



**SLOVENSKI STANDARD**  
**SIST ETS 300 791 E1:2003**  
**01-december-2003**

---

**Omrežni vidiki (NA ) – Svetovne osebne telekomunikacije (UPT) – Varnostna arhitektura za UPT – Faza 2: Specifikacija za preskušanje skladnosti (CTS)**

Universal Personal Telecommunication (UPT); Security architecture for UPT phase 2; Conformance Test Specification (CTS)

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

Ta slovenski standard je istoveten z: **ETS 300 791 Edition 1**  
<https://standards.iteh.ai/catalog/standards/sist/d4c9b14c-28e8-4c15-9bd4-c3212ef42ab4/sist-ets-300-791-e1-2003>

---

**ICS:**

33.040.35      Telefonska omrežja      Telephone networks

**SIST ETS 300 791 E1:2003**      en

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

SIST ETS 300 791 E1:2003

<https://standards.iteh.ai/catalog/standards/sist/d4c9bf4c-28e8-4c15-9bd4-c3212ef42ab4/sist-ets-300-791-e1-2003>



**E**UROPEAN  
**T**ELECOMMUNICATION  
**S**TANDARD

**ETS 300 791**

October 1997

Source: NA

Reference: DE/NA-064007

ICS: 33.020

**Key words:** UPT, security, card, CTS

**Network Aspects (NA);  
Universal Personal Telecommunication (UPT);  
Security architecture for UPT Phase 2;  
Conformance Test Specification (CTS)**

**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

**Copyright Notification:** No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1997. All rights reserved.

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST ETS 300 791 E1:2003](https://standards.iteh.ai/catalog/standards/sist/d4c9bf4c-28e8-4c15-9bd4-c3212ef42ab4/sist-ets-300-791-e1-2003)

<https://standards.iteh.ai/catalog/standards/sist/d4c9bf4c-28e8-4c15-9bd4-c3212ef42ab4/sist-ets-300-791-e1-2003>

## Contents

Foreword .....	5
Introduction .....	5
1 Scope .....	7
2 Normative references .....	7
3 Abbreviations .....	8
4 Test Suite Structure (TSS) .....	8
5 Test purposes .....	9
5.1 Terminal test group .....	9
5.1.1 CHV test purposes .....	9
5.1.2 Two-pass strong authentication test purposes .....	10
5.1.3 Timer test purposes .....	10
5.2 UPT card test group .....	10
5.2.1 CHV test purposes .....	11
5.2.2 Two-pass strong authentication test purposes .....	11
5.2.3 Timer test purposes .....	12
5.3 Authentication Entity (AE) test group .....	12
5.3.1 PUI check test purposes .....	13
5.3.2 Two-pass strong authentication test purposes .....	13
5.3.3 SAPIN verification test purposes .....	14
5.3.4 OCPIN verification test purposes .....	14
5.3.5 PIN change test purpose .....	15
6 Test methods and configurations .....	15
6.1 Card reading terminal .....	15
6.2 UPT card .....	16
6.3 AE .....	16
7 Test cases .....	17
7.1 UPT card reading terminal .....	18
7.1.1 CHV .....	18
7.1.2 Two-pass strong authentication .....	19
7.1.3 Timer .....	20
7.2 UPT card .....	21
7.2.1 CHV .....	21
7.2.2 Two-pass strong authentication .....	23
7.2.3 Timer .....	23
7.3 AE .....	24
7.3.1 PUI check .....	24
7.3.2 Two-pass strong authentication .....	24
7.3.3 SAPIN check .....	25
7.3.4 OCPIN check .....	25
7.3.5 Change PIN check .....	26
History .....	27

Blank page

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

SIST ETS 300 791 E1:2003

<https://standards.iteh.ai/catalog/standards/sist/d4c9bf4c-28e8-4c15-9bd4-c3212ef42ab4/sist-ets-300-791-e1-2003>

## Foreword

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

This ETS, in association with ETS 300 790 [1], forms the specification of the security architecture for UPT Phase 2.

Transposition dates	
Date of adoption:	3 October 1997
Date of latest announcement of this ETS (doa):	31 January 1998
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 July 1998
Date of withdrawal of any conflicting National Standard (dow):	31 July 1998

## Introduction

Universal Personal Telecommunication (UPT) is a service that enables improved access to telecommunication service by allowing personal mobility. It enables each UPT user to participate in a user defined set of subscribed services, and to initiate and receive calls on the basis of a unique, personal, network independent UPT number across multiple networks at any terminal, fixed, movable or mobile.

ETS 300 790 [1] specifies the additions of UPT Phase 2, compared to UPT Phase 1, as specified in ETS 300 391-1 [3]. The Conformance Test Specification (CTS) for ETS 300 391-1 [3] is specified in ETS 300 391-3 [4].

This ETS specifies the conformance tests for ETS 300 790 [1] only.

In ETS 300 790 [1] a card, two-pass strong authentication, a mechanism for extra authentication for outgoing calls, authentication for secure answer and storage of a timer value in the card have been introduced. The conformance tests for these new features are all specified in this ETS.

Blank page

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ETS 300 791 E1:2003](https://standards.iteh.ai/catalog/standards/sist/d4c9bf4c-28e8-4c15-9bd4-c3212ef42ab4/sist-ets-300-791-e1-2003)

<https://standards.iteh.ai/catalog/standards/sist/d4c9bf4c-28e8-4c15-9bd4-c3212ef42ab4/sist-ets-300-791-e1-2003>



## 1 Scope

This European Telecommunication Standard (ETS) provides a Conformance Test Specification (CTS) specifying the tests which are necessary to verify the conformance of UPT cards, UPT card reading terminals and Authenticating Entities (AEs) with ETS 300 790 [1].

