use a PIM for authentication without a previous successful card holder verification. The reason is to protect the user against unauthorized use in case the device is stolen or lost. Therefore, the INTERNAL AUTHENTICATION command cannot be performed without a previous successful card holder verification.

7.5 Identification, keying and algorithm information

The following data used for identification, secret keys and input to the authentication algorithm are stored in the PIM:

- PUI (for identification of a UPT subscriber);
- LPIN (for card holder verification);
- SLPIN (for unblocking of the relevant CHV1);
- n (sequence number as a challenge to the authentication algorithm);
- K (secret key for the authentication algorithm).

8 Description of the functions

This clause specifies the minimum requirements for the functions and the commands and their respective responses. Associated status conditions, error codes and their corresponding codings are specified in clause 9.

It shall be mandatory for all cards complying with the present document to support all functions described in the present document. The command GET RESPONSE which is needed for the protocol T = 0 is specified in clause 9.

The following general functions are defined:

1) SELECT;
2) READ BINARY;
3) UPDATE BINARY;
4) READ RECORD;
5) UPDATE RECORD;
6) SEEK;
7) VERIFY CHV;
8) CHANGE CHV;
9) UNBLOCK CHV;
10) INTERNAL AUTHENTICATION.

Table 7 lists the file types and structures together with the functions which may act on them during the UPT session. These are indicated by a "*".

Table 7: Functions on files in UPT session

	File				
Function	MF	DF	EF transparent	EF linear fixed	EF cyclic
SELECT	*	*	*	*	*
READ BINARY			*		
UPDATE BINARY			*		
READ RECORD				*	*
UPDATE RECORD				*	*
SEEK				*	
NOTE: The specified set of functions in UPT is a subset of the one specified in EN 726-3 [14]. For some of the functions the full functionality as specified in EN 726-3 [14] is not required.					

8.1 SELECT

This function selects a file according to the methods described in clause 6. After a successful selection the record pointer in a linear fixed file is undefined.

Input:

- file ID.

Output:

- refer to subclause 9.3.1 for a description of the output data in case the selected file is a DF, an EF or a keyfile.

After a successful selection of an EF, the selected file becomes the current EF and the current DF remains unchanged. After a successful selection of a DF, the selected file becomes the current DF and the current EF is not defined.

NOTE: For this function, no ACs are defined.

8.2 READ BINARY

This function reads a string of bytes from the current transparent EF. This function shall only be performed if the READ access condition for the current EF is satisfied.

Input:

- relative address and the length of the string.

Output:

- string of bytes.

Refer to subclause 9.3.2 for a description of the input and output data.

8.3 UPDATE BINARY

This function updates the current transparent EF with a string of bytes. This function shall only be performed if the UPDATE access condition for the current EF is satisfied. An update can be considered as a replacement of the string already present in the EF by the string given in the update command.

Input:

- relative address and the length of the string;
- string of bytes.

Refer to subclause 9.3.3 for a description of the input data.

Output:

- none.

8.4 READ RECORD

This function is mandatory in case $DF_{TELECOM}$ exists in the card.

This function reads one complete record in the current linear EF. This function shall only be performed if the READ access condition for this EF is satisfied.

The record pointer shall not be changed by an unsuccessful READ RECORD function. If the record pointer is not defined, it shall remain not defined after an unsuccessful READ RECORD function. The READ RECORD function modes are described below. Four modes are defined:

CURRENT: The current record is read. The record pointer is not affected.

ABSOLUTE: The record given by the record number is read. The record pointer is not affected.

NEXT: The record pointer is incremented before the READ RECORD function is performed and the pointed record is read. If the record pointer has not been previously set within the selected EF, then READ RECORD (next) shall read the first record and set the record pointer to this record.
If the record pointer addresses the last record in a linear fixed EF, READ RECORD (next) shall not cause the record pointer to be changed and no data shall be read.

If the record pointer addresses the last record in a cyclic EF, READ RECORD (next) shall set the record pointer to the first record in this EF and this record shall be read.

PREVIOUS: The record pointer is decremented before the READ RECORD function is performed and the pointed record is read. If the record pointer has not been previously set within the selected EF, then READ RECORD (previous) shall read the last record and set the record pointer to this record.
If the record pointer addresses the first record in a linear fixed EF, READ RECORD (previous) shall not cause the record pointer to be changed, and no data shall be read.

If the record pointer addresses the first record in a cyclic EF, READ RECORD (previous) shall set the record pointer to the last record in this EF and this record shall be read.

Input:

- mode, record number (absolute mode only) and the length of the record.

Output:

- the record.

Refer to subclause 9.3.4 for a description of the input and output data.

8.5 UPDATE RECORD

This function is mandatory in case $DF_{TELECOM}$ exists in the card.

This function updates one complete record in the current linear fixed or cyclic EF. This function shall only be performed if the UPDATE access condition for this EF is satisfied. The UPDATE can be considered as a replacement of the relevant record data of the EF by the record data given in the command.

The record pointer shall not be changed by an unsuccessful UPDATE RECORD function. If the record pointer is not defined, it shall remain not defined after an unsuccessful UPDATE RECORD function. The UPDATE RECORD function modes are described below. Four modes are defined of which only PREVIOUS is allowed for cyclic files:

CURRENT: The current record is updated. The record pointer is not affected.

ABSOLUTE: The record given by the record number is updated. The record pointer is not affected.

NEXT: The record pointer is incremented before the UPDATE RECORD function is performed and the pointed record is updated. If the record pointer has not been previously set within the selected EF, then UPDATE RECORD (next) shall update the first record in the linear fixed EF and set the record pointer to this record. If the record pointer addresses the last record in a linear fixed EF, UPDATE RECORD (next) shall not cause the record pointer to be changed and no record shall be updated.

PREVIOUS: For a linear fixed EF the record pointer is decremented before the UPDATE RECORD function is performed and the pointed record is updated. If the record pointer has not been previously set within the selected EF, then UPDATE RECORD (previous) shall update the last record in a linear fixed EF and set the record pointer to this record. If the record pointer addresses the first record in a linear fixed EF, UPDATE RECORD (previous) shall not cause the record pointer to be changed and no record shall be updated.

For a cyclic EF the record containing the oldest data is updated, the record pointer is set to this record and this record becomes record number 1.

Input:

- mode, record number (absolute mode only) and the length of the record;
- the data used for updating the record.

Output:

- none.

Refer to subclause 9.3.5 for a description of the input data.

8.6 SEEK

This function is mandatory in case $DF_{TELECOM}$ exists in the card.

This function searches through the current linear fixed EF to find a record starting with the given pattern. This function shall only be performed if the READ access condition for the current EF is satisfied.

Two types of SEEK are defined:

Type 1: the record pointer is set to the record containing the pattern, no output is available;

Type 2: the record pointer is set to the record containing the pattern, the output is the record number.

The pattern length shall be less or equal to 16 bytes. The length of the pattern shall not exceed the record length.

Four modes are defined:

- from the beginning forwards;
- from the end backwards;
- from the next location forwards;
- from the previous location backwards.

If the record pointer has not been previously set (undefined) within the selected linear fixed EF, then the search begins:

- with the first record in the case of SEEK from the next location forwards; or
- with the last record in the case of SEEK from the previous location backwards.

If the record pointer is set to the last record in a linear fixed EF, a SEEK from the next location forwards shall not be allowed.

If the record pointer is set to the first record in a linear fixed EF, a SEEK from the previous location backwards shall not be allowed.

After a successful SEEK, the record pointer is set to the record in which the pattern was found. The record pointer shall not be changed by an unsuccessful SEEK function.

Input:

- type and mode;
- pattern;
- length of the pattern.

Output:

- type 1: none;
- type 2: record number.

Refer to subclause 9.3.6 for a description of the input and output data.

8.7 VERIFY CHV

This function verifies the CHV1 presented by the CAD_{UPT} by comparing it with the relevant one stored in the PIM.

If the access condition for a function to be performed on the last selected file is CHV1, then a successful verification of the relevant CHV1 is required prior to the use of the function on this file.

If the CHV1 presented is correct, the number of remaining card holder verification attempts for CHV1 shall be reset to its initial value 3.

If the CHV1 presented is false, the number of remaining card holder verification attempts for CHV1 shall be decremented. After 3 consecutive false CHV1 presentations, the respective CHV1 shall be blocked and the access condition granted by this CHV1 is immediately lost and can never be fulfilled until the UNBLOCK CHV function has been successfully performed on the respective CHV1.

Input:

- indication CHV1.

Output:

- none.

Refer to subclause 9.3.7 for a description of the input data.

8.8 CHANGE CHV

This function assigns a new value to the relevant CHV1 subject to the following condition being fulfilled:

- CHV1 is not blocked.

The old and new CHV1 shall be presented.

If the old CHV1 presented is correct, the number of remaining card holder verification attempts for that CHV1 shall be reset to its initial value 3 and the new value for the CHV1 becomes valid.

If the old CHV1 presented is false, the number of remaining card holder verification attempts for that CHV1 shall be decremented and the value of the CHV1 is unchanged. After 3 consecutive false CHV1 presentations, not necessarily in the same card session, the respective CHV1 shall be blocked and the access condition granted by this CHV1 is immediately lost and can never be fulfilled until the UNBLOCK CHV function has been performed successfully on the respective CHV1.

Input:

- indication CHV1, old CHV1, new CHV1.

Output:

- none.

Refer to subclause 9.3.8 for a description of the input data.

8.9 UNBLOCK CHV

This function unblocks a CHV1 which has been blocked by 3 consecutive wrong card holder verification presentations. This function may be performed whether or not the relevant CHV1 is blocked.

If the UNBLOCK CHV value presented is correct, the new CHV1 value presented is stored in the relevant CHV1, the number of remaining UNBLOCK CHV attempts for that UNBLOCK CHV is reset to its initial value 10 and the number of remaining card holder verification attempts for that CHV1 is reset to its initial value 3.

After a successful CHV1 unblocking, the relevant access condition CHV1 is satisfied.

If the presented UNBLOCK CHV value is false, the number of remaining UNBLOCK CHV attempts for that UNBLOCK CHV shall be decremented and that CHV1 attempt counter remain unchanged, this shall have no effect on the previous granted access conditions. After 10 consecutive false UNBLOCK CHV presentations, not necessarily in the same card session, the respective UNBLOCK CHV shall be blocked.

Input:

- indication CHV1, the UNBLOCK CHV and the new CHV1.

Output:

- none.

Refer to subclause 9.3.9 for a description of the input data.

8.10 INTERNAL AUTHENTICATION

This function allows the external world to authenticate an application in the card. For this purpose, the card has to calculate and send out a cryptogram, using the relevant key, and a challenge given to the card as input parameter of the INTERNAL AUTHENTICATION function. For this purpose, the card runs the appropriate algorithm (see ETS 300 391-1 [2].

For DF_{UPT}, INTERNAL AUTHENTICATION shall not be executable before CHV1 has been successfully verified.

Input:

- challenge (n).

Output:

- cryptogram.

Refer to subclause 9.3.10 for a description of the input and output data.

9 Description of the commands

9.1 Mapping principles

The mapping principles shall be in accordance with ISO/IEC 7816-4 [12] subclause 5.3 for the description of the message structure for the functions described in clause 8 of the present document.

9.1.1 Command Application Protocol Data Unit

The command Application Protocol Data Unit (APDU) shall be in accordance with ISO/IEC 7816-4 [12], subclause 5.3.1.

9.1.2 Response APDU

The response APDU shall be in accordance with ISO/IEC 7816-4 [12], subclause 5.3.3.

9.1.3 Command APDU conventions

The command APDU conventions shall be in accordance with ISO/IEC 7816-4 [12], subclause 5.3.2.

The transport of the APDUs of a command-response pair by the transmission protocols defined in ISO/IEC 7816-3 [11] shall be as specified in annex A of ISO/IEC 7816-4 [12] for T = 0, and as specified in annex B of ISO/IEC 7816-4 [12] for T = 1.

9.2 Definitions and coding

In all representations, the leftmost bit represents the Most Significant Bit (MSB) of the most significant byte while the rightmost bit represents the Least Significant Bit (LSB) of the least significant byte.

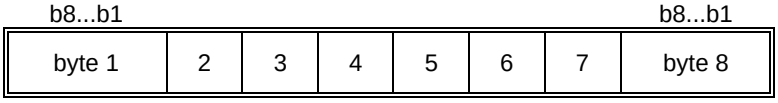


Figure 8: Notation for a string of bytes

Unless otherwise specified, data fields are left justified and padded with bits set to 1.

In a UPT specified card all bytes which are Reserved for Future Use (RFU) shall be set to '00' and RFU bits to 0. When the UPT application exists on a multi-application card or is built on a generic telecommunications card (e.g. EN 726-3 [14]) then other values may apply. The values will be defined in the appropriate specifications for such cards these bytes and bits shall not be interpreted by an CAD_{UPT} in a UPT session.

9.3 Coding of the commands

Table 8: Coding of the commands

Command	INS	P1	P2
Select	'A4'	'00'	'00'
Read binary	'B0'	offset high	offset low
Update binary	'D6'	offset high	offset low
Read record	'B2'	record number	mode
Update record	'DC'	record number	mode
Seek	'A2'	'00'	type/mode
Verify CHV	'20'	'00'	'01'
Change CHV	'24'	'00'	'01'
Unblock CHV	'2C'	'00'	'01'
Internal authentication	'88'	'00'	'00'
Get response	'C0'	'00'	'00'

9.3.1 SELECT

Table 9: Coding of the SELECT command

COMMAND	CLASS	INS	P1	P2	Lc
SELECT	'A0'	'A4'	'00'	'00'	'02'

Table 10: Command parameters: data

Bytes	Description	Length
1 - 2	File ID	2 bytes

Table 11: Response parameters/data in case of an MF or DF

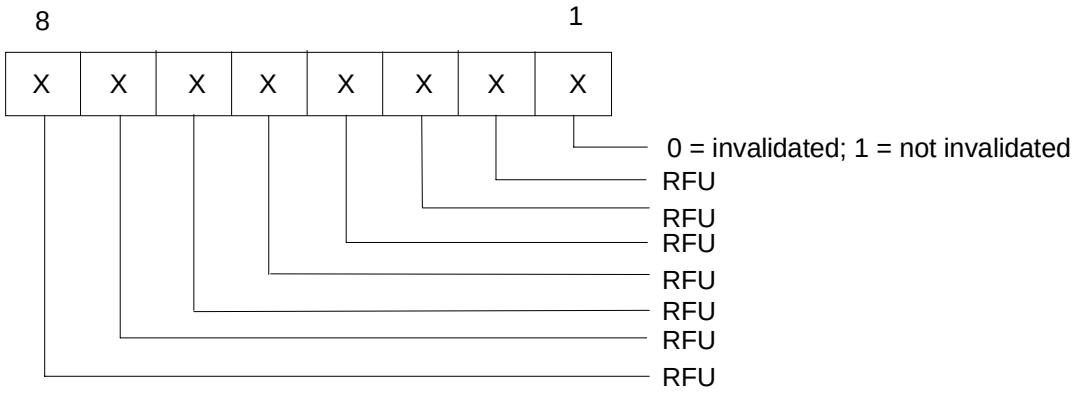
Bytes	Description	Length
1	RFU	1 byte
2	RFU	1 byte
3 - 4	Total amount of memory of the current directory which has not been allocated to any of the directories or EFs under the current directory	2 bytes
5 - 6	File ID	2 bytes
7	Type of file	1 byte
8	see subclause 9.4	1 byte
9 - 11	RFU	3 bytes
12	File status	1 byte
13	Length of the following data (byte 14 to the end)	1 byte
14	Current directory characteristics	1 byte
15	Number of direct son DFs under the current directory	1 byte
16	Number of direct son EFs under the current directory	1 byte
17	Number of secret codes	1 byte
18	RFU	1 byte
19	CHV1 status	1 byte
20	UNBLOCK CHV1 status	1 byte
21	RFU	1 byte
22	RFU	1 byte

Byte 7: Type of file:

'01'MF;

'02'DF.

Byte 12: File status



Byte 13: Length of the following data byte 14 to the end. (e.g. if the DF has a relevant EF_{CHV1} and no relevant EF_{CHV2}; the value of byte 13 is '07').

Byte 14: DF characteristics

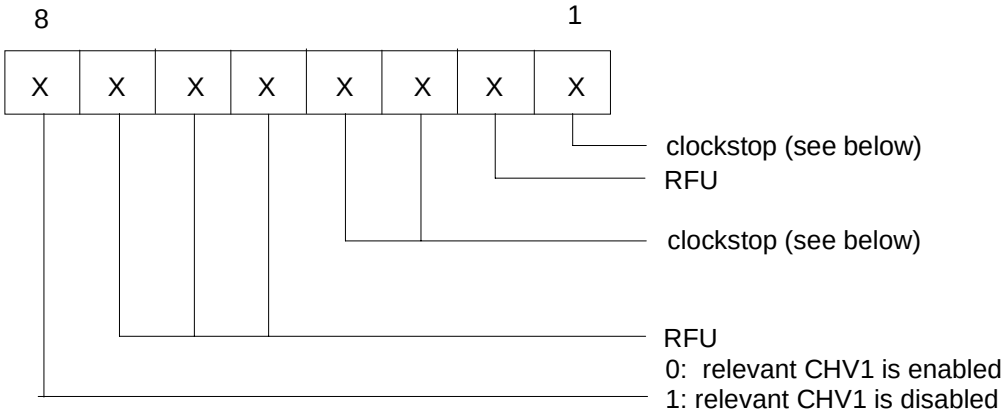


Table 12: Clockstop

bit1	bit3	bit4	Description
1	0	0	Clockstop allowed, no preferred level
1	1	0	Clockstop allowed, high level preferred
1	0	1	Clockstop allowed, low level preferred
0	0	0	Clockstop not allowed
0	1	0	Clockstop only allowed on high level
0	0	1	Clockstop only allowed on low level

Table 12 gives the coding of the conditions for stopping the clock (note that stopping the clock is an optional feature):

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

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

Byte 17: Number of secret codes.

