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).

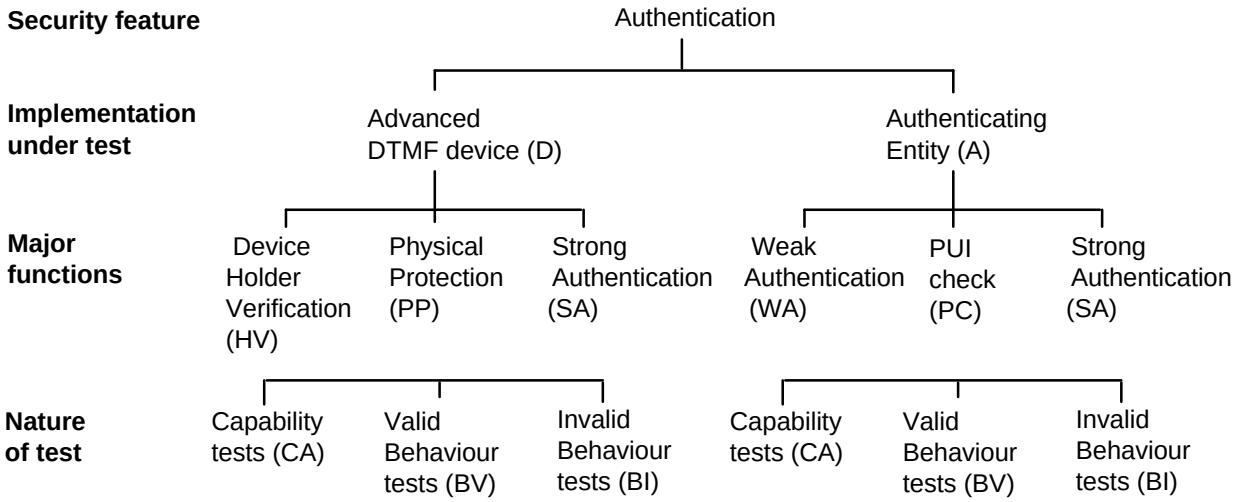


Figure 1: The TSS

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.

5.1.2 Strong authentication test purposes

DSACA3:	Check that the Authentication Code (AC) is correctly calculated and correctly converted to DTMF signals by the device.
Initial conditions:	A DHV has been successfully performed and the time-out has not been reached. The expected value of AC and the value of n and K used are known by the tester.
Reference:	11 authentication algorithms and 8.2 processing.

DSABV3:	Check that n is incremented by one at every authentication attempt.
Initial conditions:	n is known by the tester and it has not reached its maximum value.
Reference:	8.2.5 Sequence number incrementation.

DSACA4:	Check that the conversion of n to n_S as DTMF signals has been correctly performed.
Initial conditions:	A successful DHV has been performed.
Reference:	8.2.3 Sequence number conversion.

DSABV1:	Check that the data field CT is correctly coded.
Initial conditions:	An authentication attempt has been made.
Reference:	9.3.2 The authentication process.

5.1.3 Physical protection test purposes

DPPCA1:	Check that the Personal User Identity (PUI), n and K cannot be written into the device by a user.
Initial conditions:	None.
Reference:	8.1 Storage of data.

DPPCA2:	Check that K and the authentication algorithm cannot be read out from the device.
Initial conditions:	None.
Reference:	8.1 Storage of data.

5.2 AE test group

The AE is tested with respect to the following aspects:

- PUI check is implemented;
- strong authentication is correctly implemented;
- and/or weak authentication is correctly implemented.

5.2.1 PUI check test purposes

APCCA1:	Check that received PUIs are checked with respect to validity at every authentication attempt.
Initial conditions:	Authentication data has been received.
Reference:	6.2 User authentication mechanisms and 10 requirements for the AE of the Service Data Function (SDF).

APCCA2:	Check that received PUIs are checked against a blacklist at every authentication attempt.
Initial conditions:	Authentication data has been received.
Reference:	6.2 User authentication mechanisms and 10 requirements for the AE of the SDF.

5.2.2 Weak authentication test purposes

AWACA1:	To check that the Personal Identification Number (PIN) is checked by the AE (covered by AWABV1 and AWABI1).
Initial conditions:	The AE supports weak authentication. A valid not blacklisted PUI has been sent to the AE. The PUI is not blocked.
Reference:	6.2.1 weak authentication and 10.2 weak authentication.

AWABV1:	To check that a correct PIN presentation results in a successful authentication.
Initial conditions:	The AE supports weak authentication. A valid not blacklisted PUI has been sent to the AE. The PUI is not blocked.
Reference:	6.2.1 weak authentication and 10.2 weak authentication.

