SLOVENSKI STANDARD
SIST EN 300 823 V1.2.2:2003

01-december-2003

Svetovne osebne telekomunikacije (UPT) ï UPT, faza 2 ï Funkcijska specifikacija vmesnika ļ ipovne kartice (ICC) sistema UPT ter terminalov 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: **EN 300 823 Version 1.2.2**

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 EN 300 823 V1.2.2:2003 **en**

EN 300 823 V1.2.2 (1999-04)

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 (7mc00ipc.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
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:	19 March 1999
Date of latest announcement of this EN (doa):	30 June 1999
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 December 1999
Date of withdrawal of any conflicting National Standard (dow):	31 December 1999

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] ITU-T 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)".