This byte consists of the total number of both CHVs and UNBLOCK CHVs. Assuming that a CHV is always associated with an UNBLOCK CHV, both are located in the same file EF_{CHV}.(e.g. if the DF has a relevant EF_{CHV1} and no relevant EF_{CHV2}; the value of byte 17 is '02').

Byte 19, 20: CHV or UNBLOCK CHV status byte.

Each of those bytes is coded as follows:

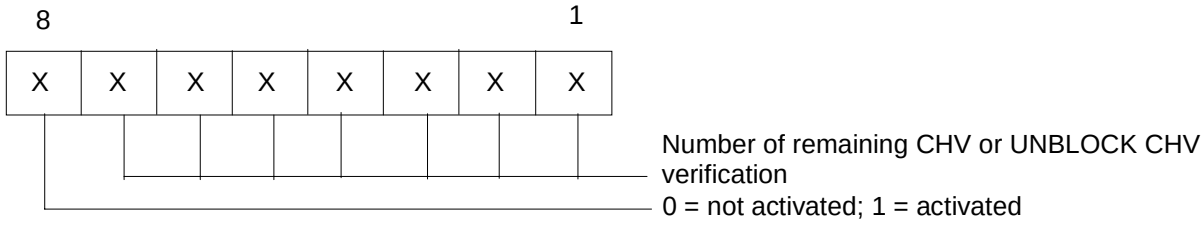


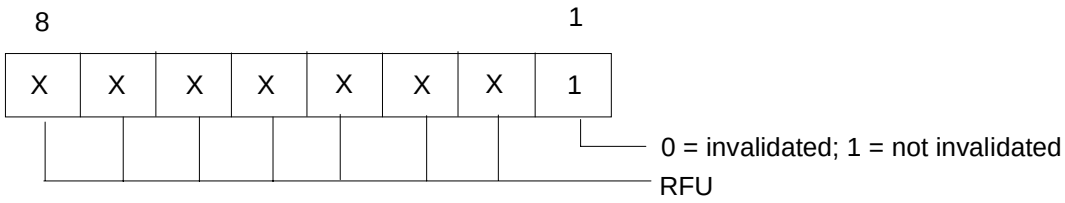
Table 13: Coding of the SELECT response in case of an EF

Bytes	Description	Length
1	RFU	1 byte
2	RFU	1 byte
3 - 4	File size (note)	2 bytes
5 - 6	File ID	2 bytes
7	Type of file	1 byte
8	RFU	1 byte
9	Access conditions (see subclause 9.4)	1 byte
10 - 11	RFU	2 bytes
12	File status	1 byte
13	Length of the following data (byte 14 to the end)	1 byte
14	Type of EF	1 byte
15	Length of a record (if linear fixed structure)	1 byte
NOTE: For a transparent file the file size indicates the number of bytes allocated for the body of the file. For a linear fixed or cyclic EF, the file size is: record length * number of records for this EF.		

Byte 7: Type of file:

'04'EF.

Byte 12: File status



Byte 13: Length of the following data (byte 14 to the end).

Byte 14: Type of EF:

'00'Transparent;

'01'Linear with fixed structure;

'03'Cyclic.

Byte 15: Length of a record.

For linear fixed or cyclic EFs this byte denotes the length of a record. For a transparent EF, this byte shall be coded '00', if this byte is sent by the PIM.

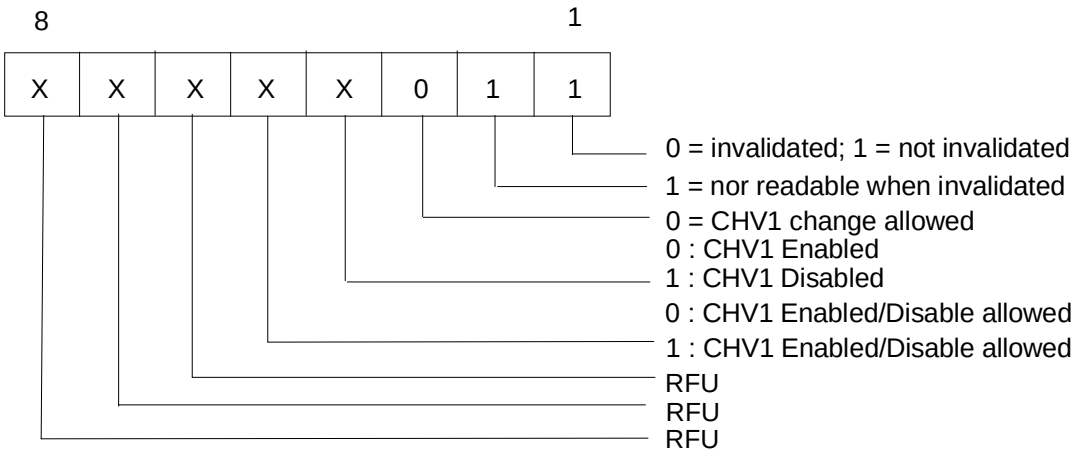
Table 14: Coding of the SELECT response in case of EF_{CHV1}

Bytes	Description	Length
1	RFU	1 byte
2	RFU	1 byte
3 - 4	File size (note)	2 bytes
5 - 6	File ID	2 bytes
7	Type of file	1 byte
8	RFU	1 byte
9	Access conditions (see subclause 9.4)	1 byte
10 - 11	RFU	2 bytes
12	File status	1 byte
13	Length of the following data (byte 14 to the end)	1 byte
14	Type of EF	1 byte
15	Number of remaining CHV1 attempts	1 byte
16	Type of user identification	1 byte
17	Way to present the CHV1	1 byte
18	Key number in the relevant EF KEY-OP	1 byte
19	Number of remaining UNBLOCK CHV1 attempts	1 byte
20	Number of remaining UNBLOCK CHV1 mechanisms	1 byte
NOTE: For a transparent file the file size indicates the number of bytes allocated for the body of the file.		

Byte 7: Type of file:

'04'EF.

Byte 12: File status



Byte 16: Type of user identification

If sent, byte 16 shall be coded '01' which means card holder verification.

Byte 17: Way to present the CHV1

If sent, byte 17 shall be coded as byte 2 of the. EF_{CHV} (see clause 10).

Byte 18, 20:

If sent, bytes 18 and 20 shall be coded 'FF' and shall not be interpreted by the CAD_{UPT}.

9.3.2 READ BINARY

Table 15: Coding of the READ BINARY command

COMMAND	CLASS	INS	P1	P2	Le
READ BINARY	'A0'	'B0'	offset high	offset low	lgth
lgth: length of data unit					

Offset is coded in 2 bytes, right justified, i.e. '00 00' means the 1st byte of the EF, '00 01' means the 2nd byte, etc.

Table 16: Response parameters/data

Bytes	Description	Length
1 - lgth	Data to be read	lgth

9.3.3 UPDATE BINARY

Table 17: Coding of the UPDATE BINARY command

COMMAND	CLASS	INS	P1	P2	Lc
UPDATE BINARY	'A0'	'D6'	offset high	offset low	lgth

Offset is coded in 2 bytes, right justified, i.e. '00 00' means the 1st byte of the EF, '00 01' means the 2nd byte, etc.

Table 18: Command parameters/data

Bytes	Description	Length
1 - lgth	Data	lgth

9.3.4 READ RECORD

Table 19: Coding of the READ RECORD command

COMMAND	CLASS	INS	P1	P2	Le
READ RECORD	'A0'	'B2'	Rec. No.	Mode	lgth

Parameter P2 specifies the mode:

- '02' = next record;
- '03' = previous record;
- '04' = absolute mode/current mode, the record number is given in P1 with P1 = '00' denoting the current record.

For the modes "next" and "previous" P1 has no significance and shall be set to '00' by the CAD_{UPT}. In this case this value shall not be interpreted by the PIM.

Table 20: Coding of the response parameters/data

Bytes	Description	Length
1 - lgth	Data	lgth

9.3.5 UPDATE RECORD

Table 21: Coding of the UPDATE RECORD command

COMMAND	CLASS	INS	P1	P2	Lc
UPDATE RECORD	'A0'	'DC'	Rec. No.	Mode	lgth

Parameter P2 specifies the mode:

- '02' = next record;
- '03' = previous record;
- '04' = absolute mode/current mode, the record number is given in P1 with P1 = '00' denoting the current record.

For the modes "next" and "previous" P1 has no significance and shall be set to '00' by the CAD_{UPT}. In this case this value shall not be interpreted by the PIM.

Table 22: Coding of the command parameters/data

Bytes	Description	Length
1 - lgth	Data	lgth

9.3.6 SEEK

Table 23: Coding of the SEEK command

COMMAND	CLASS	INS	P1	P2	Lc
SEEK	'A0'	'A2'	'00'	Type/Mode	lgth

Parameter P2 specifies type and mode:

- 'x0' = from the beginning forward;
- 'x1' = from the end backward;
- 'x2' = from the next location forward;
- 'x3' = from the previous location backward,

with x = '0' specifies type 1 and x = '1' specifies type 2 of the SEEK command.

Table 24: Coding of the command parameters/data

Bytes	Description	Length
1 - lgth	Pattern	lgth

There are no response parameters/data for a type 1 SEEK. A type 2 SEEK returns the following response parameters/data:

Table 25: Coding of the response parameters/data

Bytes	Description	Length
1	Record number	1 byte

9.3.7 VERIFY CHV

Table 26: Coding of the VERIFY CHV command

COMMAND	CLASS	INS	P1	P2	Lc
VERIFY CHV	'A0'	'20'	'00'	'01'	'08'
NOTE: '01' in parameter P2 indicates CHV1.					

Table 27: Coding of the command parameters/data

Bytes	Description	Length
1 - 8	CHV1 value	8 bytes

9.3.8 CHANGE CHV

Table 28: Coding of the CHANGE CHV command

COMMAND	CLASS	INS	P1	P2	Lc
CHANGE CHV	'A0'	'24'	'00'	'01'	'10'
NOTE: '01' in parameter P2 indicates CHV1.					

Table 29: Coding of the command parameters/data

Bytes	Description	Length
1 - 8	Old CHV1 value	8 bytes
9 - 16	New CHV1 value	8 bytes

9.3.9 UNBLOCK CHV

Table 30: Coding of the UNBLOCK CHV command

COMMAND	CLASS	INS	P1	P2	Lc
UNBLOCK CHV	'A0'	'2C'	'00'	'01'	'10'
NOTE: '01' in parameter P2 indicates CHV1.					

Table 31: Coding of the command parameters/data

Bytes	Description	Length
1 - 8	UNBLOCK CHV1 value	8 bytes
9 - 16	New CHV1 value	8 bytes

9.3.10 INTERNAL AUTHENTICATION

Table 32: Coding of the INTERNAL AUTHENTICATION command

COMMAND	CLASS	INS	P1	P2	Lc
INTERNAL AUTHENTICATION	'A0'	'88'	'00'	'00'	lgth

Table 33: Coding of the command parameters/data

Bytes	Description	Length
1 - 8	Challenge (sequence number)	8 bytes

Table 34: Coding of the response parameters data

Bytes	Description	Length
1 - 8	Cryptogram (AC)	8 bytes

9.3.11 GET RESPONSE

Table 35: Coding of the GET RESPONSE command

COMMAND	CLASS	INS	P1	P2	Le
GET RESPONSE	'A0'	'C0'	'00'	'00'	lgth

The response data depends on the preceding command. Response data is available after the commands INTERNAL AUTHENTICATION, SEEK (type 2), SELECT and GET RESPONSE. If the command GET RESPONSE is executed, it is required that it is executed just after the command it is related to (no other command shall come between the command/response pair and the command GET RESPONSE). If the sequence is not respected, the PIM shall send the status information "technical problem with no diagnostic given" as a reaction to the GET RESPONSE.

The response data itself is defined in the subclause for the corresponding command.

9.4 Access condition coding

The access conditions for the commands are coded on byte 9 of the response data of the SELECT command.

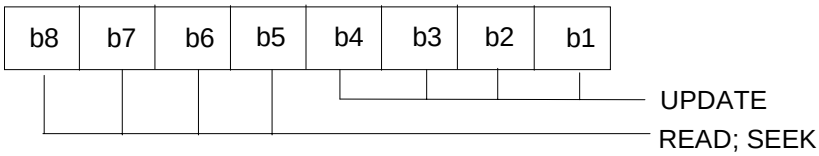
For byte 9, all the possible access conditions are coded on 4 bits as defined in table 36.

Table 36

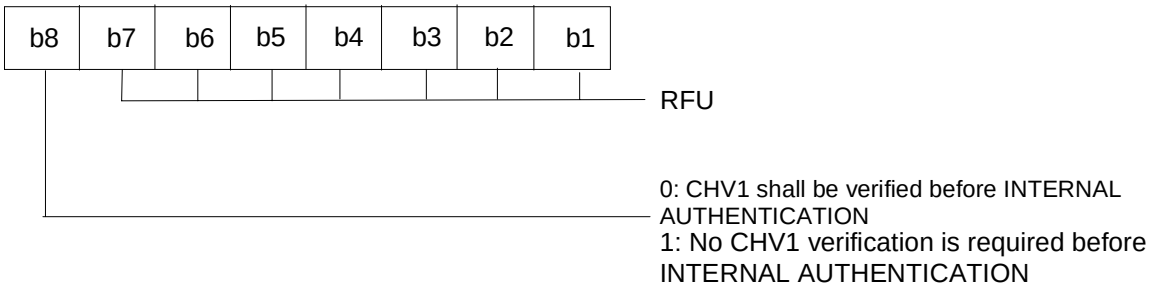
ALWAYS	'0'
CHV1	'1'
NEVER	'F'

The coding of Byte 9 in case of an EF is as follows:

Byte 9:



Byte 8:



For DF_{UPT}, bit 8 shall be set to 0.

Bytes 10 and 11 of the response data to the SELECT command shall not be interpreted by the CAD_{UPT}.

9.5 Coding of CHVs and UNBLOCK CHVs

Only decimal digits (0-9) shall be used for CHV and UNBLOCK CHV. The coding shall be ASCII (as described in CCITT Recommendation T.50 [4] with bit 8 set to zero).

CHV1 consists of 4 to 8 decimal digits. If the number of digits presented by the user is less than 8, the CAD_{UPT} shall pad the presented CHV with 'FF' before sending it to the PIM.

The UNBLOCK CHV1 consists of 8 decimal digits.

9.6 Status conditions returned by the card

According to ISO/IEC 7816-3 [11] two status bytes, Status Word 1 (SW1) and Status Word 2 (SW2), are returned after each command.

9.6.1 Security management

Table 37

SW1	SW2	Error description
'98'	'02'	- No CHV and/or key defined.
'98'	'04'	- AC not fulfilled. - Unsuccessful card holder verification but verify CHV mechanism still possible (number of false consecutive verifications < 3). - Unsuccessful UNBLOCK CHV verification but verify UNBLOCK CHV mechanism still possible (number of false consecutive verifications < 10).
'98'	'08'	- In contradiction with CHV status.
'98'	'10'	- In contradiction with the invalidation status.
'98'	'40'	- Unsuccessful CHV verification, verify CHV mechanism no longer possible (number of false consecutive verifications ≥ 3). - Unsuccessful UNBLOCK CHV verification, verify UNBLOCK CHV mechanism no longer possible (number of false consecutive verifications ≥ 10). - CHV blocked. - UNBLOCK CHV blocked.

9.6.2 Memory management

Table 38

SW1	SW2	Error description
'92'	'0X'	- Update successful but after using an internal retry routine X times.
'92'	'40'	- Memory problem.

9.6.3 Referencing management

Table 39

SW1	SW2	Error description
'94'	'00'	- No EF selected as current. - EF not selected.
'94'	'02'	- Out of range (invalid address).
'94'	'04'	- File ID not found. - Pattern not found.
'94'	'08'	- Current file-type is inconsistent with the command.

9.6.4 Application independent errors

Table 40

SW1	SW2	Error description
'6E'	'XX'	- Wrong instruction class given in the command.
'6D'	'XX'	- Unknown instruction code given in the command.
'6F'	'XX'	- Technical problem with no diagnostic given (command aborted).
'6B'	'XX'	- Incorrect parameters P1 or P2.
'67'	'XX'	- Checking error: wrong length.

9.6.5 Responses to commands which are correctly executed or supporting chaining mechanism

Table 41

SW1	SW2	Error description
'90'	'00'	- Normal ending (ACK) of the command.
'9F'	'XX'	- Length 'XX' of the response data.