In particular, the following issues are considered:

- test suite and test purposes;
- test methods and configurations;
- test steps and test cases.

The Tree and Tabular Combined Notation (TTCN) description of test cases is outside the scope of this ETS. However, the TTCN description may be part of the CTSS of the overall Universal Personal Telecommunication (UPT) protocol specifications.

A partial Protocol Implementation eXtra Information for Testing (PIXIT) proforma is not identified as applicable for this CTS.

The conformance testing methodology and framework used in this ETS is given in ISO/IEC 9646 Parts 1–5 [2] and ETS 300 406 [5].

## 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] prETS 300 790: "Universal Personal Telecommunication (UPT); Security architecture for UPT Phase 2; Specification".  
<https://standards.itec.int/catalog/standards/sist/d4c9b46-28e8-4e15-9bd4-c3212e42ab4/sist-ets-300-791-e1-2003>
- [2] ISO/IEC 9646, Parts 1-5: "Conformance Testing Methodology and Framework".
- [3] ETS 300 391-1: "Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT Phase 1; Part 1: Specification".
- [4] ETS 300 391-3: "Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT Phase 1; Part 3: Conformance Test Specification (CTS)".
- [5] ETS 300 406: "Methods for Testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

### 3 Abbreviations

For the purposes of this ETS, the following abbreviations apply:

AC	Authentication Code, calculated in the UPT card
AE	Authenticating Entity
CHV	Card Holder Verification
CT	Command Type
IUT	Implementation Under Test
K	Key
OCPIN	Outgoing Call PIN
PCO	Point of Control and Observation
PIN	Personal Identification Number
PIXIT	Protocol Implementation eXtra Information for Testing
PUI	Personal User Identity
SAPIN	Secure Answer PIN
SDF	Service Data Function
TSS	Test Suite Structure
TTCN	Tree and Tabular Combined Notation
UPT	Universal Personal Telecommunication

### 4 Test Suite Structure (TSS)

A full conformance test of a UPT Phase 2 implementation shall be based on both ETS 300 391-3 [4] and this ETS.

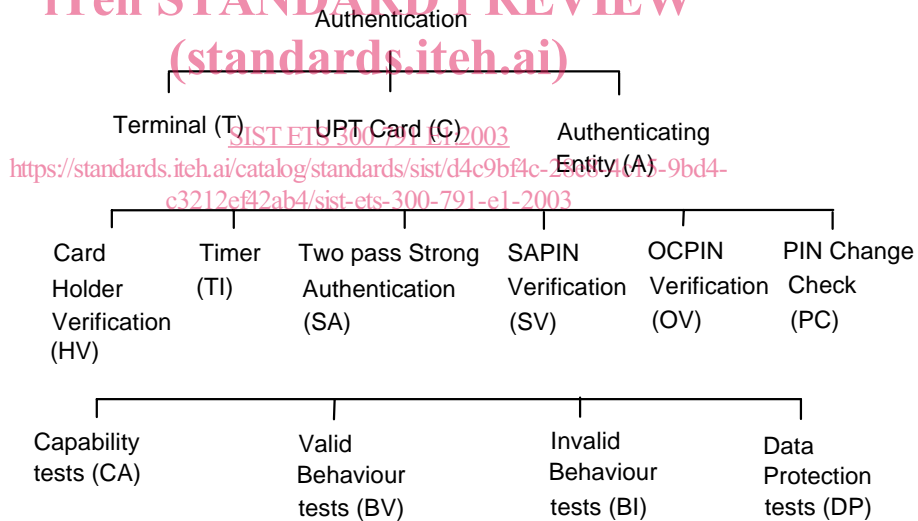
Figure 1 shows the Test Suite Structure (TSS).

#### Security feature

#### Implementation under test

#### Major functions

#### Nature of test



**Figure 1: The TSS**

The characters within parenthesis in figure 1 are used in the mnemonics identifying each test purpose in the following clauses. Every mnemonic consists of four fields:

- (implementation under test);
- (major function);
- (nature of test);
- (number within the test group).

EXAMPLE:                      Capability test number 1 of the two-pass strong authentication of the terminal is coded TSACA1.

## 5 Test purposes

Three entities in the UPT security architecture have been identified to need testing:

- the terminal;
- the UPT card;
- and the AE.

There are two objectives to be met:

- to ensure that both entities have been implemented in accordance with the requirements stated in ETS 300 790 [1];
- to achieve interoperability between products from different manufacturers.

The references made in this clause can be found in ETS 300 790 [1].

### 5.1 Terminal test group

The terminal is tested with respect to the following aspects:

- Card Holder Verification (CHV) is supported by the terminal;
- the data for strong authentication is correctly sent;
- the timer is correctly implemented.

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

#### 5.1.1 CHV test purposes

[SIST ETS 300 791 E1:2003](https://standards.iteh.ai/standards/sist/300-791-e1-2003)

<b>THVCA1:</b>	Check that the terminal supports CHV.
<b>Initial conditions:</b>	The card is not blocked.
<b>Reference:</b>	Subclause 5.2.2 Authentication of the user to the UPT card.

<b>THVBV1</b>	Check that changing of the CHV is supported by the terminal.
<b>Initial conditions:</b>	The card is not blocked. The card is reset.
<b>Reference:</b>	Subclause 7.3 User interface.

<b>THVBV2:</b>	Check that unblocking CHV is supported by the terminal.
<b>Initial conditions:</b>	The card is blocked.
<b>Reference:</b>	Subclause 7.3 User interface.