AWABI1:	To check that a correct PIN presentation results in authentication failure and does not unblock the PUI, if it is blocked.
Initial conditions:	The AE supports weak authentication. The PUI is blocked.
Reference:	6.2.1 weak authentication and 10.2 weak authentication.

AWABI2:	To check that a wrong PIN presentation results in a authentication failure.
Initial conditions:	The AE supports weak authentication. A valid not blacklisted PUI has been sent to the AE. The PUI is not blocked.
Reference:	6.2.1 weak authentication and 10.2 weak authentication.

AWABI3:	To check that the PUI is blocked in case wrong PIN is given a predefined number of times consecutively.
Initial conditions:	The AE supports weak authentication. The PUI is not blocked.
Reference:	6.2.1 weak authentication.

AWACA2:	To check that the PIN can be changed by the user.
Initial conditions:	The AE supports weak authentication. A successful weak authentication has been performed.
Reference:	6.2.1 weak authentication and 10.2 weak authentication.

AWABI4:	To check that the PIN is not changed only if the two PINs given are not equal.
Initial conditions:	The AE supports weak authentication. Authentication data has been received and the PUI has been checked and accepted by the AE.
Reference:	6.2.1 weak authentication and 10.2 weak authentication.

AWABV2:	To check that a correct presentation of the Special Personal Identification Number (SPIN) unblocks the PUI.
Initial conditions:	The AE supports weak authentication and on-line unblocking. The PUI is blocked.
Reference:	6.2.1 weak authentication.

AWABI5:	To check that a wrong SPIN does not unblock a blocked PUI.
Initial conditions:	The AE supports weak authentication. The PUI is blocked.
Reference:	6.2.1 weak authentication and 10.2 weak authentication.

5.2.3 Strong authentication test purposes

ASABV1:	To check that the accepted range of n is updated after each successful authentication.
Initial conditions:	The AE supporting strong authentication. A successful strong authentication has been performed.
Reference:	6.2.2 Strong authentication and 10 requirements for the AE of the SDF.

ASABI1:	To check that authentication fails if n is outside the accepted range.
Initial conditions:	The AE supports strong authentication. PUI has been checked and accepted and authentication data has been received.
Reference:	6.2.2 Strong authentication and 10 requirements for the AE of the SDF.

ASACA1:	To check that the AC is checked by the AE (covered by ASABV2 and ASABI2).
Initial conditions:	The AE supports strong authentication. A valid not blacklisted PUI has been sent to the AE.
Reference:	6.2.2 Strong authentication and 10 requirements for the AE of the SDF.

ASABV2:	To check that a correct AC results in a successful authentication.
Initial conditions:	The AE supports strong authentication. A valid not blacklisted PUI and n_S, within its accepted range, has been sent to the AE.
Reference:	6.2.2 Strong authentication and 10 requirements for the AE of the SDF. K, n and the expected AC is known by the tester.

ASABI2:	To check that an incorrect AC value results in authentication failure.
Initial conditions:	The AE supports strong authentication. A valid not blacklisted PUI has been sent to the AE. K, n and the expected AC is known by the tester.
Reference:	6.2.2 Strong authentication and 10 requirements for the AE of the SDF.

6 Test methods and configurations

This clause describes the methods and configurations to test the advanced DTMF device and the AE. The Implementation Under Test (IUT), the upper tester, the lower tester, and the Points of Control and Observation (PCOs) are described in detail.

All protocols that are described in ETS 300 391-1 [1] are application protocols. Therefore, only the application layer is considered.

6.1 Advanced DTMF device

The security related tests of the advanced DTMF device should be done together with the other tests according to I-ETS 300 380 [3]. The tests shall be done locally.

The PCOs are the keyboard and the display of the advanced DTMF device (interface to the upper tester) and the loudspeaker of the advanced DTMF device together with the microphone of the lower tester (interface to the lower tester). This is shown in figure 2.