9.6.6 Commands versus possible status responses

Table 42 shows the possible status conditions returned for each command (marked by *).

Table 42: Status responses

	OK		Mem st.		Reference status				Security status					Application independent errors				
Commands	90 00	9F XX	92 0X	92 40	94 00	94 02	94 04	94 08	98 02	98 04	98 08	98 10	98 40	6E XX	6D XX	6F XX	6B XX	67 XX
CHANGE CHV	*		*	*					*	*	*		*	*	*	*	*	*
GET RESPONSE	*													*	*	*	*	*
INTERNAL AUTHENTICATION		*						*	*	*				*	*	*	*	*
READ BINARY	*				*	*		*		*		*		*	*	*	*	*
READ RECORD	*				*	*		*		*		*		*	*	*	*	*
SEEK	*	*			*		*	*		*		*		*	*	*	*	*
SELECT		*					*							*	*	*	*	*
UNBLOCK CHV	*		*	*					*	*	*		*	*	*	*	*	*
UPDATE BINARY	*		*	*	*	*		*		*		*		*	*	*	*	*
UPDATE RECORD	*		*	*	*	*		*		*		*		*	*	*	*	*
VERIFY CHV	*		*	*					*	*	*		*	*	*	*	*	*

10 Contents of the EFs

This clause specifies the EFs for the UPT application defining access conditions, data items and coding. A data item is a part of an EF which represents a complete logical entity, e.g. the alpha tag in a EF-Abbreviated Dialling Number (EF_{ADN}) record.

EFs or data items having an unassigned value, or, which during the UPT application, are cleared by the CAD_{UPT}, shall have their bytes set to 'FF'. During the operational phase all data items shall have a defined value or have their bytes set to 'FF'.

EFs are mandatory (M) or optional (O). All implemented EFs shall contain all mandatory data items.

Optional data items may either be filled with 'F', or, if located at the end of an EF, need not exist.

For an overview containing all files see figure 9.

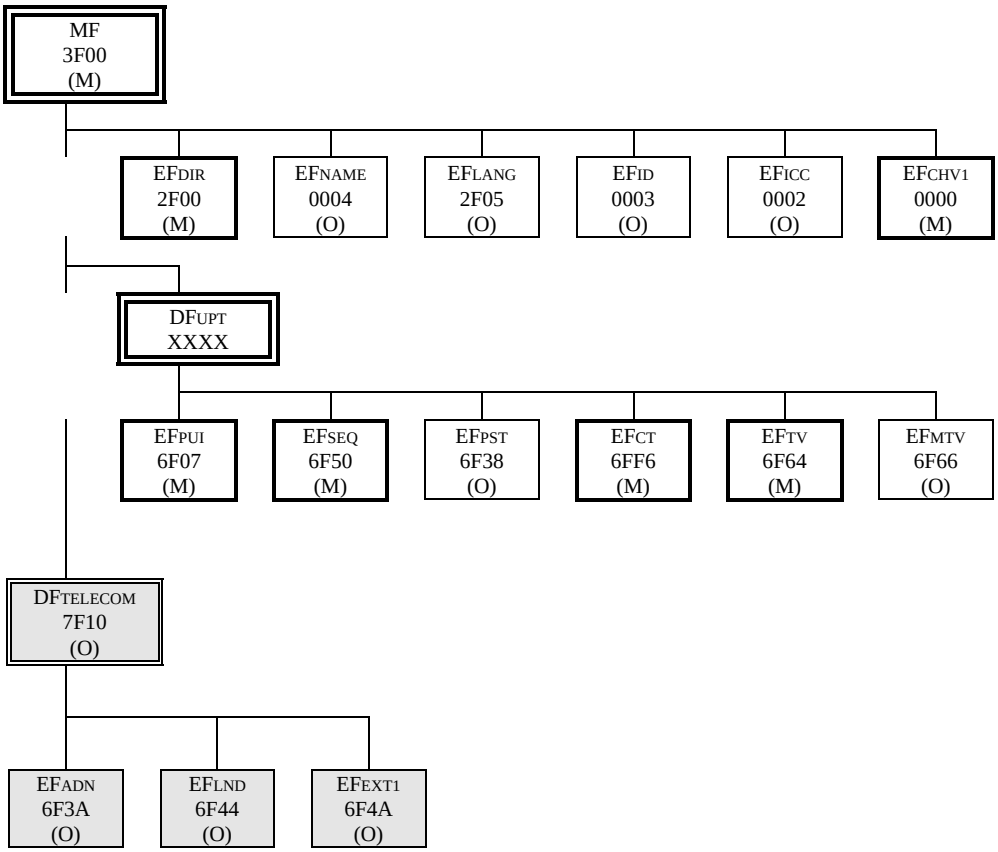


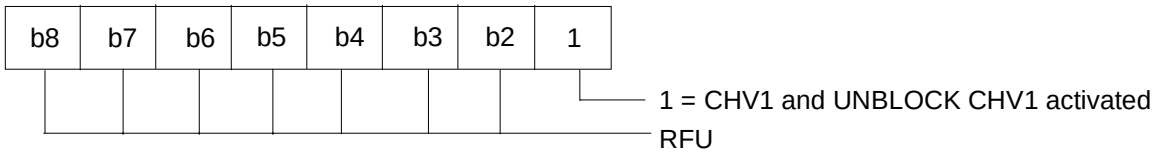
Figure 9

10.1 EF_{CHV1}

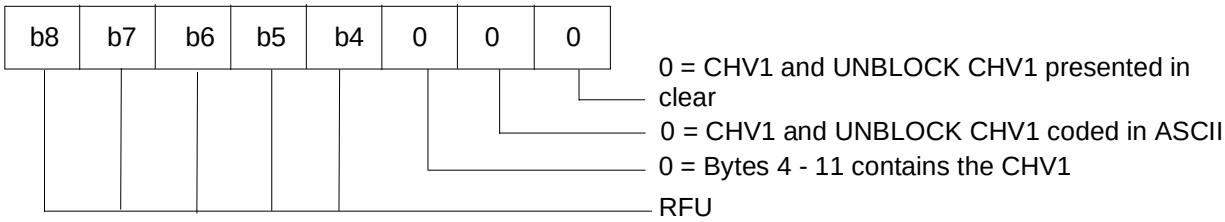
EF_{CHV1} is a transparent file (MF, DF level).

Identifier: '0000'	Structure: transparent		Mandatory
File size: 23 bytes			
Access conditions: READ NEVER UPDATE NEVER			
Bytes	**Description**	**M/O**	**Length**
1	EF_{CHV1} activation byte	M	1 byte
2	Way to present the CHV1/UNBLOCKCHV1	M	1 byte
3	Not used in the UPT application - coded 'FF'	M	1 byte
4 - 11	CHV1	M	8 bytes
12	CHV1 attempts Preset value N	M	1 byte
13	Remaining CHV1 attempt counter	M	1 byte
14 -21	UNBLOCK CHV1	M	8 bytes
22	Remaining UNBLOCK CHV1 attempt counter	M	1 byte
23	Number of remaining UNBLOCK CHV1 mechanism use	M	1 byte

Byte 1: EF_{CHV1} activation byte



Byte 2: Way to present the CHV1 / UNBLOCK CHV1



Byte 4-11: CHV1, 4 to 8 decimal digits, coded in ASCII, right padded with 'FF'.

Byte 12: Preset value:

Byte 12 is set to '03'.

Byte 14-21: UNBLOCK CHV1, 8 decimal digits, coded in ASCII.

Byte 23: Number of remaining UNBLOCK CHV1 mechanism use:

Byte 23 shall be coded 'FF'.

NOTE: This implies that the UNBLOCK CHV1 mechanism may be used an infinite number of times (subject to the correct value being entered).

10.2 Contents of the EFs at the MF level

The EFs at the MF level used by the UPT application during the operational phase are specified here.

10.2.1 EF_{ID}

This EF provides a unique identification number for the PIM.

Identifier: '0003'	Structure: transparent		Optional
File size: 10 to 19 bytes			
Access conditions: READ ALWAYS UPDATE NEVER			
Bytes	**Description**	**M/O**	**Length**
1 - 10	Identification number	M	10 bytes
11 - 13	Date of activation	O	3 bytes
14 - 16	Card expiry date	O	3 bytes
17	Card sequence number	O	1 byte
18 - 19	Country code	O	2 bytes

For the coding of the data items refer to EN 726-3 [14].

These bytes shall not be interpreted by the CAD_{UPT}.

10.2.2 EF_{ICC}

This EF provides a unique identification number for the PIM.

Identifier: '0002'	Structure: transparent		Optional
File size: 15 to 19 bytes			
Access conditions: READ ALWAYS UPDATE NEVER			
Bytes	**Description**	**M/O**	**Length**
1	Clockstop	M	1 byte
2 - 5	IC card serial number	M	4 bytes
6 - 9	IC card manufacturing references ID	M	4 bytes
10	Card personalizer ID	M	1 byte
11 - 15	Embedder/IC assembler ID	M	5 bytes
16 - 17	IC identifier	O	2 bytes
18	Card profile	O	1 byte
19	Type of selection	O	1 byte

For the coding of the data items refer to EN 726-3 [14].

Those bytes shall not be interpreted by the CAD_{UPT}.

10.2.3 EF_{DIR} (Directory)

This EF contains the application identifier for UPT and its relevant path.

Identifier: '2F00'	Structure: transparent		Mandatory
File size: X bytes			
Access conditions: READ ALWAYS or CHV1 UPDATE ADM			
Bytes	**Description**	**M/O**	**Length**
1	Application1 identifier tag '4F'	M	1 byte
2	Application1 identifier length	M	1 byte
3 -	Application1 identifier	M	1 - 16 bytes
	Application1 label tag '50'	M	1 byte
	Application1 label length	M	1 byte
	Application1 label (Verbal description)	M	0 - 16 bytes
	Path tag '51'	M	1 byte
	Path length	M	1 byte
	Path	M	Y bytes
...	...	...	...
	Application identifier tag '4F'	M	1 byte
	UPT Application identifier length	M	1 byte
	UPT Application identifier (see note)	M	1 - 16 bytes
	UPT Application label tag '50'	M	1 byte
	UPT Application label length	M	1 byte
	UPT Application label (Verbal description)	M	0 - 16 bytes
	UPT Path tag '51'	M	1 byte
	UPT Path length	M	1 byte
	UPT Path	M	Z bytes
...	...	...	...

NOTE: The application identifier is administered by ETSI.

In a mono-application card, the UPT application shall be coded in Application 1. In a multi-application card, the UPT application can be coded in any place.

10.2.4 EF_{LANG} (Language preference)

This EF contains the codes for one or more languages. This information, determined by the user/operator, defines the preferred languages of the user in order of priority. This information may be used by the CAD_{UPT} for Man Machine Interface (MMI) purposes.

Identifier: '2F05'	Structure: transparent		Optional
File size: 8 bytes			
Access conditions: READ ALWAYS UPDATE CHV1			
Bytes	**Description**	**M/O**	**Length**
1 - 2	1st language preference	M	2 bytes
3 - 4	2nd language preference	O	2 bytes
5 - 6	3rd language preference	O	2 bytes
7 - 8	4th language preference	O	2 bytes

- Language preference:

purpose: to provide the relevant indication to the CAD_{UPT};
contents: the preferred language;
coding: the representation of the language is coded according to ISO 639 [5] and the characters are coded according to ISO 8859-1 [13].

10.2.5 EF_{NAME}

This EF contains the card holder name.

Identifier: '0004'	Structure: transparent		Optional
File size: X bytes			
Access conditions: READ ALWAYS (note) UPDATE ADM			
Bytes	**Description**	**M/O**	**Length**
1 - X	Card holder name	M	X bytes

NOTE: In EN 726-3 [14] the access condition to READ this file is different.

- Card holder name:

purpose: to provide the relevant indication to the CAD_{UPT};
contents: the name of the card holder;
coding: the card holder name is coded according to ISO 8859-1 [13].

10.3 Contents of files at the UPT application level

The EFs in the UPT Dedicated Files (DF_{UPT}) contain UPT network related information.

10.3.1 EF_{CT}

This EF contains the CT value.

Identifier: '6FF6'	Structure: transparent		Mandatory
File size: 1 byte			
Access conditions: READ CHV1 UPDATE NEVER			
Bytes	**Description**	**M/O**	**Length**
1	CT	M	1 byte

- CT: '2': TESA-7.

'1': USA-4.

'3': All other algorithms.

10.3.2 EF_{PUI} (PUI)

This EF contains the PUI.

Identifier: '6F07'	Structure: transparent		Mandatory
File size: 9 bytes			
Access conditions: READ CHV1 UPDATE ADM			
Bytes	**Description**	**M/O**	**Length**
1	Length of PUI	M	1 byte
2 - 9	PUI	M	8 bytes

- PUI:

coding: Binary Coded Decimal (BCD), left justified and padded with 'F'.

10.3.3 EF_{SEQ} (Sequence number)

This EF contains the sequence number n.

Identifier: '6F50'	Structure: transparent		Mandatory
File size: 8 bytes			
Access conditions: READ CHV1 UPDATE CHV1			
Bytes	**Description**	**M/O**	**Length**
1 - 8	Individual sequence number	M	8 bytes

- Individual sequence number:

purpose: parameter used as challenge to the one pass strong authentication procedure;
contents: individual sequence number;
coding: binary.

10.3.4 EF_{PST} (PIM service table)

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

Table 43: PIM services table

Identifier: '6F38'	Structure: transparent		Optional
File size: 4 bytes			
Access conditions: READ CHV1 UPDATE ADM			
Bytes	**Description**	**M/O**	**Length**
1	Services number 1 to number 4	M	1 byte
2	Services number 5 to number 8	M	1 byte
3	Services number 9 to number 12	M	1 byte
4	Services number 13 to number 14	M	1 byte

- PIM services table:

purpose: to give information on telecom services in the card are offered for UPT;
contents: Service number 1: RFU;
Service number 2: ADN;
Service number 3: RFU;
Service number 4: RFU;
Service number 5: RFU;
Service number 6: RFU;
Service number 7: RFU;
Service number 8: RFU;
Service number 9: RFU;
Service number 10: Extension1;
Service number 11: RFU;
Service number 12: RFU;
Service number 13: LND;
Service number 14: RFU.

NOTE: Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the responsibility of ETSI.

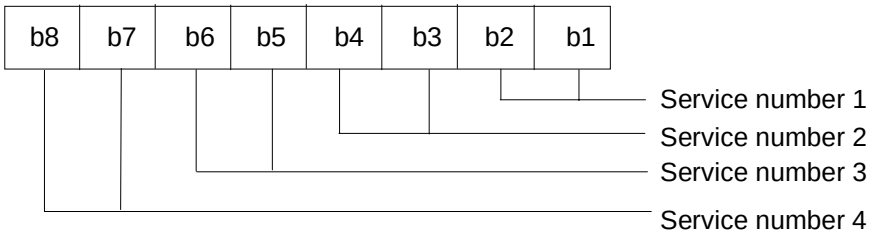
coding: 2 bits are used to code each service:
first bit = 1: service allocated;
first bit = 0: service not allocated,
where the first bit is b1, b3, b5 or b7;
second bit = 1: service activated;
second bit = 0: service not activated,
where the second bit is b2, b4, b6 or b8.

Service allocated means that the PIM has the capability to support the service. Service activated means that the service is available for the card holder (only valid if the service is allocated).

The following coding is possible:

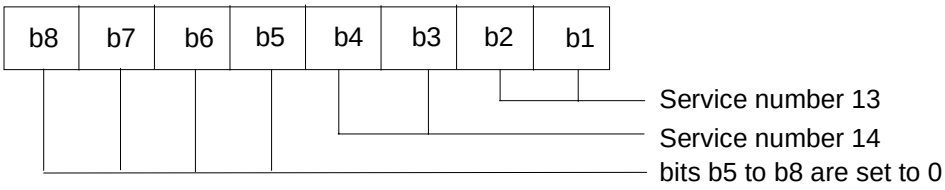
- first bit = 0: service not allocated, second bit has no meaning;
- first bit = 1 and second bit = 0: service allocated but not activated;
- first bit = 1 and second bit = 1: service allocated and activated.

First byte:



etc.

Fourth byte:



The following example of coding for the first byte means that service number 1 "ADN" is allocated but not activated:

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

10.3.5 EF_{TV} (Time-out value)

This EF contains the time-out value. A default value shall be set by the UPT service provider. This value can be changed by the user.

Identifier: '6F64'	Structure: transparent		Mandatory
File size: 2 bytes			
Access conditions: READ CHV1 UPDATE CHV1			
Bytes	**Description**	**M/O**	**Length**
1-2	Number of minutes	M	2 bytes

purpose: to give the time-out value, T, in order to initialize the timer in the CAD_{UPT};
contents: the number of minutes;
coding: binary. The time-out value T= 0 is not allowed. T= FFFF means that no time-out shall occur.

10.3.6 EF_{MTV} (Maximum time-out value)

This EF contains the maximum time-out value specified by the UPT service provider. If EF_{MTV} is not present, then it shall be interpreted that there is no maximum time-out value.

