Draft EN 300 823 V1.2.1 (1998-11)

European Standard (Telecommunications series)

Universal Personal Telecommunication (UPT);
UPT phase 2;
Functional specification of the interface of a UPT Integrated Circuit Card (ICC) and Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN) and Global System for Mobile communications (GSM) terminals (one pass and multiple pass authentication)

Reference

REN/NA-064013 (7mc00ioo.PDF)

Keywords

UPT, CARD, PSTN, GSM, ISDN

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
http://www.etsi.org

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), and is now submitted for the ETSI standards One-step Approval Procedure.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

1 Scope

The present document in combination with ETS 300 477 [1] 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.

The present document relates to the interface between a UPT card and Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN) and Global System for Mobile (GSM) communications terminals. These interfaces are completely described by ETS 300 477 [1] plus the additions and modifications contained in the present document; i.e. the present document is a delta document.

The following clauses from ETS 300 477 [1] are amended or modified in the present document:

- logical model (combined PIM1/PIM2);
- security (two pass strong authentication);
- functions (internal authentication);
- commands (internal authentication);
- Elementary Files (EF_{SEQ}, EF_{DIR});
- Application Protocol (AP) (two pass strong authentication);
- Implementation Conformance Statement (ICS) proformas.

The clause numbering of ETS 300 477 [1] is kept in order to ease comparisons. Unmodified clauses and subclauses are marked appropriately.

The present document together with ETS 300 477 [1] 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.

The information flow between the CAD_{UPT} and the network is outside the scope of the present document.

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] ETS 300 477: "Universal Personal Telecommunication (UPT); UPT Phase 2; Functional specification of the interface of a UPT Integrated Circuit Card (ICC) and Card Accepting Devices (CADs); UPT card accepting Dual Tone Multiple Frequency (DTMF) device".

[2] ETS 300 790: "Universal Personal Telecommunication (UPT); Security architecture for UPT phase 2; Specification".

[3] CCITT Recommendation E.164: "The internatonal public telecommunication numbering plan".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply, together with those contained in ETS 300 477 [1]:

PIM1: Personal Identification Module according to ETS 300 477 [1].

PIM2: Personal Identification Module according to the present document.

3.2 Symbols

For the purposes of the present document, the symbols contained in ETS 300 477 [1] apply.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply, together with those of ETS 300 477 [1]:

AE	Application Entity
AP	Application Protocol
CT	Cordless Telephone
ICS	Implementation Conformance Statement
ISDN	Integrated Services Digital Network
PSTN	Public Switched Telephone Network
RAND	Random challenge sent by the network to be used for authentication

4 Physical characteristics

The same text as in ETS 300 477 [1] is valid.

5 Electronic signals and transmission protocols

The same text as in ETS 300 477 [1] is valid.

6 Logical model

The same text as in ETS 300 477 [1] is valid with the following modifications:

In subclause 6.4, "DF_{UPT}" is replaced by "DF_{UPT2}", and the following note is added:

NOTE: Both PIM1 and PIM2 can be implemented in one card, each representing its own application.

7 Security services and facilities

The same text as in ETS 300 477 [1], clause 7 is valid with the following modifications:

PIM is replaced by PIM2, and "ETS 300 391-1" is replaced by "ETS 300 790 [2]".

7.1 Authentication key

The same text as in ETS 300 477 [1] subclause 7.1 is valid with the following addition:

If both PIM1 and PIM2 are implemented in the same card, then they shall use a different authentication key.

7.2 Algorithms and processes

The same text is valid with reference "ETS 300 790 [2]" instead of "ETS 300 391-1".

7.2.1 Card Holder Verification (CHV)

The same text as in ETS 300 477 [1] subclause 7.2.1 is valid, with the addition of the following note:

NOTE: If both PIM1 and PIM2 are implemented in the same card, for security reasons, two different CHVs should be used for PIM1 and PIM2.

7.2.2 Strong authentication

The two 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 CT are obtained from the PIM and are sent to the Authenticating Entity (AE) in an authentication request;

5) the AE sends a random number RAND to the CAD_{UPT} in an authentication request;

6) the RAND is given to the PIM, which calculates an Authentication Code (AC) and returns it to the CAD_{UPT};

7) the CAD_{UPT} sends the PUI, CT 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

The same text as in ETS 300 477 [1] subclause 7.3 is valid.

7.4 Function access condition

The same text as in ETS 300 477 [1] subclause 7.4 is valid.

7.5 Identification, keying and algorithm information

The following data used for identification and secret keys are stored in the PIM:

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

8 Description of the functions

The same text as in ETS 300 477 [1] is valid with the following modifications:

- "DF_{UPT}" is replaced by "DF_{UPT2}".

