EUROPEAN TELECOMMUNICATION STANDARD

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

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, 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

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".

[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).

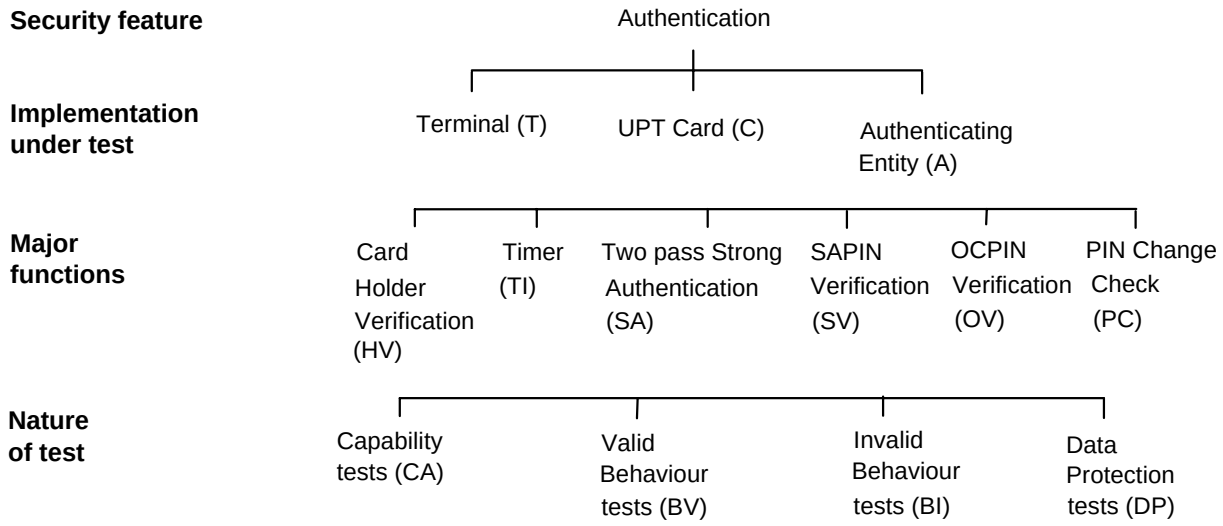

Figure 1: The TSS

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:

a) (implementation under test);
b) (major function);
c) (nature of test);
d) (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.

5.1.1 CHV test purposes

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

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

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

5.1.2 Two-pass strong authentication test purposes

TSACA1:	Check that two-pass strong authentication is supported.
Initial conditions:	-
Reference:	Subclause 5.2.1 Weak authentication..

5.1.3 Timer test purposes

TTICA1:	Check that the timer is implemented. Covered by TTIBV1, TTIBV2, TTIBV3 and TTIBI1.
Initial conditions:	The timer value T and T_{MAX} are known by the tester.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

TTIBV1:	Check that the timer is initiated with the timer value T from the card.
Initial conditions:	A successful CHV has been performed.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

TTIBV2:	Check that the user's access rights, granted by the CHV are lost when time-out is reached.
Initial conditions:	A successful CHV has been performed, and the timer has started.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

TTIBV3:	Check that the user can change the time-out value, T.
Initial conditions:	A successful CHV has been performed.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

TTIBI1:	Check that $T < T_{MAX}$ when it is changed.
Initial conditions:	A successful CHV has been performed and T_{MAX} is available in the card.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

5.2 UPT card test group

The UPT card is tested with respect to the following aspects:

- CHV;
- two-pass strong authentication;
- storage of T and T_{MAX} in the card.

5.2.1 CHV test purposes

CHVCA1:	Check that CHV has been implemented in the card. Covered by CHVCA2 and CHVCA3.
Initial conditions:	The card is reset.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

CHVCA2:	Check that the authentication algorithm cannot be used without a previous successful CHV. Covered by CHVBV1 and CHVBI1.
Initial conditions:	The card is reset.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

CHVCA3:	Check that the authentication algorithm cannot be used after reset.
Initial conditions:	A successful CHV is performed, a two-pass strong authentication is performed and then the card is reset.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

CHVBV1:	Check that presenting the correct CHV enables the two-pass strong authentication.
Initial conditions:	The card is reset.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

CHVBI1:	Check that presenting wrong CHV disables the two-pass strong authentication.
Initial conditions:	A successful CHV has been performed and the time-out has not been reached.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

CHVBI2:	Check that 3 consecutive wrong CHV presentations blocks the card.
Initial conditions:	A successful CHV has been performed.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

5.2.2 Two-pass strong authentication test purposes

CSACA1:	Check that two-pass strong authentication is supported by the card. Covered by CSABV1 and CSABV2.
Initial conditions:	A successful CHV has been performed and the time-out has not been reached.
Reference:	Subclause 5.2.1 Weak authentication..

CSABV1:	Check that the PUI and CT can be read out from the card.
Initial conditions:	A successful CHV has been performed.
Reference:	Subclause 5.2.1 Weak authentication..

CSABV2:	Check that the AC is correctly calculated by the card.
Initial conditions:	A successful CHV has been performed. The tester knows the expected result for the RAND and authentication key used by the algorithm in the card.
Reference:	Subclause 5.2.1 Weak authentication..