Identifier: '6F66'	Structure: transparent		Optional
File size: 2 bytes			
Access conditions: READ CHV1 UPDATE ADM			
Bytes	**Description**	**M/O**	**Length**
1-2	Number of minutes	M	2 bytes

purpose: to ensure that the UPT service provider specified maximum time-out value, T_{MAX}, is not exceeded;
contents: the number of minutes;
coding: binary. The maximum time-out value T_{MAX} = 0 is not allowed. T_{MAX} = FFFF means that there is no maximum time-out value.

10.4 Contents of files at the telecom level

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

10.4.1 EF_{ADN} (Abbreviated Dialling Numbers)

This EF contains ADNs. In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging.

Identifier: '6F3A'	Structure: linear fixed		Optional
Record size: X+14 bytes			
Access conditions: READ CHV1 UPDATE CHV1			
Bytes	**Description**	**M/O**	**Length**
1 - X	Alpha identifier	O	X bytes
X+1	Length of BCD number	M	1 byte
X+2	Type Of Number (TON) and Numbering Plan Identifier (NPI)	M	1 byte
X+3 / X+12	Dialling number	M	10 bytes
X+13	Not to be interpreted by the CAD_{UPT}	M	1 byte
X+14	Extension1 record identifier	M	1 byte

- Alpha identifier:

contents: alpha-tagging of the associated dialling number;
coding: this alpha-tagging shall use the 7-bit coded alphabet as in CCITT Recommendation T.50 [4] with bit 8 set to 0. Unused bytes shall be set to 'FF'.

NOTE 1: The value of X may be zero. Using the command GET RESPONSE the CAD_{UPT} can determine the value of X.

- Length of BCD number:

contents: this byte gives the number of bytes of the following two data items containing actual BCD number. This means that the maximum value is 11, even when the actual ADN information length is greater than 11. When an ADN requires more than 20 digits it is indicated by the Extension1 identifier being unequal to 'FF'. The remainder is stored in the EF_{EXT1} with the remaining length of the overflow data being coded in the appropriate overflow record itself (see subclause 10.4.3);
coding: BCD.

- TON and NPI:

contents: TON and NPI;
coding: according to EN 726-6 [15].

- Dialling number:

contents: up to 20 digits of the telephone number;
coding: BCD. If the telephone number is longer than 20 digits, the first 20 digits are stored in this data item and the overflow data is stored in an associated record in the EF_{EXT1}. The record is identified by the Extension1 Record Identifier. If ADN require less than 20 digits, excess nibbles at the end of the data item shall be set to 'F'.

Byte X+3;

Byte X+4; etc.

- Extension1 record identifier:

contents: Extension1 record identification byte. This byte identifies the number of a record in the EF_{EXT1} containing an associated called party subaddress or an overflow. The use of this byte is optional. If it is not used it shall be set to 'FF'.
If the ADN requires both overflow and called party subaddress, this byte identifies the overflow record. A chaining mechanism inside EF_{EXT1} identifies the record of the appropriate called party subaddress (see subclause 10.4.3);
coding: binary.

NOTE 2: Since the CAD_{UPT} is not aware of its location, it is not expected to handle international prefixes automatically. Therefore, the user has the following choices:

1) To store numbers in the specific format for each country (not indicating in the TON field that it is an international number). Possible formats are:

International Prefix	Country Code	Area Code	Subscriber Number

or

		Area Code	Subscriber Number

2) To store numbers including the country code (indicating in the TON field an international number). In this case, the international prefix (e.g. '00') is entered manually by the user. A possible format is:

	Country Code	Area Code	Subscriber Number

NOTE 3: When the CAD_{UPT} acts upon the EF_{ADN} with a SEEK command in order to identify a character string in the alpha-identifier, it is the responsibility of the CAD_{UPT} to ensure that the number of characters used as SEEK parameters are less than or equal to the value of X if the MMI allows the user to offer a greater number.

Table 44: Extended coding

BCD value	Character/Meaning
'0'	"0"
...	...
'9'	"9"
'A'	"*"
'B'	"#"
'C'	DTMF Control digit separator
'D'	"Wild" value. This will cause the MMI to prompt the user for a single digit.
'E'	Expansion digit ("Shift Key"). It has the effect of adding '10' to the following digit. The following BCD digit will hence be interpreted in the range of '10'-'1E'. The purpose of digits in this range is for further study.
'F'	End mark e.g. in case of an odd number of digits.

BCD values 'C', 'D' and 'E' are never sent by the CAD_{UPT}.

NOTE 4: The interpretation of values 'D', 'E' and 'F' as DTMF digits is for further study.

NOTE 5: A second or subsequent 'C' BCD value will be interpreted as a 3 second PAUSE.

10.4.2 EF_{LND} (Last number dialled)

This EF contains LNDs. This function is only possible if the last number was dialled by the DTMF device. In this case, this EF contains the LND. In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain associated alpha-tagging.

Identifier: '6F44'	Structure: cyclic		Optional
Record size: X + 14 bytes			
Access conditions: READ CHV1 UPDATE CHV1			
Bytes	**Description**	**M/O**	**Length**
1 - X	Alpha identifier	O	X byte
X + 1	Length of BCD number	M	1 byte
X + 2	TON and NPI	M	1 byte
X + 3/X + 12	Dialling Number	M	10 bytes
X + 13	not to be interpreted by the CAD_{UPT}	M	1 byte
X + 14	Extension1 record identifier	M	1 byte

Contents and coding: see EF_{ADN}.

NOTE: The value of X shall be equal to the value of X in EF_{ADN}. Using the command GET RESPONSE the CAD_{UPT} can determine the value of X.

10.4.3 EF_{EXT1} (Extension1)

This EF contains extension data of an ADN or of a LND. Extension data is caused by:

- an ADN or a LND which is greater than the 20 digit capacity of the ADN EF resp. of the LND EF. The remainder is stored in this EF as a record, which is identified by a specified identification byte inside the ADN EF resp. the LND EF. The EXT1 record in this case is specified as overflow data;
- an associated called party subaddress. The EXT1 record in this case is specified as subaddress data.

Identifier: '6F4A'	Structure: linear fixed		Optional
Record size: 13 bytes			
Access conditions: READ CHV1 UPDATE CHV1			
Bytes	**Description**	**M/O**	**Length**
1	Record type	M	1 byte
2 - 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

- Record type:

contents: type of the record;
coding:

b3-b8 are reserved and set to 0;

a bit set to 1 identifies the type of record;

only one type can be set;

'00' indicates the type "unknown".

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

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

- Extension data:

contents: overflow data or called party subaddress depending on record type;
coding: Case 1, Extension1 record is overflow data:
The first byte of the extension data gives the number of bytes of the remainder of ADN (resp. LND). The coding of remaining bytes is BCD, according to the coding of ADN (resp. LND). Unused nibbles at the end have to be set to 'F'. It is possible if the number of overflow digits exceeds the capacity of the overflow record to chain another record inside the EXT1 EF by the identifier in byte 13.
Case 2, Extension1 record is called party subaddress:
For a Called Party Subaddress two extension records have to be used, which are chained by the identifier field. The extension record containing the first part of the called party subaddress points to the record which contains the second part of the subaddress.

- Identifier:

contents: identifier of the next extension record to enable storage of information longer than 11 bytes;
coding: record number of next record. 'FF' identifies the end of the chain.

EXAMPLE: A chain of extension records being associated to an ADN. The Extension1 record identifier (Byte 14 + X) of ADN is set to 3.

No of Record Type Extension Data Next Record
. . . .
. . . .
Record 3 '02' xx .....xx '06' >----------¦
Record 4 'xx' xx .....xx 'xx' ¦
Record 5 '01' xx .....xx 'FF' <----------¦
Record 6 '01' xx .....xx '05' <----------¦
. . . .
. . . .

In this example ADN is associated to an overflow (record 3) and a called party subaddress (records 6 and 5).

11 Application protocol

The application protocol is the information exchange between the PIM and the CAD_{UPT} that starts after the ATR - PTS procedure.

When involved in UPT card administrative management operations, the PIM interfaces with appropriate terminal equipment. These operations are outside the scope of the present document.

When involved in UPT network operations the PIM interfaces with a CAD_{UPT} with which messages are exchanged. A message can be a command or a response:

- a UPT command/response pair is a sequence consisting of a command and the associated response;
- a UPT procedure consists of one or more UPT command/response pairs which are used to perform all or part of an application-oriented task. A procedure shall be considered as a whole, that is to say that the corresponding task is achieved if and only if the procedure is completed. The CAD_{UPT} shall ensure that, when operated according to the manufacturer's manual, any unspecified interruption of the sequence of command/response pairs which realize the procedure, leads to the abortion of the procedure itself;
- a UPT session of the PIM in the UPT application is the interval of time starting at the completion of the PIM initialization procedure and ending either with the start of the UPT session termination procedure, or at the first instant the link between the PIM and the CAD_{UPT} is interrupted.

During the UPT network operation phase, the CAD_{UPT} plays the role of the master and the PIM plays the role of the slave.

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

Some procedures are automatically initiated by the CAD_{UPT} and these procedures will not require any MMI interaction at all. They are marked "CAD" in the list given below.

The list of procedures at the PIM/CAD_{UPT} interface in UPT network operation is as follows.

General procedures:

- reading an EF CAD
- updating an EF CAD
- seek in an EF CAD
- select an EF or DF CAD

PIM management procedures:

- PIM session initialization CAD/MMI
- PIM session CAD
- PIM session termination CAD/MMI
- application selection procedure CAD
- Timer value substitution MMI
- Start Timer CAD

CHV related procedures:

- CHV verification CAD/MMI
- CHV value substitution MMI
- CHV unblocking MMI

UPT security related procedures:

- one pass strong authentication MMI

General telecommunication procedures:

- dialling numbers (ADN and LND) MMI/CAD

General information procedures:

- language request/update procedures CAD/MMI
- name request procedure CAD/MMI

The procedures listed in subclause 11.2 are required for every UPT session. If a procedure is related to a specific service indicated in table 43, it shall only be executed if the corresponding bits denote this service as "allocated and activated" (see subclause 10.2.4). In all other cases this procedure shall not start.

The figures describing the procedures are for information.

NOTE: Other functions may be included where appropriate.

If an error occurs, the procedure can be interrupted and aborted before it reaches its end. If an optional EF cannot be found in the PIM, it shall never cause the CAD_{UPT} to treat this as an error condition.

If a procedure is interrupted by MMI interaction, the function shall not be aborted before it reaches its completion, and the rest of the procedure is then aborted before the normal ending.

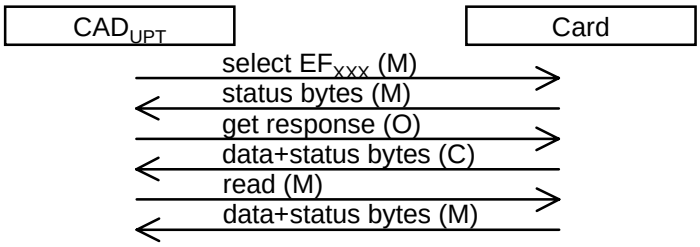
The letter in parentheses within the header indicates:

- (M) for mandatory, meaning that this procedure shall be implemented in the PIM;
- (O) for optional, meaning that implementation is up to the application provider/terminal manufacturer;
- (C) for conditional, the applicable condition(s) is given at the end of the figure.

11.1 General procedures

These procedures are general, which means that they are used in the same way for different EFs.

11.1.1 Reading an EF (M)

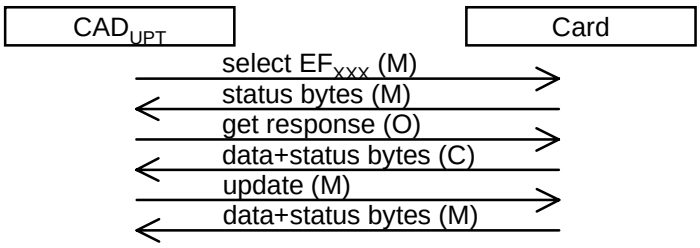


C: Always if the get response command is used.

Figure 10

The EF shall be successful selected before the CAD_{UPT} sends a READ command. If the access condition for READ is fulfilled, the PIM sends the requested data contained in the EF to the CAD_{UPT}. If the access condition is not fulfilled, no data will be sent and an error code will be returned.

11.1.2 Updating an EF (M)

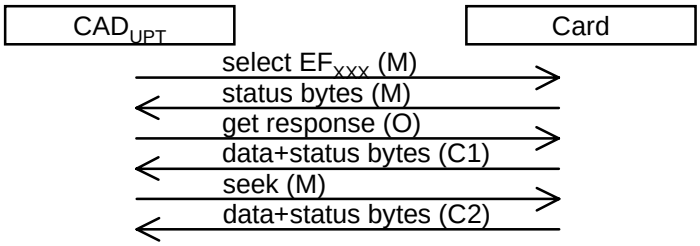


C: Always if the get response command is used.

Figure 11

The EF shall be successful selected before the CAD_{UPT} sends an UPDATE command containing the data to be stored. If the access condition for UPDATE is fulfilled, the PIM updates the selected EF by storing the presented data. If the access condition is not fulfilled, the data existing in the EF will remain unchanged, the new data will not be stored, and an error code will be returned.

11.1.3 Seeking in an EF (O)

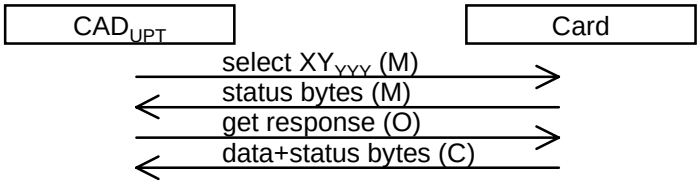


C1: Always if the get response command is used.
C2: The return of the data is dependant upon the type of seek used.

Figure 12

The EF shall be successful selected before the CAD_{UPT} sends a SEEK command containing the data to be seeking for. If the access condition for SEEK is fulfilled, the PIM seeks for the given data pattern in the selected EF. If the access condition is not fulfilled, no seek will be performed and an error code will be returned.

11.1.4 Selecting an EF or DF (M)



C: Always if the get response command is used.

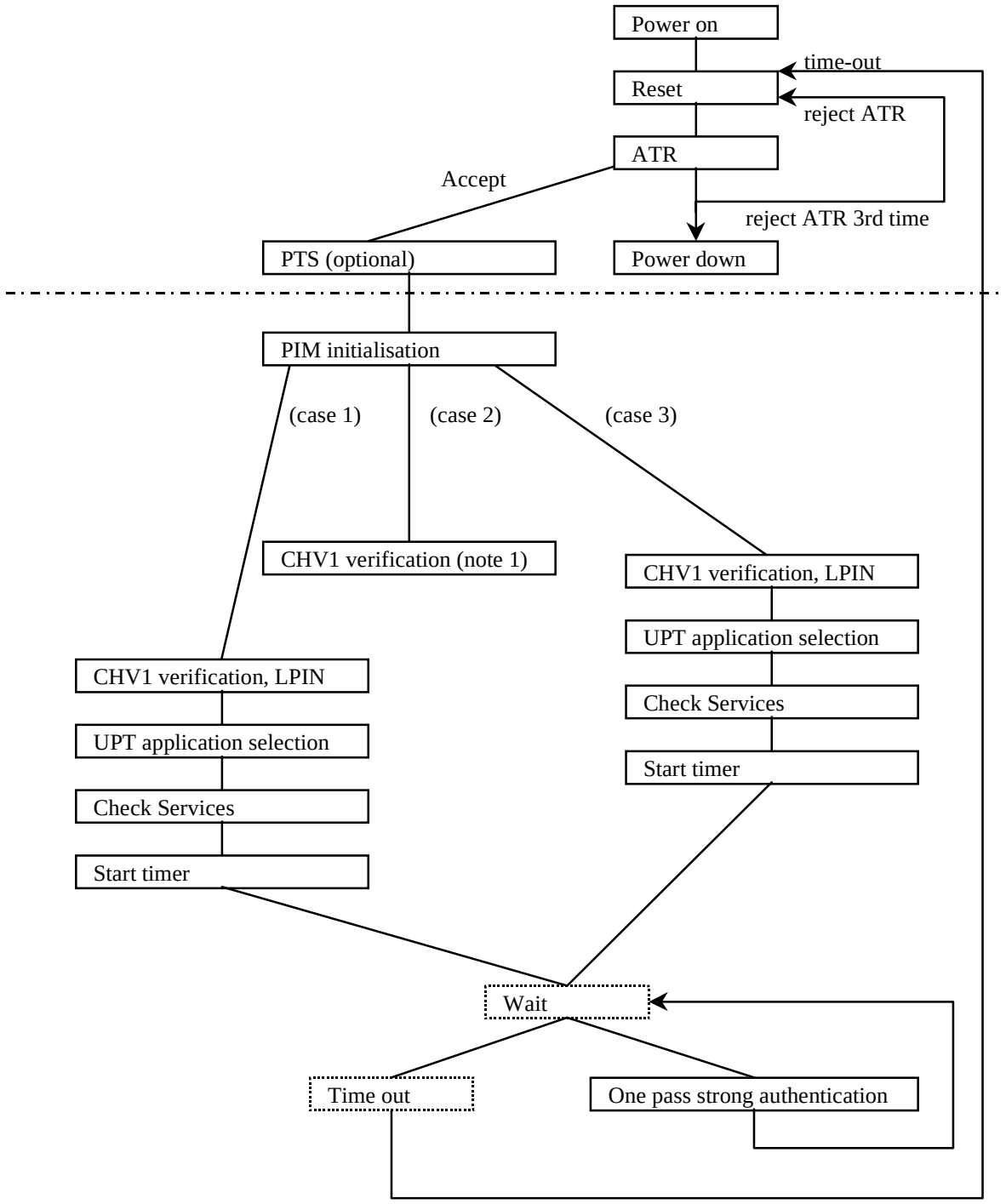
Figure 13

The CAD_{UPT} sends an SELECT command containing the file identifier of the file to select. The response will have the status information of the selected file.

