SIST

SLOVENSKI STANDARD
SIST ETS 300 823 E1:2003

01-december-2003

Svetovne osebne telekomunikacije (UPT) ï UPT, faza 2 ï Funkcijska specifikacija vmesnika ļ ipne kartice (ICC) sistema UPT in javnega komutiranega telefonskega omreģja (PSTN), digitalnega omreģja z integriranimi storitvami (ISDN) in globalnega sistema mobilnih komunikacij (GSM) (enkratna in veļ kratna avtentikacija)

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)

Ta slovenski standard je istoveten z: **ETS 300 823 Edition 1**

ICS:

33.040.35	Telefonska omrežja	Telephone networks
33.070.50	Globalni sistem za mobilno telekomunikacijo (GSM)	Global System for Mobile Communication (GSM)
33.080	Digitalno omrežje z integriranimi storitvami (ISDN)	Integrated Services Digital Network (ISDN)

SIST ETS 300 823 E1:2003 **en**

EUROPEAN
TELECOMMUNICATION
STANDARD

ETS 300 823

December 1997

Source: NA

Reference: DE/NA-064010

ICS: 33.020

Key words: UPT, CARD, PSTN, GSM, ISDN

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)

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

Contents

Foreword

This European Telecommunication Standard (ETS) has been produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI).

Transposition dates	
Date of adoption:	21 November 1997
Date of latest announcement of this ETS (doa):	31 March 1998
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	30 September 1998
Date of withdrawal of any conflicting National Standard (dow):	30 September 1998

Blank page

1 Scope

This European Telecommunication Standard (ETS) 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.

This ETS 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 this ETS; i.e. this ETS is a delta document.

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

- 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.

This ETS 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.

This ETS 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. This ETS 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 this ETS.

2 Normative references

This ETS incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[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: "Numbering plan for the ISDN era".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of this ETS, the following 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 this ETS.

3.2 Symbols

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

3.3 Abbreviations

For the purposes of this ETS, 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 $\text{DF}_{\text{TELECOM}}$ 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.