SLOVENSKI STANDARD
SIST ETS 300 391-3 E1:2003

01-december-2003

Svetovne osebne telekomunikacije (UPT) – Specifikacija varnostne arhitekture za 1. fazo sistema UPT – 3. del: Specifikacija za preskušanje skladnosti (CST)

Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT phase 1; Part 3: Conformance Test Specification (CTS)

Ta slovenski standard je istoveten z: ETS 300 391-3 Edition 1

ICS:

33.040.35 Telefonska omrežja Telephone networks

SIST ETS 300 391-3 E1:2003 **en**

EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 391-3

August 1995

Source: ETSI TC-NA

Reference: DE/NA-071403

ICS: 33.040

Key words: Authentication, DTMF, security, UPT

Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT phase 1; Part 3: 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 92 94 42 00 - Fax: +33 93 65 47 16

Contents

Blank page

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 consists of 3 parts as follows:

Part 1: "Specification".

Part 2: "Implementation Conformance Statement (ICS) proformas".

Part 3: "Conformance Test Specification (CTS)".

Transposition dates	
Date of adoption of this ETS:	28 July 1995
Date of latest announcement of this ETS (doa):	30 November 1995
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 May 1996
Date of withdrawal of any conflicting National Standard (dow):	31 May 1996

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.

ETSI Sub Technical Committee (STC) NA 7 has defined three service scenarios for UPT (see ETR 055-2). The specification of the security architecture for UPT phase 1 (ETS 300 391-1 [1]) deals only with the restricted, short term UPT service scenario for UPT phase 1. This scenario has restrictions on networks, services, user friendliness and also on the possibilities to implement security features.

ETS 300 391-1 [1] has specified the mechanisms for weak and strong authentication. The detailed specification of the protocols within the Intelligent Network will be described elsewhere as part of the specification of the overall UPT protocols.

Blank page

1 Scope

This European Telecommunication Standard (ETS) provides a Conformance Test Specification (CTS) specifying the tests which are necessary to verify the conformance of advanced Dual Tone Multi Frequency (DTMF) devices and Authenticating Entities (AEs) with ETS 300 391-1 [1] and ETS 300 391-2 [2].

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 [4].

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

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

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

[4] ISO/IEC 9646, parts 1 - 5: "Conformance Testing Methodology and Framework".

3 Abbreviations

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

AC	Authentication Code, calculated in the UPT access device
AE	Authenticating Entity
d	tolerance for the difference between the sequence number sent by the UPT access device and the sequence number stored in the SDF
DHV	Device Holder Verification
DTMF	Dual Tone Multi Frequency
f	algorithm for the calculation of the AC
IUT	Implementation Under Test
K	Key
LPIN	Local Personal Identification Number
n	sequence number, used by the UPT access device
n_s	sent part of the sequence number, i.e. the 16 least significant bits of n
PCO	Point of Control and Observation
PIN	Personal Identification Number
PIXIT	Protocol Implementation eXtra Information for Testing
PUI	Personal User Identity
SDF	Service Data Function
SLPIN	Special Local Personal Identification Number
SPIN	Special Personal Identification Number
TSS	Test Suite Structure
TTCN	Tree and Tabular Combined Notation
UPT	Universal Personal Telecommunication

4 Test suite structure

Figure 1 shows the Test Suite Structure (TSS).

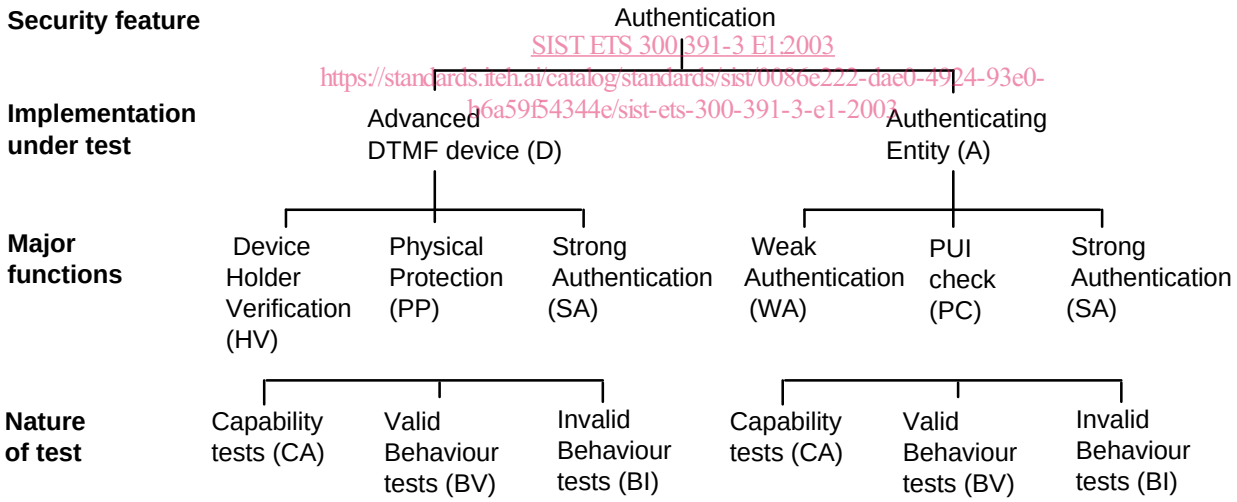

Figure 1: The TSS

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

a) {implementation under test};
b) {major function};
c) {nature of test};
d) {number within the test group}.

EXAMPLE: Capability test number 1 of the strong authentication of the advanced DTMF device is coded DSACA1.

5 Test purposes

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

- the advanced DTMF device; 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 300 391-1 [1];
- to achieve interoperability between products from different manufacturers.

The references made in this clause can be found in ETS 300 391-1 [1].

5.1 Advanced DTMF device test group

The advanced DTMF device is tested with respect to the following aspects:

- Device Holder Verification (DHV) is correctly implemented;
- the data for strong authentication is correctly sent;
- sensitive data is physically protected.

5.1.1 DHV test purposes

DHVCA1:	Check that the device can perform DHV (covered by DHVBV1 and DHVBI1).
Initial conditions:	The device is not blocked.
Reference:	8 requirements for the security module and 8.2 processing.

DHVBV1:	Check that the authorised user is accepted by the DHV.
Initial conditions:	The device is not blocked.
Reference:	8.2 processing.

DHVBV2:	Check that authentication attempts can be performed after a successful DHV.
Initial conditions:	The device is not blocked.
Reference:	8.2 processing.

DHVBI1:	Check that incorrect DHV attempts fail.
Initial conditions:	The device not being blocked.
Reference:	8 requirements for the security module, 8.2 processing.

DHVBI2:	Check that no authentication attempt can be performed without a previous successful DHV.
Initial conditions:	None.
Reference:	8.2 processing.

DHVBI3:	Check that an authentication attempt cannot be performed when the time-out has been reached.
Initial conditions:	A successful DHV has been performed.
Reference:	8.2 processing.