11.2 PIM management procedures

These procedures are relating specifically to the UPT application.

Figure 14 outlines the procedures in a normal UPT session.



NOTE 1: This procedure is only needed if the EF_{DIR} is CHV1 protected.
NOTE 2: The dotted lined boxes refer to CAD_{UPT} internal procedures and are included for clarification.
NOTE 3: The procedures above the dotted line are not part of the application protocol, but included for clarification.

Figure 14: Procedure flow chart

11.2.1 PIM initialization (M)

The CAD_{UPT} selects the MF.

NOTE: This is to be sure that the MF is the current working directory in case the MF is not implicitly selected after the ATR, e.g. in a multi-application card.

The response to the select of the MF may be investigated to initialize the clock stop. The response to the select to the MF also gives the information about the appearance of a CHV1 at this level and information whether it is disabled or not.

Optionally the CAD_{UPT} can perform the name request procedure.

After the MF selection, the CAD_{UPT} selects the EF_{LANG} and requests the language preference. If this EF is not available or the languages in the EF are not supported then the CAD_{UPT} selects a default language.

The CAD_{UPT} performs a select procedure on EF_{CHV1}. If a CHV1 is present, the CAD_{UPT} investigates the response to see whether a disabling of the CHV1 is allowed.

NOTE: For this procedure, refer to figure 14. The normal ending of the PIM initialization procedure gives three possibilities to proceed (see figure 15).

Case 1: There is no CHV1 at the MF level or the CHV1 at the MF level is disabled. The UPT application selection procedure is performed followed by the CHV1 verification (LPIN) procedure. This case is ended with that the timer is started in the CAD_{UPT}. The PIM is now ready for the UPT session.

Case 2: There is a CHV1 at the MF level where the disabling is allowed, but it is not disabled. The CHV1 verification procedure is only performed if it is necessary to perform the UPT application selection procedure. The rest of the procedure is identical to the case above, first run the UPT application selection procedure, then run the CHV1 verification (LPIN) procedure. End by starting the timer in the CAD_{UPT}. The PIM is now ready for the PIM session.

Case 3: There is a CHV1 at MF level which does not allow the disable/enable function. The CHV1 verification procedure is performed as the LPIN presentation. After that the UPT application selection is performed and then the timer is started in the CAD_{UPT}. The PIM is now ready for a PIM session.

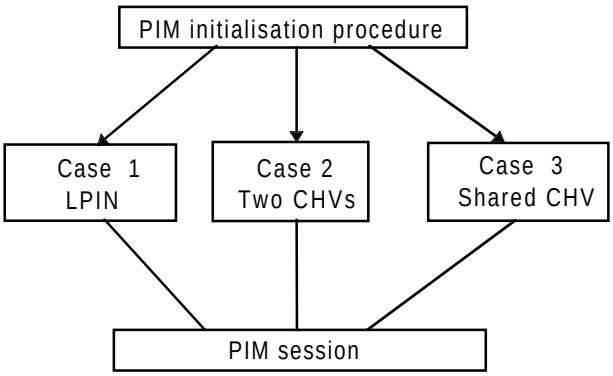
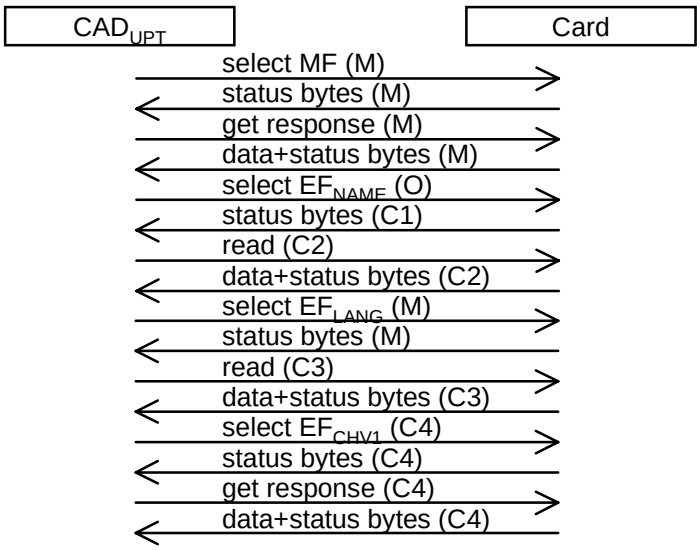


Figure 15: The 3 different cases of how to get from the PIM initialization procedure to the PIM session



C1: Mandatory if the above command is performed.
C2: Mandatory if the response to the selection of EF_{NAME} is normal ending of command.
C3: Mandatory if the select of EF_{LANG} is performed and the response to it is normal ending of the command
C4: Mandatory if there is a CHV1 at the MF level and it is not disabled.

Figure 16: Proposed flow of the commands and responses

11.2.2 PIM session (M)

After the PIM initialization has been completed successfully, the application selection and CHV1 verification shall be performed (not necessarily in this order, see note above), followed by the check services procedure and the start timer procedure. Then the CAD_{UPT} is ready for a PIM session.

A PIM session can consist of the following procedures:

- timer value substitution (O);
- CHV unblocking (O);
- one pass strong authentication (M);
- language preference update procedure (O);
- dialling number procedures (O);
- CHV1(LPIN) substitution procedure (O).

The procedures listed above may be executed in any order.

All procedures in the PIM session are initiated by the user.

NOTE: No command-response figures are included in this subclause. The information needed can be achieved by adding the figures from the involved procedures described below.

11.2.3 PIM session termination (M)

NOTE 1: This procedure should not be confused with the de-activation procedure given in subclause 4.3.2.

The UPT session may be terminated by one of the following actions:

1) the termination is done automatically by a time-out of the timer in the CAD_{UPT}. When the timer reaches its time out value before the one pass strong authentication procedure is performed, the CAD_{UPT} shall make a hardware reset on the PIM;

NOTE 2: This can only be done in a mono-application card or in a multi-application card where only the UPT application is open. This is always the case in CAD_{UPT}s.

2) the PIM is removed from the CAD_{UPT};

3) a reset signal is given at contact C6;

4) the power to the card is switched off by deactivating of the contacts.

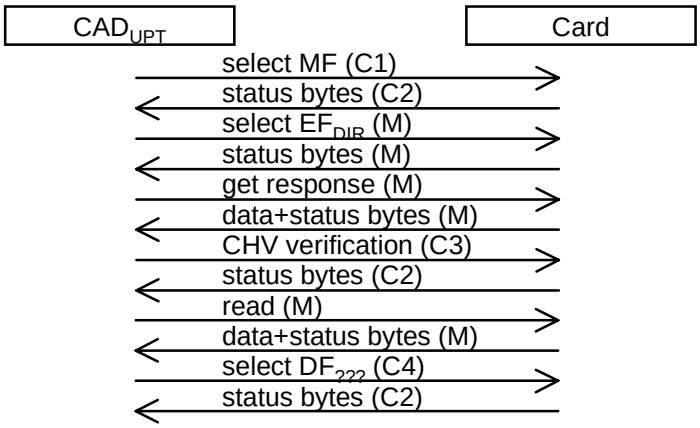
After executing the UPT session termination procedure all values relating to the authentication process shall be deleted from the CAD_{UPT}.

11.2.4 Application selection procedure (M)

The CAD_{UPT} selects the MF (if this is not already the current DF). Then the CAD_{UPT} selects EF_{DIR}.

NOTE: A CHV1 verification procedure may be needed before the read procedure can be performed.

The CAD_{UPT} performs the read procedure with EF_{DIR}. Then each DF in the obtained path is selected in order to select the UPT (or other) application in DF_{UPT}.

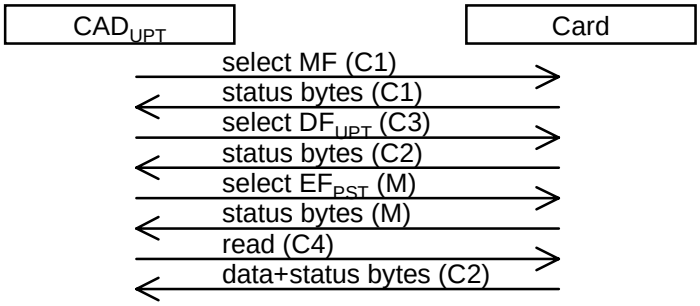


C1: (M) if the current DF is not the MF, else it is not needed.
C2: (M) if the previous command is performed.
C3: (M) if the access condition CHV1 is not fulfilled.
C4: (M) this shall be repeated for each file ID contained in the path to the wanted application.

Figure 17

11.2.5 Check services (M)

The CAD_{UPT} selects the DF_{UPT} via selecting Masterfile unless DF_{UPT} is already selected. The CAD_{UPT} sends a select command for EF_{PST}. If EF_{PST} does not exist the procedure is aborted. Otherwise the CAD_{UPT} reads the content of EF_{PST}.



C1: (M) if the current DF is not the MF and not the DF_{UPT}, else it is not needed.
C2: (M) if the previous command is performed.
C3: (M) if the current DF is not the DF_{UPT}, else it is not needed.
C4: (M) if the EF_{PST} exist.

Figure 18

11.2.5A Start timer

In case of a successful LPIN Verification, the user specified time-out value T shall be read out from the EF_{TV}.

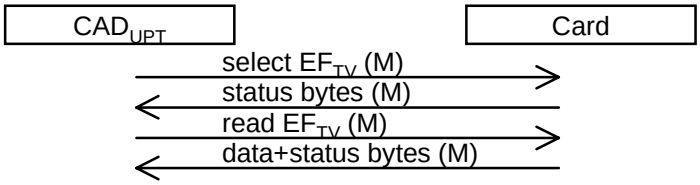
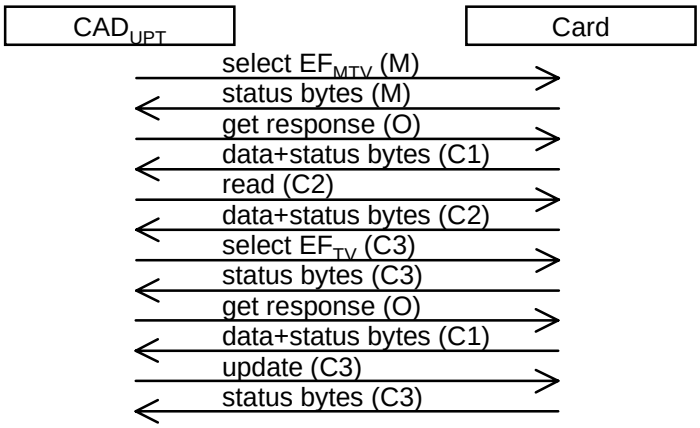


Figure 19

NOTE: The timer is initialized with the time-out value T and started if T≠'FFFF'.

11.2.6 Timer value substitution (O)



C1: Always if the get response command is used.
C2: Mandatory if the EF_{MTV} is present.
C3: Mandatory if the new value T, presented by the user, is greater than 0, but not greater than the maximum time-out value T_{MAX}, stored in EF_{MTV} (if present).

Figure 20

This procedure is performed by the user to change the time-out value T. The CAD_{UPT} selects EF_{MTV} and obtains the maximum time-out value. If the value presented by the user is greater than 0, but not greater than the value T_{MAX} specified in EF_{MTV}, then the CAD_{UPT} selects EF_{TV} and updates it with the value presented by the user. Otherwise, the procedure is terminated unsuccessfully.

11.3 CHV related procedures

A successful completion of one of the following procedures grants the access right by the corresponding CHV1 for the UPT session if performed on the relevant CHV1 for the UPT application. This means that the corresponding access right is valid for all files protected by this CHV1. This also grants the right to perform a successful INTERNAL AUTHENTICATION.

After the third consecutive presentation of a wrong CHV1 value to the PIM (not necessarily in the same card session), the respective CHV1 becomes "blocked" and the access right previously granted by this CHV1 is lost immediately.

After the tenth consecutive presentation of a wrong UNBLOCK CHV, not necessarily in the same card session, the respective UNBLOCK CHV value gets irreversibly blocked, and the UNBLOCK CHV function can never be successfully performed again.

If a procedure is aborted for any reason, the completion is not successful. An unsuccessful completion of any of the following procedures does not grant any access right.

NOTE: It is not necessary to select the relevant EF_{CHV} to perform CHV procedures.

11.3.1 CHV verification (M)

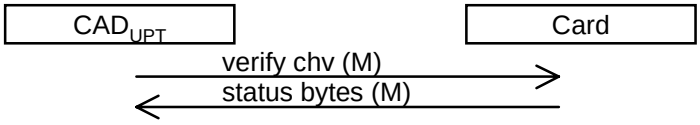


Figure 21

The CAD_{UPT} checks the CHV status. If the CHV status is set to "blocked", i.e. the number of remaining false CHV presentations is 0, the procedure is terminated unsuccessfully.

If the CHV status is not "blocked" and the enabled/disabled indicator set "enabled" (this shall always be the case in the UPT application), the CAD_{UPT} uses the VERIFY CHV function. If the CHV value presented by the CAD_{UPT} is equal to the corresponding CHV value stored in the respective EF_{CHV}, the procedure is finished successfully; otherwise, the function is terminated unsuccessfully.

11.3.2 CHV value substitution (O)

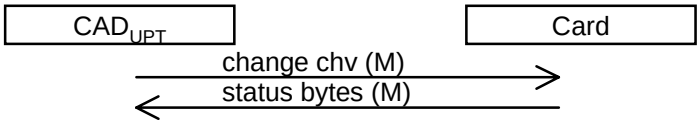


Figure 22

To ensure that only the LPIN can be changed when the PIM is placed in the CAD_{UPT}, this procedure shall only be performed when DF_{UPT} is selected.

The CAD_{UPT} checks the CHV status. If the CHV status is "blocked", i.e. the number of remaining false CHV presentations is 0, the procedure is terminated unsuccessfully.

If the CHV status is not "blocked" and the enabled/disabled indicator set to "enabled" (this shall always be the case in the UPT application), the CAD_{UPT} uses the CHANGE CHV function. If the old CHV1 value presented by the CAD_{UPT} is equal to the corresponding CHV1 value stored in the respective EF_{CHV}, the new CHV1 value is stored in the PIM in the respective EF_{CHV} and the procedure is terminated successfully.

If the presented old CHV1 value and the CHV1 value stored in the PIM are not identical, then the card holder verification is terminated unsuccessfully.

11.3.3 CHV unblocking (O)

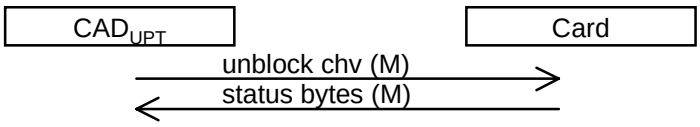


Figure 23

The execution of the CHV unblocking procedure is independent of the corresponding CHV status, i.e. being blocked or not.

The CAD_{UPT} checks the UNBLOCK CHV status. If the UNBLOCK CHV status is set to "blocked", the procedure is terminated unsuccessfully.

If the UNBLOCK CHV status is not "blocked", the CAD_{UPT} uses the UNBLOCK CHV function. If the UNBLOCK CHV value presented by the CAD_{UPT} is equal to the corresponding UNBLOCK CHV value stored in the respective EF_{CHV}, the relevant CHV status is set to "unblocked", and the procedure is terminated successfully. If the UNBLOCK CHV value presented by the CAD_{UPT} is not equal to the UNBLOCK CHV value stored in the relevant EF_{CHV}, the CHV status shall remain "blocked" and the procedure is terminated unsuccessfully.

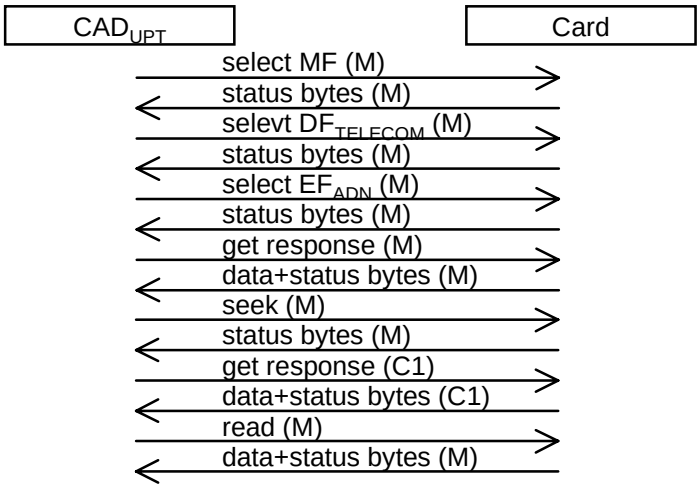
11.4 UPT security related procedures

Only one UPT security related procedure is recognized for the PIM. The mechanism is specified in clause 7.