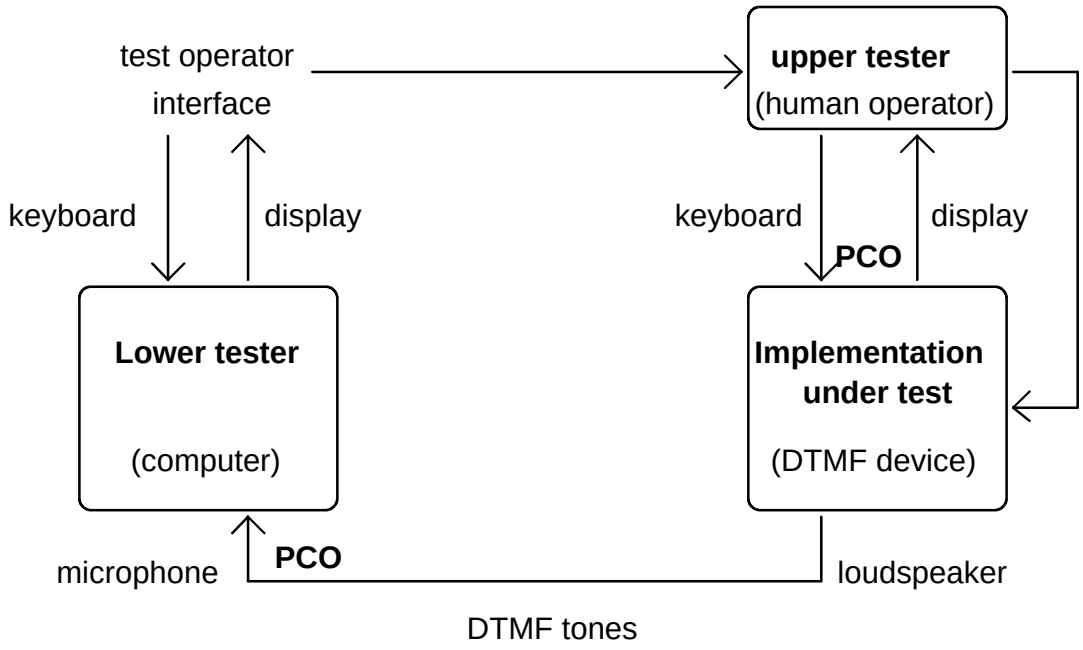


Figure 2: Advanced DTMF device

The values for PUI, key, and sequence number can not be entered directly into the advanced DTMF device. The manufacturer shall implement these values according to the requirements of the test laboratory. The interface for this procedure is not standardized.

The sequence number is automatically incremented by 1 after each authentication attempt.

The values for DHV (e.g. Local Personal Identification Number (LPIN), Special Local Personal Identification Number (SLPIN), new LPIN) are entered via the keyboard of the advanced DTMF device (if not specified differently by the manufacturer). The request for authentication is entered via the keyboard of the advanced DTMF device.

The output of the advanced DTMF device is done by DTMF tones in case of an authentication attempt.

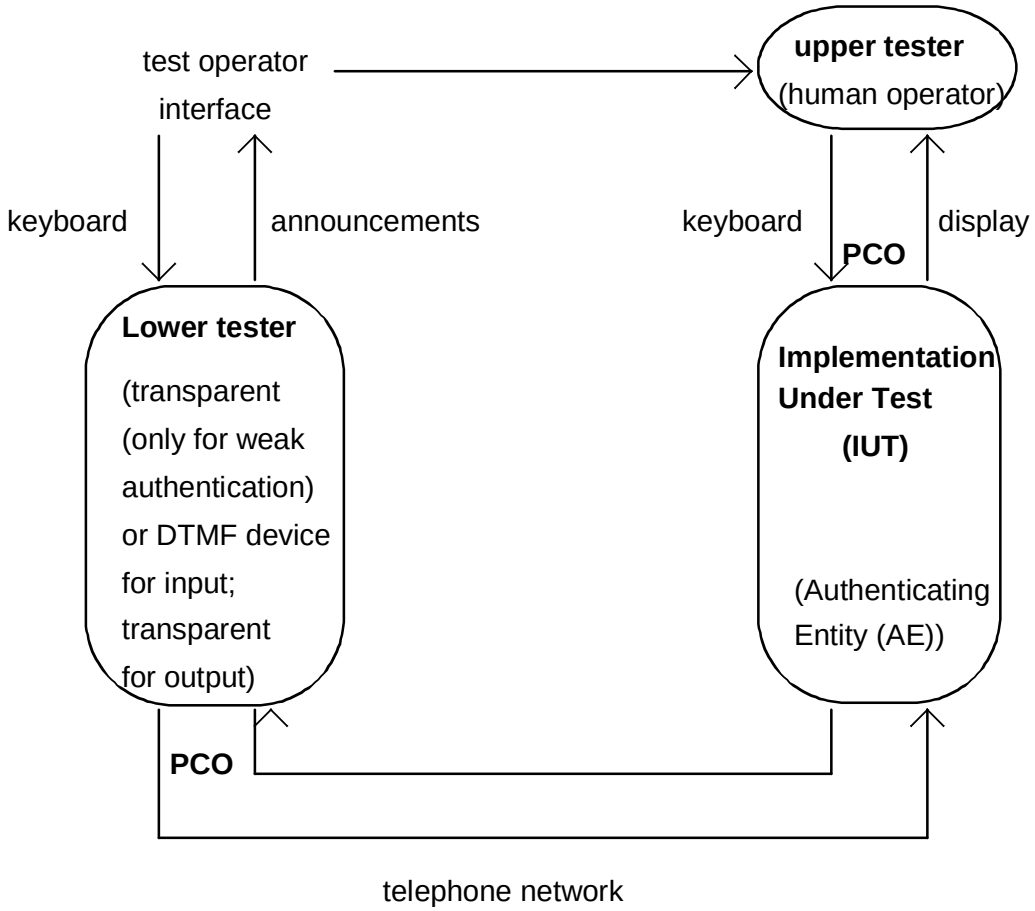
If a DHV procedure (e.g. unblocking by use of an SLPIN or change of the LPIN) is performed, the result (successful or not successful) may be indicated in a display of the advanced DTMF device. In any case, the result can be tested by succeeding authentication attempts.