In subclause 8.10, the input is "challenge (RAND)" instead of "challenge (n)".

9 Description of the commands

The same text as in ETS 300 477 [1] is valid with the following modification:

- In subclause 9.3.10, "challenge (sequence number)" is replaced by "challenge (RAND)".

10 Contents of the EFs

The same text as in ETS 300 477 [1] is valid with the following modifications:

- "DF_{UPT}" is replaced by "DF_{UPT2}".
- EF_{SEQ} is deleted from figure 9.

In subclause 10.2.3, "UPT application" is replaced by "PIM2 application".

In subclause 10.2.3, the following note is added:

NOTE 1: The PIM2 application identifier is different from the UPT application identifier.

Subclause 10.3.3 is deleted.

In subclause 10.4, note 2 is replaced by the following text:

NOTE 2: The CAD_{UPT} should interpret the TON and NPI information.

As EF_{ADN} is part of the $DF_{TELECOM}$ it may be used by UPT and also other applications in a multi-application card. If the other application does not recognize the use of TON and NPI, then the information relating to the national dialling plan should be held within the data item dialling number and the TON and NPI fields set to UNKNOWN. This format would be acceptable for UPT operation and also for the other application where the TON and NPI fields should be ignored.

EXAMPLE: PIM storage of an International Number using CCITT Recommendation E.164 [3] numbering plan.

	TON	NPI	Digit field
UPT application	001	0001	abc...
Other application compatible with UPT	000	0000	xxx...abc...

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

11 Application protocol

The same text as in ETS 300 477 [1], clause 11, is valid except that "one-pass strong authentication" is replaced by "two-pass strong authentication".

11.1 General procedures

The same text as in ETS 300 477 [1], subclause 11.1, is valid.

11.2 PIM management procedures

The same text as in ETS 300 477 [1], subclause 11.2, is valid except that "one-pass strong authentication" is replaced by "two-pass strong authentication", "UPT application selection" by "PIM2 application selection", "UPT session" by "PIM2 session", and "DF_{UPT}" by "DF_{UPT2}".

11.3 CHV related procedures

The same text as in ETS 300 477 [1], clause 11, is valid except that "UPT application" is replaced by "PIM2 application".

11.4 UPT security related procedures

The following UPT security related procedure is recognized for the PIM2:

- two-pass strong authentication.

The mechanism is specified in clause 7.

The specification of the data elements used in the authentication procedure and in the secure answer procedure can be found in ETS 300 790 [2].

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

11.4.1 Two-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:

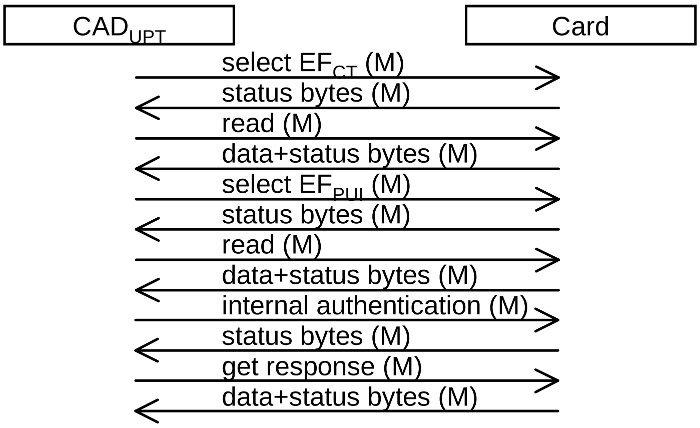
1) the CAD$_{UPT}$ selects and reads EF$_{CT}$;

2) the CAD$_{UPT}$ selects and reads EF$_{PUI}$;

3) the CAD$_{UPT}$ gives an INTERNAL AUTHENTICATION command with the random number RAND received from the AE as a challenge to the command. Then the PIM calculates an AC, which is returned in the response;

4) the CAD$_{UPT}$ sends PUI, CT and AC to the network.

Step 4 is not part of the protocol between the CAD$_{UPT}$ and the PIM, but is included for clarification.



NOTE: Regarding the interface between the PIM2 and the CAD$_{UPT}$, the procedure "secure answer", which may be activated by the calling party or by the called party, is the same procedure as the two-pass strong authentication.

Figure 1

11.5 Telecommunication procedures

The same text as in ETS 300 477 [1], subclause 11.5, is valid except that the half sentence "this is only possible with the last numbers dialled by the DTMF device" is obsolete for the PIM2 since it is inserted directly into a card reading terminal.

11.6 General information procedures

The same text as in ETS 300 477 [1], subclause 11.6, is valid.

Annex A (normative): Plug-in UPT card

The same text as in ETS 300 477 [1] is valid.