- one pass strong authentication.

The specification of the data elements used in the authentication procedure can be found in ETS 300 391-1 [2].

NOTE: It is possible to select EF_{ADN} and to read out the service provider's telephone number before running the one pass strong authentication procedure. This makes it possible to automatically dial the service provider by use of the telecom features in the PIM.



C1: (M) if type 2 seek is used, else it is not needed.

NOTE: The following assumption is made: the DF_{UPT} and $DF_{TELECOM}$ are placed directly under the MF.

Figure 24

11.4.1 One pass strong authentication (M)

This procedure is used by the PIM to authenticate itself to the network.

Before this procedure can be performed, a successful CHV1 procedure shall be completed:

1) the CAD_{UPT} selects and reads $EF_{CT;}$
2) the CAD_{UPT} selects and reads EF_{PUI};
3) the CAD_{UPT} selects and reads EF_{SEQ};
4) the CAD_{UPT} obtains n_s which is the 16 least significant bits of n (see ETS 300 391-1 [2]);
5) the CAD_{UPT} gives a INTERNAL AUTHENTICATION command with previous read sequence number (n) as a challenge to the command. Then the PIM calculates an AC, which is returned in the response from the PIM to the CAD_{UPT};
6) the CAD_{UPT} increments the sequence number (n);
7) the CAD_{UPT} performs an update on EF_{SEQ} with the new value of the sequence number (n);
8) the CAD_{UPT} sends PUI, CT, n_s and AC to the network.

Steps 4), 6) and 8) are not part of the protocol between the CAD_{UPT} and the PIM, but are included for clarification.

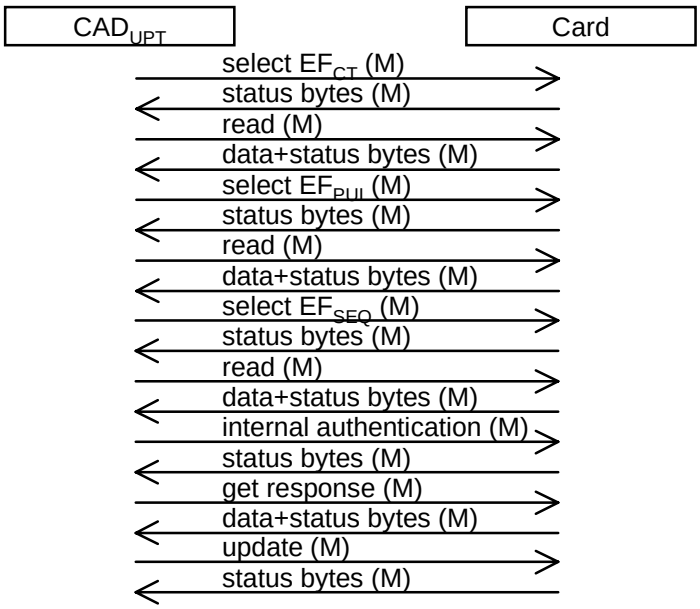


Figure 25

11.5 Telecom procedures (O)

This is the part describing the functionality of the telecom features which can be used in the PIM.

Before the procedures described below can be executed, the telecom directory ($DF_{TELECOM}$) needs to be selected. The following is a short list of actions:

- select MF;
- select $DF_{TELECOM}$ (using of the whole application selection procedure is not necessary because the content of EF_{DIR} is already read by the CAD_{UPT});
- if $DF_{TELECOM}$ has its own CHV, then card holder verification is needed.

NOTE: To clarify the use of the CHV: $DF_{TELECOM}$ can have its own CHV, meaning that an EF_{CHV1} shall reside under $DF_{TELECOM}$, or it can be shared with the UPT application meaning that the (only) EF_{CHV1} shall reside under the MF. The latter should always be the case in mono-application cards. There is also a third possibility, where an EF_{CHV1} resides under $DF_{TELECOM}$, DF_{UPT} and the MF. This means that the user can be asked to enter three different CHVs to use the PIM, which should be avoided.

11.5.1 Dialling numbers

The PIM can contain a list of ADNs in the file EF_{ADN}. The PIM also offers the opportunity to have the LND information stored inside the PIM, this is only possible with the last numbers dialled by the DTMF device. The LND information is stored in EF_{LND}.

The following procedures may only be applied to the EFs EF_{ADN}, EF_{LND} and EF_{EXT1} as shown in the procedures below. They apply to ADN and LND.

Requirement: service n°2 for ADN or service n°13 for LND "allocated and activated".

11.5.1.1 Update

The CAD_{UPT} analyses and assembles the information to be stored as follows (the byte identifiers used below correspond to those in the description of the EFs given in subclauses 10.4.1, 10.4.2 and 10.4.3):

a) the CAD_{UPT} identifies the alpha-tagging and Extension 1 record identifier;

b) the dialling number string shall be analysed and allocated to the bytes of the EF as follows:

- if the dialling number starts with a "+", the TON identifier is set to 'International';
- if 20 or less "digits" remain, they shall form the dialling number string;
- if more than 20 "digits" remain, the procedure shall proceed as follows:

  requirement: service n°10 "allocated and activated".

  The CAD_{UPT} seeks for a free record in the EF_{EXT1}. If an Extension1 record is not marked as "free", the CAD_{UPT} runs the purge procedure, specified in subclause 11.5.1.4. If an Extension1 record is still unavailable, the procedure is aborted.

  The first 20 "digits" are stored in the dialling number string. The value of the length of the dialling number string 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 "overflow data". The first byte of the Extension1 record is set with the number of bytes of the remaining overflow data. The number of bytes containing digit information is the sum of the length of the dialling number string of the EF_{ADN} or EF_{LND} and byte 2 of all associated chained Extension1 records containing overflow data (see subclauses 10.4.1 and 10.4.3);

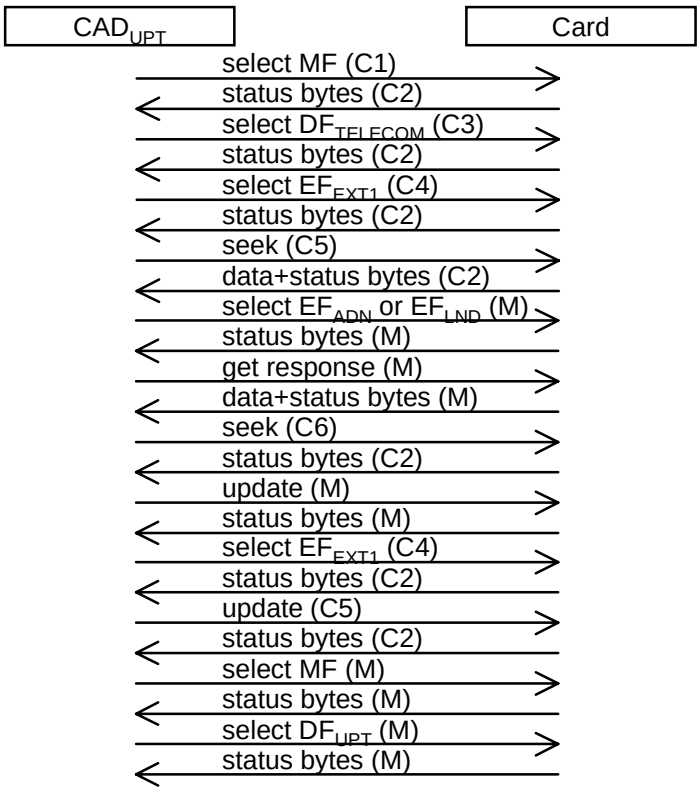
c) if a called party subaddress is associated to the ADN resp. to the LND, the procedure shall proceed as follows:

  requirement: service n°10 "allocated and activated".

  The CAD_{UPT} seeks for two free records in the Extension1 data field. If no such two Extension1 records are found, the CAD_{UPT} runs the purge procedure, specified in subclause 11.5.1.4. If two Extension1 records are still unavailable, the procedure is aborted.

  The CAD_{UPT} stores the called party subaddress in the two Extension1 records.

If the PIM has no available empty space to store the received ADN resp. the received LND, or if the procedure has been aborted, the CAD_{UPT} advises the user. For the LND it is not necessary to find a "free" record in EF_{LND} because the oldest record will be updated.



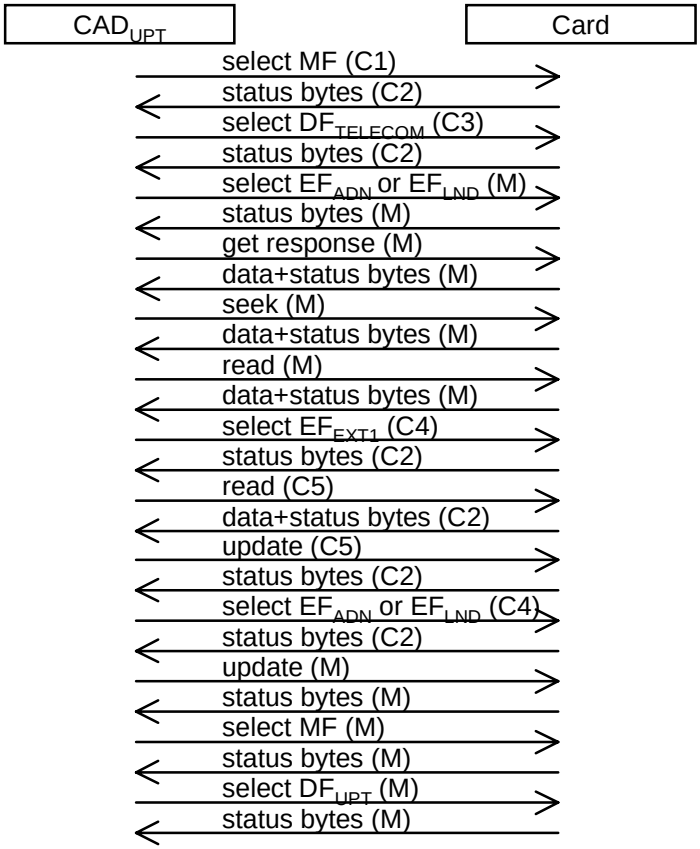
C1: (M) if the current DF is not the MF and not the $DF_{TELECOM}$, else it is not needed.
C2: (M) if the previous command is performed, else it shall never be performed.
C3: (M) if the current DF is not the $DF_{TELECOM}$, else it is not needed.
C4: (M) if more than 20 digits remains or a called party subaddress is associated to this dialling number, then a link to EF_{EXT1} is needed, else it is not needed.
C5: (M) if there is a link to EF_{EXT1}, else it is not needed. This part can be repeated if the chain has more links.
C6: (M) if the file is EF_{ADN}, else it is not needed. (In case of EF_{LND} the oldest record will be updated even though it is not a free one.)

NOTE: For reasons of memory efficiency, the CAD_{UPT} is allowed to analyse all Extension1 records to recognize if the overflow or subaddress data to be actually stored already exists in the EF_{EXT1}. If so, the CAD_{UPT} may use an existing chain or part of an existing chain up to the end for multiple access. The CAD_{UPT} is only allowed to store the actual extension data in unused records. If existing records are used for multiple access, the CAD_{UPT} should not change any data in those records to prevent corruption of existing chains.

Figure 26

11.5.1.2 Erasure

The CAD_{UPT} sends the identification of the requested information to be erased. This identification may be an alphanumeric pattern contained in the EF_{ADN} resp. in the EF_{LND}. The PIM seeks for the identified ADN resp. LND. If an ADN resp. a LND is found, the CAD_{UPT} asks the user for confirmation of the erasure. Depending on the confirmation, the CAD_{UPT} performs the updating procedure with EF_{ADN} resp. EF_{LND}. If the ADN resp. LND is not to be erased, the CAD_{UPT} requests again the PIM for a further ADN resp. LND corresponding to the same identification or aborts this procedure.



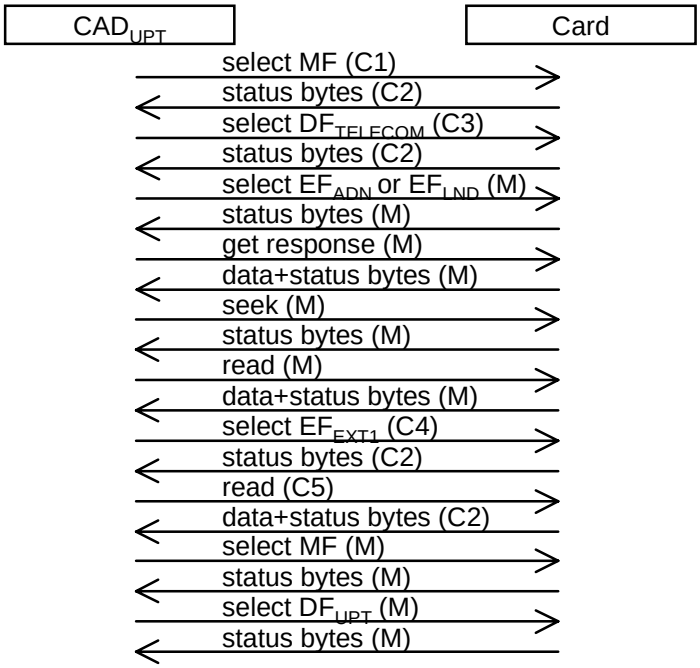
C1: (M) if the current DF is not the MF and not the $DF_{TELECOM}$, else it is not needed.
C2: (M) if the previous command is performed, else it shall never be performed.
C3: (M) if the current DF is not the $DF_{TELECOM}$, else it is not needed.
C4: (M) if there is a link to EF_{EXT1}, else it is not needed.
C5: (M) if there is a link to EF_{EXT1}, else it is not needed. This part can be repeated if the chain has more links.

NOTE: The following assumption is made: The user confirms the erasure.
(If the user rejects the erasure, if the user ask for a further seeking and if the currently indicated number has no extensions, the procedure has to go on with "seek".
If the user rejects the erasure, if the user ask for a further seeking and if the currently indicated number has extensions, the procedure has to go on with "select EF_{ADN} or EF_{LND}" at the beginning.)

Figure 27

11.5.1.3 Request

The CAD_{UPT} sends the identification of the requested information to be read. This identification may be an alphanumeric pattern contained in the EF_{ADN} resp. in the EF_{LND}. The PIM seeks for the identified ADN resp. LND. If the ADN resp. LND is found, the CAD_{UPT} analyses the contents of the ADN record resp. of the LND record according to subclauses 10.4.1 and 10.4.3 and presents it to the user. If the identified ADN resp. LND is not found, the CAD_{UPT} advises the user.



C1: (M) if the current DF is not the MF and not the $DF_{TELECOM}$, else it is not needed.
C2: (M) if the previous command is performed, else it shall never be performed.
C3: (M) if the current DF is not the $DF_{TELECOM}$, else it is not needed.
C4: (M) if there is a link to EF_{EXT1}, else it is not needed.
C5: (M) if there is a link to EF_{EXT1}, else it is not needed. This part can be repeated if the chain has more links.

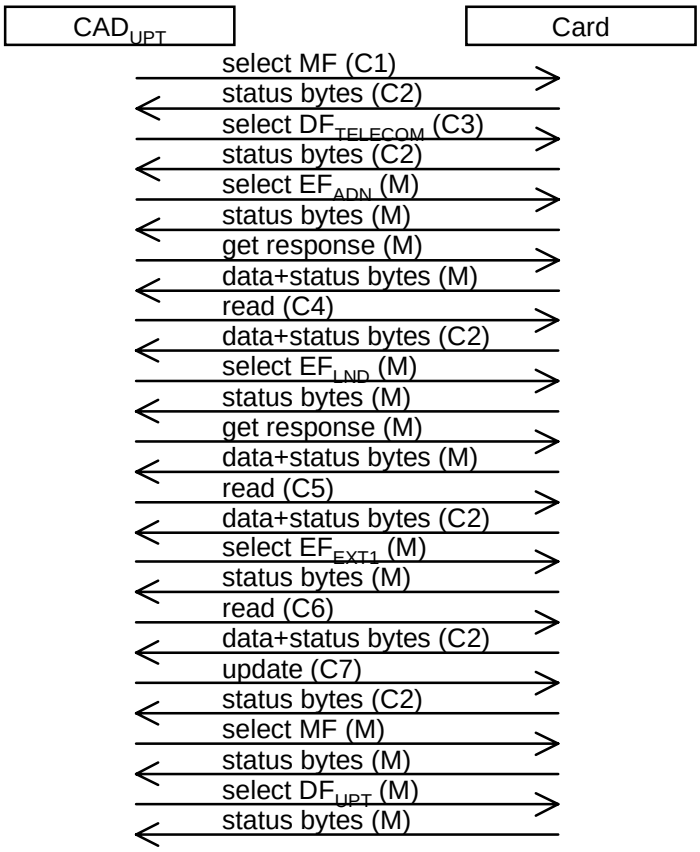
Figure 28

11.5.1.4 Purge

The CAD_{UPT} shall access each EF which references EF_{EXT1} for storage and shall identify records in these files using extension data (overflow data or called party subaddress).