The timer can be tested by waiting the appropriate time between DHV and authentication.

6.2 AE

The AE shall be tested by the "distributed test method (M)". The test laboratory shall choose the values for the identification and authentication parameters which shall be implemented into the AE as well as into the advanced DTMF device (if applicable).

The PCO at the lower tester is the keyboard of the telephone or advanced DTMF device (if applicable) and the loudspeaker of the telephone (or a simulator of these entities). The PCO at the upper tester might be a standardized software interface or a human operator interface. The testing architecture is shown in figure 3.



_____ test coordination procedure:

- selection of PUI, key, (initial) sequence number in case of strong authentication;
- selection of PUI, (initial) PIN, SPIN in case of weak authentication.

Figure 3: Authenticating entity

NOTE: In addition to this, there will be other (possibly local) test configurations when the protocols between the IN entities are specified in detail. Then the security related protocol elements may be tested together with the other UPT protocol elements.

6.2.1 Strong authentication

The values for PUI, key, and (initial) sequence number shall be implemented into the AE by the manufacturer according to the requirements of the test laboratory. The interface for this procedure is not standardized. It will normally be done via an operator terminal.

The sequence number in the AE is automatically updated after each successful authentication attempt.

The request for authentication is entered via the keyboard of an advanced DTMF device, after DHV.

The result of an authentication attempt (successful or not successful) is given by an appropriate announcement.

6.2.2 Weak authentication

The values for PUI, (initial) PIN and SPIN shall be implemented into the AE by the manufacturer according to the requirements of the test laboratory. The interface for this procedure is not standardized. It will normally be done via an operator terminal.

The values for PUI, PIN, SPIN, new PIN are entered directly into the (DTMF capable) telephone or via the keyboard of a (simple) DTMF device; also the request for authentication.

The result of an authentication attempt (successful or not successful) is given by an appropriate announcement.

If an unblocking (by use of an SPIN) or a PIN change is performed, the result (successful or not successful) shall be indicated by an appropriate announcement. Additionally, the result can be tested by succeeding authentication attempts.

7 Test cases

The following information is included in the specification of each test case:

- name of the test case;
- reference to the corresponding test purpose;
- specification of test steps;
- expected result (conditions to be fulfilled to pass the test).

7.1 Advanced DTMF device

The following test cases of the advanced DTMF device are specified:

- DHV;
- strong authentication.

The physical protection of sensitive data in the advanced DTMF device is considered to be non-testable.

7.1.1 DHV

T C 1:	Fulfils the test purposes DHVBV1 and DHVBV2.
Test steps:	1) Switch on the device. 2) Perform a correct DHV. 3) Activate the authentication procedure. 4) Record the output data.
Expected result:	Authentication data shall be sent by the device.

T C 2:	Fulfils the test purpose DHVBI1 and DHVBI2.
Test steps:	1) Switch on the device. 2) Perform an incorrect DHV. 3) Activate the authentication procedure. 4) Record the output data.
Expected result:	No authentication data shall be sent by the device.

T C 3:	Fulfils the test purpose DHVBI3.
Test steps:	1) Switch on the device. 2) Perform a correct DHV. 3) Wait for the time-out. 4) Activate the authentication procedure. 5) Record the output data.
Expected result:	No authentication data shall be sent by the device.