Annex B (normative): Implementation Conformance Statement (ICS) for the PIM2

A supplier of implementations of PIMs that are claimed to conform to the present document 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 PIM2

The purpose of the ICS proforma is to submit suppliers and implementers 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 version 2 (PIM2) for UPT

Phase: UPT phase 2

Specification: ETS 300 823, Edition 1

Supplier:

Company:

Address:

Country:

Contact person:

Telephone:

Facsimile:

Test laboratory client:

Company:

Address:

Country:

Contact person:

Telephone:

Facsimile:

B.3 Identification of the standard

This ICS proforma applies to the PIM requirements in the present document.

B.4 Global statement of conformance

The implementation described in this ICS meets all the mandatory requirements of the present document.

( ) Yes

( ) No

NOTE: Answering "No" to this question indicates non-conformance to the PIM2 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 implementer. 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 (reference [9] in ETS 300 477 [1]) and ISO/IEC 7816-2 (reference [10] in ETS 300 477 [1]).	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 (reference [9] in ETS 300 477 [1]) and ISO/IEC 7816-2 (reference [10] in ETS 300 477 [1]).	4.1.1	M	
3	Polarization mark provided.	4.1.1	M	
4	Embossing provided in accordance with ISO 7811-1 (reference [7] in ETS 300 477 [1]) and ISO 7811-3 (reference [8] in ETS 300 477 [1]).	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.	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 (reference [11] in ETS 300 477 [1]).	5	M	
2	T = 0 provided.	5	M	
3	Other protocols.	5	O	
4	Baud rate = (clock frequency)/372.	5.7	M	
5	Error detection and character repetition procedure in accordance with ISO/IEC 7816-3 [11] in ETS 300 477 [1]).	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 PIM2.	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	0V ≤ 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	(0,7 × Vcc) ≤ 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	$(0,7 \times Vcc) \leq V_{IH} \leq Vcc + 0,3$ V, $I_{IHmax} = \pm 20$ 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 $\leq V_{OL} \leq$ 0,4V, with I_{OLmax} = -1 mA	5.5	M	
5	t_R $t_F \leq$ 1µS 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 = "3 F00"	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$_{UPT2}$ 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 "7 F1X" and "6 FXX" are not used under DF$_{UPT2}$.	6.7	M	
11	No DFs except "7 F4X" are used for administrative purposes under DF$_{UPT2}$.	6.7	M	
12	No EFs except "2 FXX" are used for administrative purposes under DF$_{UPT2}$.	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$_{UPT2}$.	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	
10	PIM1 and PIM2 use different authentication keys if implemented in the same card.	7.1	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_{PST}	10.3.4	O	
10	EF_{TV}	10.3.5	M	
11	EF_{MTV}	10.3.6	O	
12	EF_{ADN}	10.4.1	O	
13	EF_{LND}	10.4.2	O	
14	EF_{EXT1}	10.4.3	O	

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

A supplier of implementations of CAD_{UPTs} that are claimed to conform to the present document 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 implementers 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 terminal

Phase: UPT phase 2

Specification: ETS 300 823, Edition 1.

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 the present document.

C.4 Global statement of conformance

The implementation described in this ICS meets all the mandatory requirements of the present document.

- ( ) 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 implementer. 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 (reference [10] in ETS 300 477 [1]).	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 (reference [11] in ETS 300 477 [1]).	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 (reference [11] in ETS 300 477 [1]).	5	M	
2	T = 0 provided	5	M	
3	Contact C6 not wired	5.3	M	
4	Baud rate = (clock frequency)/372	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 PIM2 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.	5.9	O	
8	Error detection and character repetition procedure following ATR/PTS in accordance with ISO/IEC 7816-3, 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 PIM2.	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 $I_{OHmax} = +20\ \mu A$	5.2	M	
2	$0V \leq V_{OL} \leq 0{,}6\ V$ with $I_{OLmax} = -200\ \mu A$	5.2	M	
3	$t_R t_F \leq 400\ \mu S$ 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	1MHz ≤ (clock frequency) ≤ 5MHz	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 $I_{OHmax} = +20\ \mu A$	5.4	M	
4	$0V \leq V_{OL} \leq 0{,}5\ V$, with $I_{OLmax} = -200\ \mu A$	5.4	M	
5	$t_R\ t_F \leq 9$ % of period (0,5µS 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, $I_{IHmax} = \pm 20$ 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	0V $\leq V_{OL} \leq 0,4$ 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	PIM2 initialization	11.2.2	M	
6	PIM2 session	11.2.3	M	
7	PIM2 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	Two 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	

History

Document history		
Edition 1	December 1997	Publication as ETS 300 823
V1.2.1	November 1998	One-step Approval Procedure OAP 9911: 1998-11-13 to 1999-03-12