NOTE: Existing chains have to be followed to the end.

All referred Extension1 records are noted by the CAD_{UPT}. All Extension1 records not noted are then marked by the CAD_{UPT} as "free" by setting the whole record to 'FF'.



C1: (M) if the current DF is not the MF and not the $DF_{TELECOM}$, else it is not needed.
C2: (M) if the previous command is performed, else it shall never be performed.
C3: (M) if the current DF is not the $DF_{TELECOM}$, else it is not needed.
C4: (M) this has to be done for every record of EF_{ADN}.
C5: (M) this has to be done for every record of EF_{LND}.
C6: (M) if there is extension indicated in EF_{ADN} or EF_{LND}. This can be carried multiple times to get to the end of all chains.
C7: (M) if there are records in EF_{EXT1}, which are not indicated within chains. This part can be repeated if there are many of these records.

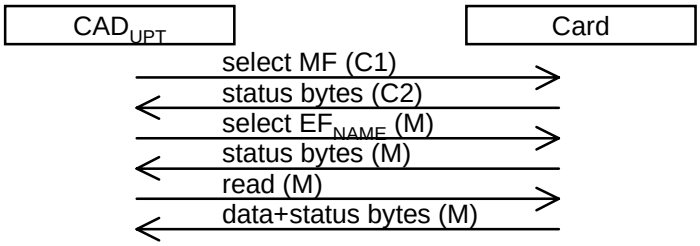
Figure 29

11.6 General information procedures

These optional procedures may be used to read/update EFs at the MF level.

11.6.1 NAME request procedure (O)

The CAD_{UPT} performs the select procedure followed by the read procedure with EF_{NAME}.



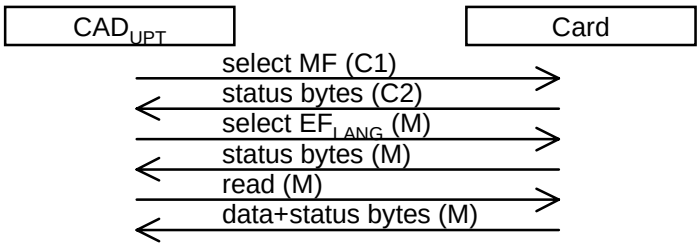
C1: (M) if the current DF is not the MF, else it is not needed.
C2: (M) if the previous command is performed.

Figure 30

11.6.2 Language preference procedures (O)

11.6.2.1 Request

The CAD_{UPT} performs the select procedure, followed by the read procedure with EF_{LANG}.

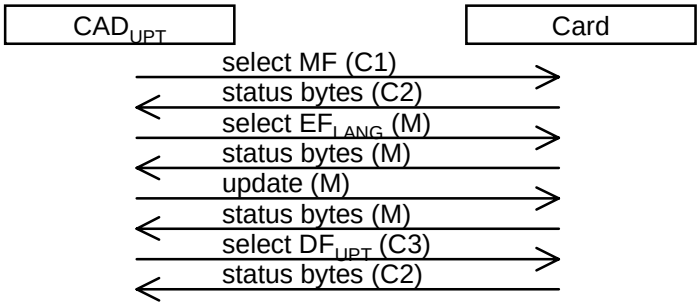


C1: (M) if the current DF is not the MF, else it is not needed.
C2: (M) if the previous command is performed.

Figure 31

11.6.2.2 Update

The CAD_{UPT} performs the select procedure, followed by the update procedure with EF_{LANG}.

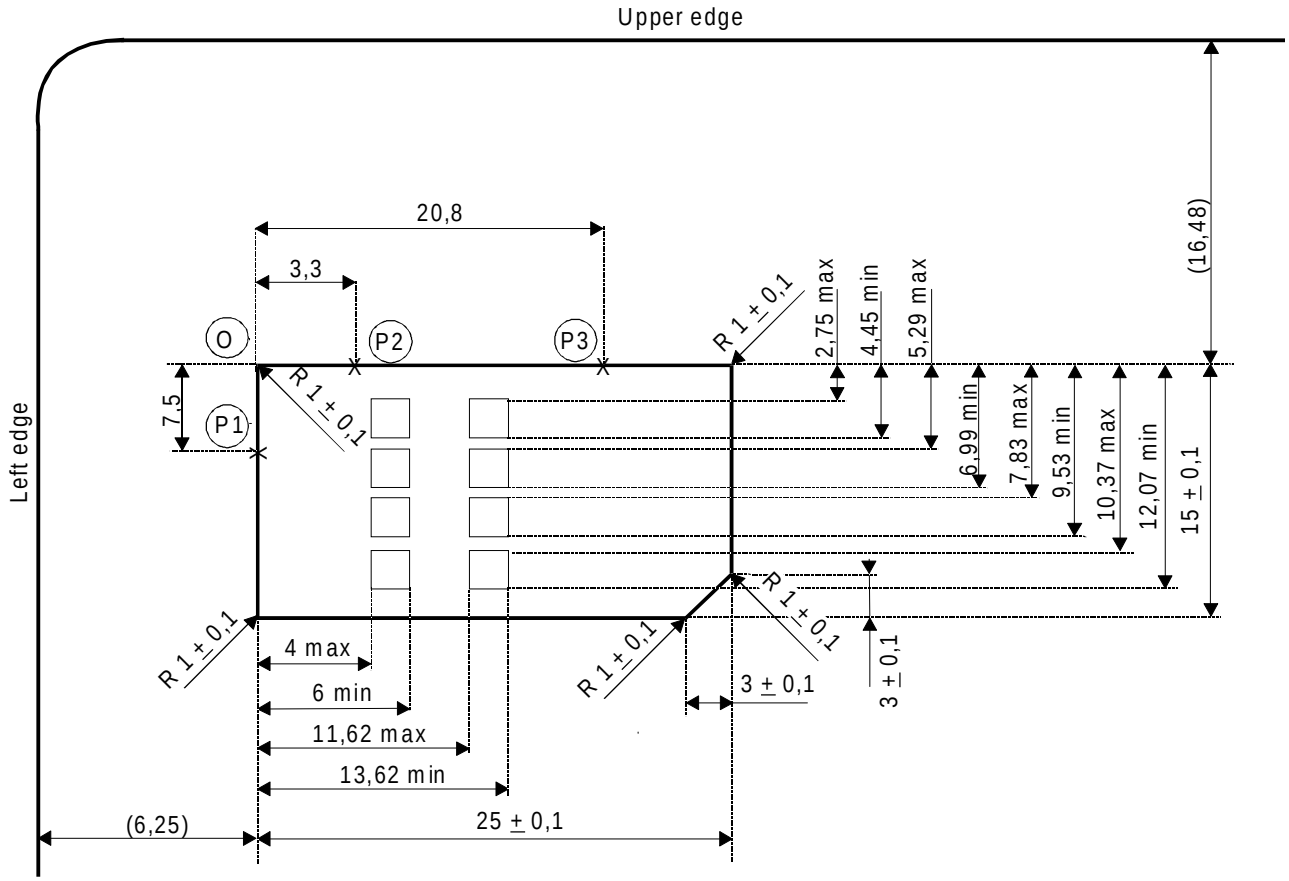


C1: (M) if the current DF is not the MF, else it is not needed.
C2: (M) if the previous command is performed.
C3: (M) this shall be repeated as many times as there are file IDs in the path to the UPT application.

Figure 32

Annex A (normative): Plug-in UPT card

This annex specifies the dimensions of the plug-in UPT card as well as the dimensions and location of the contacts of the plug-in UPT card. For further details of the plug-in card, see clause 4.



NOTE: The values in parentheses show the positional relationship between the plug-in and the ID-1 UPT card and are for information only.

Figure A.1: Plug-in UPT card

Annex B (normative): Implementation Conformance Statement (ICS) for the PIM

A supplier of implementations of PIMs that are claimed to conform to EN 300 477 is required to complete a copy of the relevant ICS proforma provided in this annex and to provide the information necessary to identify both the supplier and the implementation.

B.1 ICS proforma for the PIM

The purpose of the ICS proforma is to submit suppliers and implementors with a questionnaire or checklist. This should be completed in order to state conformance with the requirements of the present document.

B.2 Identification of the implementation, product supplier and test laboratory client

To be filled in by the involved parties:

Date:

Implementation:

Application name: Personal Identification Module (PIM) for UPT

Phase: UPT phase 2

Specification: EN 300 477

Supplier:	**Test laboratory client:**
Company:	Company:
Address:	Address:
Country:	Country:
Contact person:	Contact person:
Telephone:	Telephone:
Facsimile:	Facsimile:

B.3 Identification of the standard

This ICS proforma applies to the PIM requirements in EN 300 477.

B.4 Global statement of conformance

The implementation described in this ICS meets all the mandatory requirements of EN 300 477.

( ) Yes

( ) No

NOTE: Answering "No" to this question indicates non-conformance to the PIM interface specification. Non-supported mandatory capabilities are to be identified in the ICS, with an explanation of why the implementation is non-conforming.

B.5 Interpretation of the tables

Each item in the following tables corresponds to a requirement specified in the standard. The columns of the tables have the following meaning:

Item: Numbers the requirements within a table.

Feature: Short verbal description of a requirement in the standard.

Reference:

Reference to (sub)clause number, where the requirement can be found in the standard.

Status: Indicates if the requirement is:

mandatory (M);

optional (O);

prohibited (X); or

conditional(Cn), description of condition "n" follows below the table.

Support: To be filled in by the implementor. If the item is supported this is indicated by "Yes", if the item is not supported, this is indicated by "No". In some cases additional information shall be given in this column.

B.6 Physical characteristics

Table B.1

Item	Feature	Reference	Status	Support
1	Physical characteristics in accordance with ISO/IEC 7816-1 [9] and ISO/IEC 7816-2 [10].	4	M	
2	ID-1 size.	4.1.1	C1	
3	Plug-in size.	4.1.2	C1	
4	Temperature range -25°C to +70°C with occasional peaks up to 85°C	4.2	M	
5	Contact pressure up to 0,5 N per contact	4.3.3	M	

C1 = It is mandatory to fulfil one of items 2 or 3.

B.6.1 ID-1 size

This table shall only be filled in if item 2 in table B.1 is fulfilled.

Table B.2

Item	Feature	Reference	Status	Support
1	Identification number on the card	4.1	M	
2	Format and layout in accordance with ISO/IEC 7816-1 [9] and ISO/IEC 7816-2 [10]	4.1.1	M	
3	Polarization mark provided	4.1.1	M	
4	Embossing provided in accordance with ISO 7811-1 [7] and ISO 7811-3 [8]	4.1.1	O	
5	Contacts and embossing located on the same side	4.1.1	C2	

C2 = Mandatory if item 4 is fulfilled.

B.6.2 Plug-in size

This table shall only be filled in if item 3 in table B.1 is fulfilled.

Table B.3

Item	Feature	Reference	Status	Support
1	Individual account identifier and check digit on the card	4.1	M	
2	Format and layout in accordance with ENV 1375-1 [16]	4.1.1	M	

B.6.3 Contacts

Table B.4

Item	Feature	Reference	Status	Support
1	Contact C4 provided	4.3.1	O	
2	Contact C6 not bonded	4.3.1	M	
3	Contact C6 provided	4.3.1	O	

B.7 Electronic signals and transmission protocols

Table B.5: Major capabilities

Item	Feature	Reference	Status	Support
1	Electronic signals and transmission protocols in accordance with ISO/IEC 7816-3 [11]	5	M	
2	T = 0 provided	5	M	
3	Other protocols	5	O	
4	Baud rate =	5.7	M	
5	Error detection and character repetition procedure in accordance with ISO/IEC 7816-3 [11]	5.9	M	

B.7.1 Supply voltage VCC (contact C1)

Table B.6: Electrical characteristics of Vcc

Item	Feature	Reference	Status	Support
1	Operating voltage range = 5 V ± 10 %	5.1	M	
2	Current consumption ≤ 10 mA at any frequency accepted by the PIM	5.1	M	
3	Idle current consumption ≤ 200 µA at 1 MHz and 25°C	5.1	M	

B.7.2 Reset RST (contact C2)

Table B.7: Electrical characteristics of RST

Item	Feature	Reference	Status	Support
1	(Vcc-0,7) ≤ V_{OH} ≤ Vcc with I_{OHmax} = +20 µA	5.2	M	
2	0 V ≤ V_{OL} ≤ 0,6 V with I_{OLmax} = -200 µA	5.2	M	
3	$t_R t_F$ ≤ 400 µS with C_{out} = C_{in} = 30 pF	5.2	M	

B.7.3 Clock CLK (contact C3)

Table B.8: Electrical characteristics of CLK

Item	Feature	Reference	Status	Support
1	1 MHz ≤ (clock frequency) ≤ 5 MHz	5.4	M	
2	Duty cycle between 40 % and 60 % of the period during stable operation	5.4	M	
3	(0,7xVcc) ≤ V_{OH} ≤ Vcc, with I_{OHmax} = +20 µA	5.4	M	
4	0 V ≤ V_{OL} ≤ 0,5 V, with I_{OLmax} = -200 µA	5.4	M	
5	t_R t_F ≤ 9 % of period (0,5 µS max), with C_{out} = C_{in} = 30 pF	5.4	M	
6	Internal clock	5.4	X	

B.7.4 I/O (contact C7)

Table B.9: Electrical characteristics of I/O

Item	Feature	Reference	Status	Support
1	(0,7 x Vcc) ≤ V_{IH} ≤ Vcc + 0,3 V, I_{IHmax} = ± 20 µA	5.5	M	
2	-0,3 V ≤ V_{IL} ≤ 0,8 V, with I_{ILmax} = +1 mA	5.5	M	
3	3,8 V ≤ V_{OH} ≤ Vcc, with I_{OHmax} = +20 µA	5.5	M	
4	0 V ≤ V_{OL} ≤ 0,4 V, with I_{OLmax} = -1 mA	5.5	M	
5	t_R t_F ≤ 1 µS with C_{out} = C_{in} = 30 pF	5.5	M	

B.7.5 States

Table B.10: Clock stop modes

Item	Feature	Reference	Status	Support
1	Clockstop allowed, no preferred level	5.6, 9.3.1	C3	
2	Clockstop allowed, high level preferred	5.6, 9.3.1	C3	
3	Clockstop allowed, low level preferred	5.6, 9.3.1	C3	
4	Clockstop allowed, only on high level	5.6, 9.3.1	C3	
5	Clockstop allowed, only on low level	5.6, 9.3.1	C3	

C3 = Optional, but only one of items 1 to 5 at the time.

B.7.6 Answer to Reset (ATR)

Table B.11: Structure, contents and PTS procedure

Item	Feature	Reference	Status	Support
1	The length of the ATR ≤ 33	5.8.1	M	
2	ATR: TS is sent	5.8.1	M	
3	ATR: T0 is sent	5.8.1	M	
4	ATR: TA1 is sent	5.8.1	O	
5	ATR: TB1 is sent	5.8.1	O	
6	ATR: PI1 = 0	5.8.1	C4	
7	ATR: TC1 is sent	5.8.1	O	
8	ATR: TC1 = 0	5.8.1	C5	
9	ATR: TC1 = 255	5.8.1	C5	
10	ATR: TD1 is sent	5.8.1	O	
11	ATR: TD1 coded that TB2 is not sent	5.8.1	C6	
12	ATR: TA2 is sent	5.8.1	C7	
13	ATR: TB2 not sent	5.8.1	M	
14	ATR: TC2 is sent	5.8.1	O	
15	ATR: TDi is/are sent	5.8.1	O	
16	ATR: Optional interface characters TAi, TBi, TCi, i > 2 (indicate which characters in the support column)	5.8.1	O	
17	ATR: Historical characters sent, T1, ..., TK (indicate which characters in the support column)	5.8.1	O	
18	Check character	5.8.1	C7	
19	PTS procedure	5.8.2	C8	
20	Error detection and character repetition procedure	5.9	M	

C4 = Mandatory if item 5 is fulfilled.
C5 = Mandatory to fulfil one of items 8 or 9.
C6 = Mandatory if item 10 is fulfilled.
C7 = Mandatory if other protocol(s) than T = 0 is/are provided.
C8 = Mandatory if item 4 is fulfilled and TA1 is not '11'.

B.8 Logical model

Table B.12

Item	Feature	Reference	Status	Support
1	File ID of the MF = '3F00'	6.2	M	
2	Two files under the same parent never have the same file ID	6.2	M	
3	A child and its parent never have the same file ID	6.2	M	
4	A child and its grandparent never have the same file ID	6.2	M	
5	A child and its grandparent's child, if it is a DF, never have the same file ID	6.2	M	
6	DF_{UPT} provided	6.4	M	
7	$DF_{TELECOM}$ provided	6.4	O	
8	Transparent EFs supported	6.5.1	M	
9	Linear fixed EFs supported	6.5.2	C9	
10	Cyclic EFs supported	6.5.3	C10	
10	File IDs '7F1X' and '6FXX' are not used under DF_{UPT}	6.7	M	
11	No DFs except '7F4X' are used for administrative purposes under DF_{UPT}	6.7	M	
12	No EFs except '2FXX' are used for administrative purposes under DF_{UPT}	6.7	M	

C9 = Mandatory if item 7 is fulfilled.
C10 = Mandatory if item 14 in table B.11 is fulfilled.