7.1.2 Strong authentication

T C 4:	Fulfils the test purposes DSACA1, DSABV1, DSACA2 and DSABV2.
Test steps:	1) Switch on the device. 2) Perform a successful DHV. 3) Activate the authentication procedure before the time out has been reached. 4) Record the output data sent by the device. 5) Activate the authentication procedure. 6) Record the output data sent by the device.
Expected result after step 4:	The result shall be in DTMF signals :*PUI*CT*n_{S1}*AC1# , all values shall be correct.
Expected result after step 6:	The result shall be in DTMF signals :*PUI*CT*n_{S2}*AC2#, all values shall be correct. The value of $n_{S2} = n_{S1}+1$. The value of AC2= depends on n_{S2} and the algorithm used.

7.1.3 Physical protection

Test purposes DPPCA1 and DPPCA2 are considered to be untestable.

7.2 AE

In this subclause, the data shall be sent to the AE according to the correct syntax specified in ETS 300 391-1 [1].

The following major functions shall be tested:

- the PUI check;
- weak authentication, if it is implemented;
- strong authentication, if it is implemented.

7.2.1 PUI check

T C 5:	Fulfils the test purpose APCCA1.
Test steps:	1) Send authentication data with an invalid PUI to the AE.
Expected result:	Authentication failure.

T C 6:	Fulfils the test purpose APCCA2.
Test steps:	1) Send authentication data with a PUI blacklisted to the AE.
Expected result:	Authentication failure.

7.2.2 Weak authentication.

T C 7:	Fulfils the test purpose AWABV1.
Test steps:	1) Perform the weak authentication procedure with a correct PUI and the corresponding correct PIN.
Expected result:	Successful authentication.

T C 8:	Fulfils the test purposes AWABI1, AWABI2 and AWABI3.
Test steps:	1) Perform the weak authentication procedure with correct PUI but wrong PIN.
Expected result:	Authentication failure.

T C 9:	Fulfils the test purpose AWABI5.
Test steps:	1) Perform the unblocking procedure with a blocked PUI and wrong SPIN.
Expected result:	Authentication failure.

T C 10:	Fulfils the test purpose AWABV2.
Test steps:	1) Perform the unblocking procedure with a blocked PUI and the corresponding correct SPIN. 2) Perform the weak authentication procedure with the now unblocked PUI and the corresponding correct PIN.
Expected result after step 1:	Successful authentication.
Expected result after step 2:	Successful authentication.

T C 11:	Fulfils the test purpose AWACA2.
Test steps:	1) Perform a successful weak authentication procedure. 2) Perform a successful change PIN procedure. 3) Disconnect. 4) Perform the weak authentication procedure with the new PIN. 5) Perform the weak authentication procedure with the old PIN.
Expected result after step 4:	Successful authentication.
Expected result after step 5:	Authentication failure.

T C 12:	Fulfils the test purpose AWABI4.
Test steps:	1) Perform a successful weak authentication. 2) Perform the change PIN procedure with two different values for the new PIN. 3) Disconnect. 4) Perform the weak authentication procedure with one of the PIN values given in step 2. 5) Perform the weak authentication with the same values as in step 1.
Expected result after step 4:	Authentication failure.
Expected result after step 5:	Successful authentication.

7.2.3 Strong authentication.

T C 13:	Fulfils the test purposes ASABI1.
Test steps:	1) Perform the strong authentication procedure, with an n outside the accepted range. The other parameters shall be correct.
Expected result:	Authentication failure.

T C 14:	Fulfils the test purposes ASABV1 and ASBV2.
Test steps:	1) Perform the strong authentication procedure with an n within the accepted range and AC calculated with the correct algorithm and correct key. 2) Perform the strong authentication procedure using n+d instead of n+1.
Expected result after step 1:	Successful authentication.
Expected result after step 2:	Successful authentication.

T C 15:	Fulfils the test purpose ASABI2.
Test steps:	1) Perform the strong authentication procedure using the wrong key, but a correct PUI and n within the accepted range.
Expected result:	Authentication failure.

Annex A (informative): Bibliography

1) ETS 300 406: "Methods for Testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization Methodology".

2) ETR 021: "Advanced Testing Methods (ATM); Tutorial on protocol conformance testing (Especially OSI standards and profiles) (ETR/ATM-1002)".

3) ETR 022: "Advanced Testing Methods (ATM); Vocabulary of terms used in communications protocols conformance testing".

4) ETR 055-1: "Universal Personal Telecommunication (UPT); The service concept; Part 1: Principles and objectives".

5) ETR 055-2: "Universal Personal Telecommunication (UPT); The service concept; Part 2: General service description".

6) ETR 083: "Universal Personal Telecommunication (UPT); General UPT security architecture".

7) DTR/NA-010010: "Universal Personal Telecommunication (UPT); Phase 1; Service description".

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 2-7437-0219-2 - Partie 3
Dépôt légal : Août 1995