EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 391-2

August 1995

Source: ETSI TC-NA

Reference: DE/NA-071404

ICS: 33.040

Key words: Authentication, DTMF, UPT

Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT phase 1; Part 2: Implementation Conformance Statement (ICS) proformas

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

To evaluate conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented. Such a statement is called an Implementation Conformance Statement (ICS).

Blank page

1 Scope

This European Telecommunication Standard (ETS) provides the Implementation Conformance Statement (ICS) proformas for the advanced Dual Tone Multi Frequency (DTMF) device and the Authenticating Entity (AE) specified in ETS 300 391-1 [1]. These components relate to the authentication procedures of UPT phase 1. They are the most relevant components for interoperability and the overall security.

This ETS allows either the service provider of a UPT system to formulate the requirements on these implementations or to decide whether an implementation meets these requirements. It details the in tabular form mandatory and optional functions for these implementations.

This ETS is in compliance with the relevant requirements and the guidelines given in ISO/IEC 9646-2 [2].

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 Telecommunications (UPT); Specification of the security architecture for UPT Phase 1; Part 1: Specification".

[2] ISO/IEC 9646-2: "Conformance testing methodology and framework".

3 Symbols and abbreviations

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

AC	Authentication Code, calculated in the UPT access device
AC'	Authentication Code, calculated in the AE
AE	Authenticating Entity
DHV	Device Holder Verification
DTMF	Dual Tone Multi Frequency
LPIN	Local Personal Identification Number
n	sequence number, used by the UPT access device
n'	expected sequence number, stored in the AE
n_s	sent part of the sequence number, i.e. the 16 least significant bits of n
PIN	Personal Identification Number
PUI	Personal User Identity
RAA	Remaining Authentication Attempts
SM	Security Module (in the DTMF device)
SPIN	Special Personal Identification Number

4 Conformance

A supplier of implementations of advanced DTMF devices or AEs which are claimed to conform to ETS 300 391-1 [1] is required to complete a copy of the relevant ICS proforma provided in this ETS and is required to provide the information necessary to identify both the supplier and the implementation.

5 ICS proforma for advanced DTMF devices

The purpose of the ICS proforma is to submit suppliers and implementors with a questionnaire or checklist. This should be completed in order to state conformance with the requirements put forward in the relevant standard.

5.1 Identification of the implementation, product supplier and test laboratory client

For administrative purposes the actual ICS shall identify:

- the implementation;
- the supplier or client of the test laboratory that is to test the implementation;
- the person to contact if there are any queries regarding the ICS.

5.2 Identification of the standard

This ICS proforma applies to ETS 300 391-1 [1].

5.3 Global statement of conformance

The implementation described in this ICS meets all the mandatory requirements of the referenced standard.

( ) Yes

( ) No

NOTE: Answering "No" to this question indicates non-conformance to the UPT security architecture. Non-supported mandatory capabilities are to be identified in the ICS, with an explanation of why the implementation is non-conforming.

5.4 Main features

Table 1: Advanced DTMF device

A1				
Item	**Features**	**Ref.**	**Status**	**Support**
1	Sensitive information is physically protected, i.e. by a Security Module (SM)	8.1	m	
2	A Device Holder Verification (DHV) method is implemented in the device	8	c1	
3	The device implements an authentication algorithm	8.1	m	

c1 = IF the UPT service provider is not performing the DHV in the central system.

Table 2: Security module

A11				
Item	**Features**	**Ref.**	**Status**	**Support**
1	The authentication key is contained in the SM	8.2	m	
2	The authentication algorithm is contained in the SM	8.2	m	
3	DHV data is contained in the SM	8.2	c2	
4	Value of key cannot be changed by the user	8.1	m	

c2 = IF A1, item 2.

Table 3: Local DHV (in device)

A12					
Item	**Features**	**Ref.**	**Status**	**Support**	**Value Supported**
1	Authentication can not be performed before DHV is performed	8.2	c2		---
2	Correct DHV entry starts a timer in the device	8.2.1	c2		
3	After the time out expires the authentication process in the device can no longer be activated without a new DHV being performed	8.2.1	c2		---
4	DHV is implemented by a Local Personal Identification Number (LPIN)	8	o		---

c2 = IF A1, item 2.

Table 4: Authentication process

A13				
Item	**Features**	**Ref.**	**Status**	**Support**
1	Authentication Code (AC) is derived from the authentication key and n	8.2.2	m	
2	n_S is derived from n	8.2.3	m	
3	n is incremented by one for every authentication process	8.2.5	m	
4	Device produces the authentication output as DTMF tones	9.3.2	m	

Table 5: Authentication algorithms

A131				
Item	**Features**	**Ref.**	**Status**	**Support**
1	Authentication output using the UPT algorithm	11.1	o1	
2	Authentication output using the TESA 7	11.2	o1	
3	Authentication output using a proprietary algorithm	11.3	o1	

o1 = one of the options shall be supported.

6 ICS proforma for the AE

The purpose of the ICS proforma is to submit suppliers and implementors with a questionnaire or checklist. This should be completed in order to state conformance with the requirements put forward in the relevant standard.

6.1 Identification of the implementation, product supplier and test laboratory client

For administrative purposes the actual ICS shall identify:

- the implementation;

- the supplier or client of the test laboratory that is to test the implementation;

- the person to contact if there are any queries regarding the ICS.

6.2 Identification of the standard

This ICS proforma applies to ETS 300 391-1 [1].

6.3 Global statement of conformance

The implementation described in this ICS meets all the mandatory requirements of the referenced standard.

( ) Yes

( ) No

NOTE: Answering "No" to this question indicates non-conformance to the UPT security architecture. Non-supported mandatory capabilities are to be identified in the ICS, with an explanation of why the implementation is non-conforming.

6.4 Main features

Table 6: AE

B1				
Item	**Features**	**Ref.**	**Status**	**Support**
1	AE supports weak authentication	6.2.1	o2	
2	AE supports strong authentication	6.2.2	o2	
3	AE supports checking of blacklisted Personal User Identities (PUIs)	6.1.1	m	

o2 = one of the options or both shall be supported.

Table 7: AE supports weak authentication

B11					
Item	**Features**	**Ref.**	**Status**	**Support**	**Values supported**
1	Personal Identification Number (PIN) has a length between 6 and 10 digits	7	m		
2	PIN change is possible	10.2.1	m		---
3	The PUI is blocked after a number of incorrect PIN entries (Remaining Authentication Attempts (RAA) counter value)	6.2.1	m		
4	Blocking is disabled by use of Special Personal Identification Number (SPIN), which has a length between 8 and 12 digits	6.2.1 7	o		
5	The number of unblocking attempts is limited	6.2.1	o		

Table 8: AE supports strong authentication

B12					
Item	**Features**	**Ref.**	**Status**	**Support**	**Values supported**
1	AE checks that n_S is inside the allowed range	6.2.2 10.3.2	m		
2	AE accepts authentication if calculated AC' equals received AC	6.2.2	m		---
3	After successful authentication n' is increased to n+1	6.2.2 10.3.2	m		---

History

Document history	
December 1994	Public Enquiry PE 75: 1994-12-05 to 1995-03-31
May 1995	Vote V 80: 1995-05-22 to 1995-07-28
August 1995	First Edition
January 1996	Converted into Adobe Acrobat Portable Document Format (PDF)

ISBN 2-7437-0216-8 - Edition complète
ISBN 2-7437-0218-4 - Partie 2
Dépôt légal : Août 1995