B.9 Security features and facilities

Table B.13

Item	Feature	Reference	Status	Support
1	TESA-7 authentication algorithm	7.2, 10.2.1	C11	
2	USA-4 authentication algorithm	7.2, 10.2.1	C11	
3	Proprietary authentication algorithm (indicate the name of the algorithm in the support column)	7.2, 10.2.1	C11	
4	Card holder verification	7.2.1	M	
5	It is not possible to disable the relevant CHV1 of DF_{UPT}.	7.2.1	M	
6	File access condition ALWAYS is supported	7.3	M	
7	File access condition CHV1 is supported	7.3	M	
8	File access condition NEVER is supported	7.3	M	
9	The INTERNAL AUTHENTICATION command cannot be used without a previous successful card holder verification	7.4	M	

C11 = Mandatory to fulfil one of items 1, 2 or 3.

B.10 Description of functions

Table B.14

Item	Feature	Reference	Status	Support
1	SELECT	8.1, 9.3.1	M	
2	READ BINARY	8.2, 9.3.2	M	
3	UPDATE BINARY	8.3, 9.3.3	M	
4	READ RECORD	8.4, 9.3.4	C12	
5	UPDATE RECORD	8.5, 9.3.5	C12	
6	SEEK	8.6, 9.3.6	C12	
7	VERIFY CHV	8.7, 9.3.7	M	
8	CHANGE CHV	8.8, 9.3.8	M	
9	UNBLOCK CHV	8.9, 9.3.9	M	
10	INTERNAL AUTHENTICATION	8.10, 9.3.10	M	
11	GET RESPONSE	9.3.11	M	
12	SW1 and SW2 returned after each command	9.4	M	

C12 = Mandatory if item 7 in table B.12 is fulfilled.

B.11 Contents of the EFs

Table B.15

Item	Feature	Reference	Status	Support
1	EF_{CHV1}	10.1	M	
2	EF_{ID}	10.2.1	O	
2a	Date of activation	10.2.1	O	
2b	Card expiry date	10.2.1	O	
2c	Card sequence number	10.2.1	O	
2d	Country code	10.2.1	O	
3	EF_{ICC}	10.2.2	O	
3a	IC identifier	10.2.2	O	
3b	Card profile	10.2.2	O	
3c	Type of selection	10.2.2	O	
4	EF_{DIR}	10.2.3	M	
5	EF_{LANG}	10.2.4	O	
5a	2nd language preference	10.2.4	O	
5b	3rd language preference	10.2.4	O	
5c	4th language preference	10.2.4	O	
6	EF_{NAME}	10.2.5	O	
7	EF_{CT}	10.3.1	M	
8	EF_{PUI}	10.3.2	M	
9	EF_{SEQ}	10.3.3	M	
10	EF_{PST}	10.3.4	O	
11	EF_{TV}	10.3.5	M	
12	EF_{MTV}	10.3.6	O	
13	EF_{ADN}	10.4.1	O	
14	EF_{LND}	10.4.2	O	
15	EF_{EXT1}	10.4.3	O	

Annex C (normative): Implementation Conformance Statement (ICS) for the CAD_{UPT}

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the ICS proforma in this annex so that it can be used for its intended purposes and may further publish the completed ICS.

A supplier of implementations of CAD_{UPT}s that are claimed to conform to EN 300 477 is required to complete a copy of the relevant ICS proforma provided in this annex and is required to provide the information necessary to identify both the supplier and the implementation.

C.1 ICS proforma for the CAD_{UPT}

The purpose of the ICS proforma is to submit suppliers and implementors with a questionnaire or checklist. This should be completed in order to state conformance with the requirements of the present document.

C.2 Identification of the implementation, product supplier and test laboratory client

To be filled in by the involved parties:

Date:

Implementation:

Application name: UPT card accepting DTMF device

Phase: UPT phase 2

Specification: EN 300 477

Supplier:	**Test laboratory client:**
Company:	Company:
Address:	Address:
Country:	Country:
Contact person:	Contact person:
Telephone:	Telephone:
Facsimile:	Facsimile:

C.3 Identification of the standard

This ICS proforma applies to the CAD_{UPT} requirements in EN 300 477.

C.4 Global statement of conformance

The implementation described in this ICS meets all the mandatory requirements of EN 300 477.

( ) Yes

( ) No

NOTE: Answering "No" to this question indicates non-conformance to the CAD_{UPT} interface specification. Non-supported mandatory capabilities are to be identified in the ICS, with an explanation of why the implementation is non-conforming.

C.5 Interpretation of the tables

Each item in the following tables corresponds to a requirement specified in the standard. The columns of the tables have the following meaning:

Item: Numbers the requirements within a table.

Feature: Short verbal description of a requirement in the standard.

Reference:

Reference to (sub)clause number, where the requirement can be found in the standard.

Status: Indicates if the requirement is:

mandatory (M);

optional (O); or

conditional(Cn), description of condition "n" follows below the table.

Support: To be filled in by the implementor. If the item is supported, this is indicated by "Yes", if the item is not supported, this is indicated by "No". In some cases additional information shall be given in this column.

C.6 Physical characteristics

Table C.1

Item	Feature	Reference	Status	Support
1	Accepts ID-1 size cards	4.1.1	C1	
2	Accepts plug-in size cards	4.1.2	C1	
3	Accepts embossed ID-1 size cards	4.1.1	C2	
4	Provision of contacts in accordance with ISO/IEC 7816-2 [10]	4.3	M	
5	Contact C4 provided	4.3.1	O	
6	Contact C6 provided	4.3.1	O	
7	Contact C8 provided	4.3.1	O	
8	Operating procedures in accordance with ISO/IEC 7816-3 [11]	4.3.2	M	
9	Activation and deactivation order respected at any voltage level	4.3.2	M	
10	Radius of curvature contacting elements ≥ 0,8 mm	4.3.3	M	
11	Contact pressure ≤ 0,5 N	4.3.3	M	
12	ID-1 size card takes precedence over plug-in size card	4.4	C3	

C1 = It is mandatory to fulfil at least one of items 1 and 2.
C2 = Mandatory only if item 1 is fulfilled.
C3 = Mandatory if both item 1 and 2 are fulfilled.

C.7 Electronic signals and transmission protocols

Table C.2

Item	Feature	Reference	Status	Support
1	Electronic signals and transmission protocols in accordance with ISO/IEC 7816-3 [11]	5	M	
2	T = 0 provided	5	M	
3	Contact C6 not wired	5.3	M	
4	Baud rate =	5.6	M	
5	Perform a Reset on receipt of an ATR which is not in accordance with the present document	5.9	M	
6	Rejection of the PIM does not occur until at least three consecutive wrong ATRs are received	5.9	M	
7	Error detection and character repetition procedure during ATR/PTS in accordance with ISO/IEC 7816-3 [11]	5.9	O	
8	Error detection and character repetition procedure following ATR/PTS in accordance with ISO/IEC 7816-3 [11], using T = 0	5.9	M	

C.7.1 Supply voltage VCC (contact C1)

Table C.3: Electrical characteristics of Vcc

Item	Feature	Reference	Status	Support
1	Supply voltage range = 5 V ± 10 %	5.1	M	
2	Supply current up to 10 mA at any frequency accepted by the PIM	5.1	M	
3	Counteract current consumption spikes as specified	5.1	M	

C.7.2 Reset RST (contact C2)

Table C.4: Electrical characteristics of RST

Item	Feature	Reference	Status	Support
1	$(Vcc - 0,7) \leq V_{OH} \leq Vcc$ with I_{OHmax} = +20 µA	5.2	M	
2	$0\ V \leq V_{OL} \leq 0,6\ V$ with I_{OLmax} = -200 µA	5.2	M	
3	$t_R t_F \leq 400$ µS with $C_{out} = C_{in}$ = 30 pF	5.2	M	

C.7.3 Clock CLK (contact C3)

Table C.5: Electrical characteristics of CLK

Item	Feature	Reference	Status	Support
1	1 MHz ≤ (clock frequency) ≤ 5 MHz	5.4	M	
2	Duty cycle between 40 % and 60 % of the period during stable operation	5.4	M	
3	$(0,7 \times Vcc) \leq V_{OH} \leq Vcc$, with I_{OHmax} = +20 µA	5.4	M	
4	$0\ V \leq V_{OL} \leq 0,5\ V$, with I_{OLmax} = -200 µA	5.4	M	
5	$t_R\ t_F \leq 9$ % of period (0,5 µS max), with $C_{out} = C_{in}$ = 30 pF	5.4	M	

C.7.4 I/O (contact C7)

Table C.6: Electrical characteristics of I/O

Item	Feature	Reference	Status	Support
1	$(0,7 \times Vcc) \leq V_{IH} \leq Vcc + 0,3\ V$, I_{IHmax} = ± 20 µA	5.5	M	
2	$-0,3\ V \leq V_{IL} \leq 0,8\ V$, with I_{ILmax} = +1 mA	5.5	M	
3	$3,8\ V \leq V_{OH} \leq Vcc$, with I_{OHmax} = +20 µA	5.5	M	
4	$0\ V \leq V_{OL} \leq 0,4\ V$, with I_{OLmax} = -1 mA	5.5	M	
5	$t_R\ t_F \leq 1$ µS with $C_{out} = C_{in}$ = 30 pF	5.5	M	

C.7.5 States

Table C.7: Clock stop modes

Item	Feature	Reference	Status	Support
1	Clockstop	5.6	O	

C.7.6 Answer to Reset (ATR)

Table C.8: Structure, contents and PTS procedure

Item	Feature	Reference	Status	Support
1	Length of the ATR up to 33 characters	5.8.1	M	
2	ATR: TS	5.8.1	M	
3	ATR: T0	5.8.1	M	
4	ATR: TA1, if present	5.8.1	M	
5	ATR: TB1, if present	5.8.1	M	
6	ATR: TC1, if present	5.8.1	M	
7	ATR: TD1, if present	5.8.1	M	
8	ATR: TA2, if present	5.8.1	O	
9	ATR: TC2, if present	5.8.1	M	
10	ATR: TDi (i > 1), if present	5.8.1	M	
11	ATR: Optional interface characters TAi, TBi, TCi, i > 2, if present	5.8.1	O	
12	ATR: Historical characters, T1, ..., TK, if present	5.8.1	O	
13	Check character, if present	5.8.1	O	
14	PTS procedure	5.8.2	C4	

C4 = Mandatory if item 4 is fulfilled and TA1 is not '11'.

C.8 Security features and facilities

Table C.9

Item	Feature	Reference	Status	support
1	Timer provided	7.2.2	M	

C.9 Coding of the commands

Table C.10

Item	Feature	Reference	Status	support
1	SELECT	8.1, 9.3.1	M	
2	READ BINARY	8.2, 9.3.2	M	
3	UPDATE BINARY	8.3, 9.3.3	M	
4	READ RECORD	8.4, 9.3.4	C5	
5	UPDATE RECORD	8.5, 9.3.5	C5	
6	SEEK	8.6, 9.3.6	C5	
7	VERIFY CHV	8.7, 9.3.7	M	
8	CHANGE CHV	8.8, 9.3.8	M	
9	UNBLOCK CHV	8.9, 9.3.9	M	
10	INTERNAL AUTHENTICATION	8.10, 9.3.10	M	
11	GET RESPONSE	9.3.11	M	
12	RFU bits and bytes are not interpreted	9.2	M	

C5 = Mandatory if one of the items 13 or 14 in table C.11 is fulfilled.

C.10 Application protocol

Table C.11

Item	Feature	Reference	Status	Support
1	Reading an EF	11.1.1	M	
2	Updating an EF	11.1.2	M	
3	Seeking in an EF	11.1.3	O	
4	Selecting an EF or DF	11.1.4	M	
5	PIM initialization	11.2.2	M	
6	PIM session	11.2.3	M	
7	PIM session termination	11.2.4	M	
8	Start timer	11.2.5	M	
9	Timer value substitution	11.2.6	M	
10	CHV verification	11.3.1	M	
11	CHV value substitution	11.3.2	O	
12	CHV unblocking	11.3.3	O	
13	One pass strong authentication	11.4.1	M	
14	ADNs	11.5.1	O	
15	LND	11.5.1	O	
16	Updating of ADN and LND	11.5.1.1	O	
17	Erasure of ADN and LND	11.5.1.2	O	
18	Request of ADN and LND	11.5.1.3	O	
19	Purge of ADN and LND	11.5.1.4	O	
20	Application selection procedure	11.6.1	M	
21	NAME request procedure	11.6.2	O	
22	Language preference procedures	11.6.3	O	

Annex D (informative): Example of a normal UPT session

Figure D.1 describes the information flow between all parts involved in a normal UPT session.

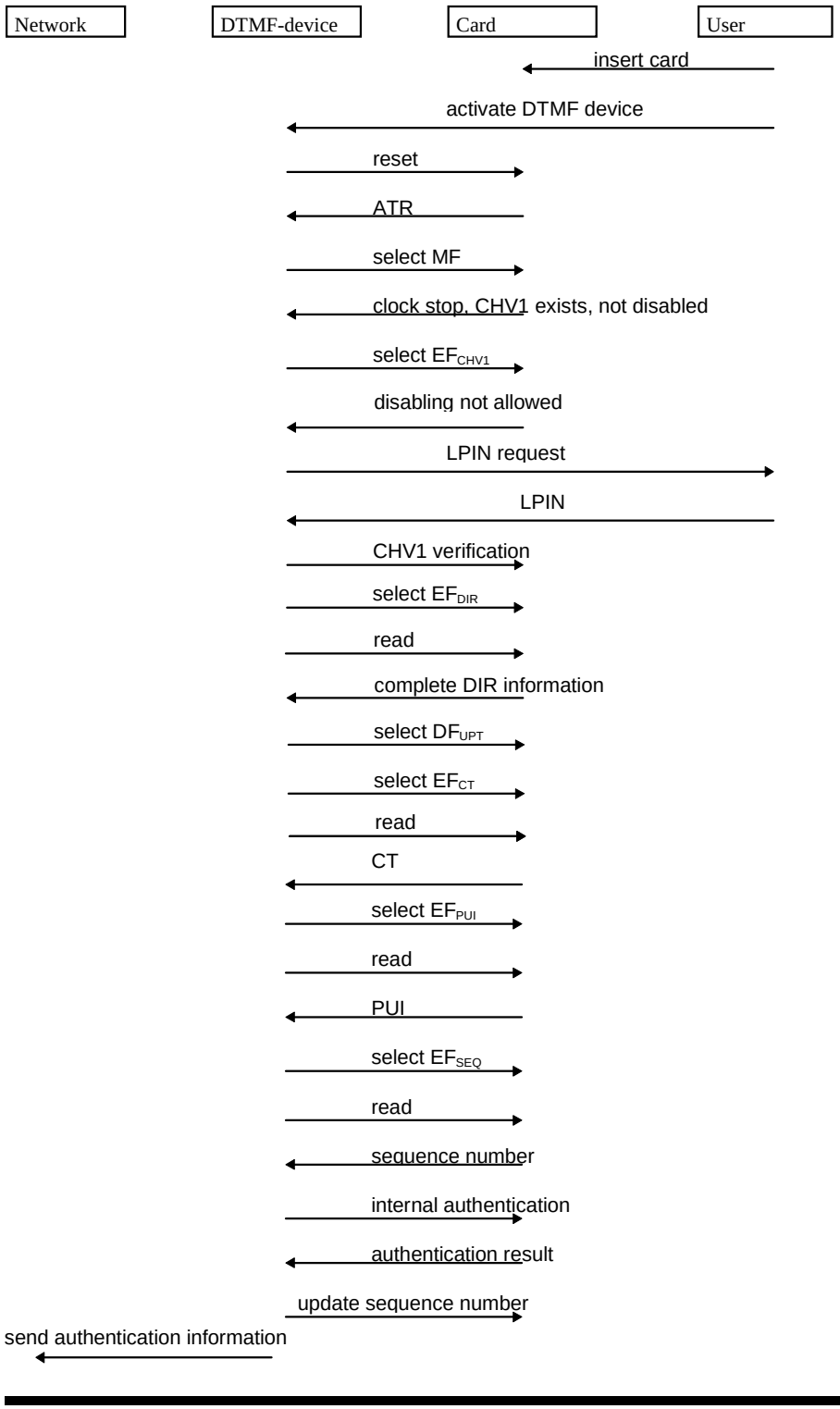


Figure D.1: The flow of the recommended implementation of the UPT application in a mono-application card

NOTE: In the flow diagram the following assumptions are made:
- EF_{DIR} is not protected by any CHV;
- the relevant CHV1 for DF_{UPT} is situated at MF level.

Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

ETR 083: "Universal Personal Telecommunications (UPT); General UPT security architecture".

History

Document history		
Edition 1	September 1996	Publication as ETS 300 477
V1.2.1	December 1998	One-step Approval Procedure OAP 9916: 1998-12-18 to 1999-04-16
V1.2.2	May 1999	Publication

ISBN 2-7437-3084-6
Dépôt légal : Mai 1999