5.2.3 Timer test purposes

CTICA1:	Check that the stated time-out value, T, is stored in the card.
Initial conditions:	The tester knows the value of T.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

CTICA2:	Check that the stated maximum time-out value, T_{MAX}, is stored in the card.
Initial conditions:	The tester knows the value of T_{MAX}.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

CTIBI1:	Check that T cannot be changed without a previous CHV.
Initial conditions:	The card is reset.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

CTIBI2:	Check that the maximum time-out value, T_{MAX}, cannot be changed.
Initial conditions:	None.
Reference:	Subclause 5.2.2 Authentication of the user to the UPT card.

5.3 Authentication Entity (AE) test group

The AE is tested with respect to the following aspects:

- the PUI is checked;
- two-pass strong authentication is correctly implemented;
- SAPIN verification is correctly implemented;
- OCPIN verification is correctly implemented;
- PIN change check is correctly implemented.

5.3.1 PUI check test purposes

APCCA1:	Check that received PUIs are checked with respect to validity at every two–pass strong authentication attempt.
Initial conditions:	Authentication data has been received.
Reference:	Subclause 5.2 User authentication mechanisms.

APCCA2:	Check that received PUIs are checked against a blacklist at every two-pass strong authentication attempt.
Initial conditions:	Authentication data has been received.
Reference:	Subclause 5.2 User authentication mechanisms and 9.1 Check of PUI and authentication type used.

5.3.2 Two-pass strong authentication test purposes

ASACA1:	Check that two-pass strong authentication is supported. Covered by ASABV2 and ASABI1.
Initial conditions:	A valid not blacklisted PUI has been sent to the AE. The PUI is not blocked.
Reference:	Subclause 5.2.1 Weak authentication and 9.2 Two-pass strong authentication.

ASABV1:	Check that a new random number, RAND, is generated at each two-pass strong authentication attempt.
Initial conditions:	A valid not blacklisted PUI has been sent to the AE. The PUI is not blocked.
Reference:	Subclause 5.2.1 Weak authentication and 9.2 Two-pass strong authentication.

ASABV2:	Check that the authentication succeeds if AC' calculated by the AE equals to the received AC.
Initial conditions:	The PUI is not blocked or blacklisted. Authentication data has been received. The tester knows the expected AC.
Reference:	Subclause 5.2.1 Weak authentication and 9.2 Two-pass strong authentication.

ASABI1:	Check that an incorrect received AC results in a authentication failure.
Initial conditions:	A valid not blacklisted PUI has been sent to the AE. The PUI is not blocked. The tester knows the expected AC.
Reference:	Subclause 5.2.1 Weak authentication..

5.3.3 SAPIN verification test purposes

ASVCA1:	Check that SAPIN verification is supported. Covered by ASVBV1 and ASVBI1.
Initial conditions:	The AE supports strong authentication.
Reference:	Subclause 5.4 Special authentication for called specified secure answering of incoming calls.

ASVBV1:	Check that a received correct SAPIN results in that the incoming call is allowed.
Initial conditions:	The user has two-pass strong authentication and has subscribed to called specified secure answer.
Reference:	Subclause 5.4 Special authentication for called specified secure answering of incoming calls.

ASVBI1:	Check that a received incorrect SAPIN results in that the incoming call is not allowed.
Initial conditions:	The user has two-pass strong authentication and has subscribed to called specified secure answer.
Reference:	Subclause 5.4 Special authentication for called specified secure answering of incoming calls.

5.3.4 OCPIN verification test purposes

AOVCA1:	Check that OCPIN verification is supported. Covered by AOVBV1 and AOVBI1.
Initial conditions:	The telephone is registered for outgoing calls.
Reference:	Subclause 5.3 Extra authentication for outgoing calls.

AOVBV1:	Check that a received correct OCPIN results in that the outgoing call can be established.
Initial conditions:	The telephone is registered for outgoing calls.
Reference:	Subclause 5.3 Extra authentication outgoing calls.

AOVBI1:	Check that a received incorrect OCPIN results in that the outgoing call is not allowed.
Initial conditions:	The user has subscribed to the OCPIN procedure.
Reference:	Subclause 5.3 Extra authentication outgoing calls.

5.3.5 PIN change test purpose

APCBI1:	Check that the PIN cannot get the same value as the OCPIN or SAPIN.
Initial conditions:	A change of PIN is performed.
Reference:	Subclause 9.4 PIN change check.

6 Test methods and configurations

This clause describes the methods and configurations to test the UPT card reading terminal, the AE and the UPT card. The Implementation Under Test (IUT), the upper tester, the lower tester, and the Points of Control and Observation (PCO) are described in detail.

All protocols that are described in this ETS are application protocols. Therefore, only the application layer is considered.

6.1 Card reading terminal

The PCOs are the keyboard and optionally the display of the terminal (interface to the upper tester) and the signalling from the terminal to the computer (interface to the lower tester). This is shown in figure 2.

The terminal will be tested with a reference UPT card which will react as a UPT card following the UPT card specifications.

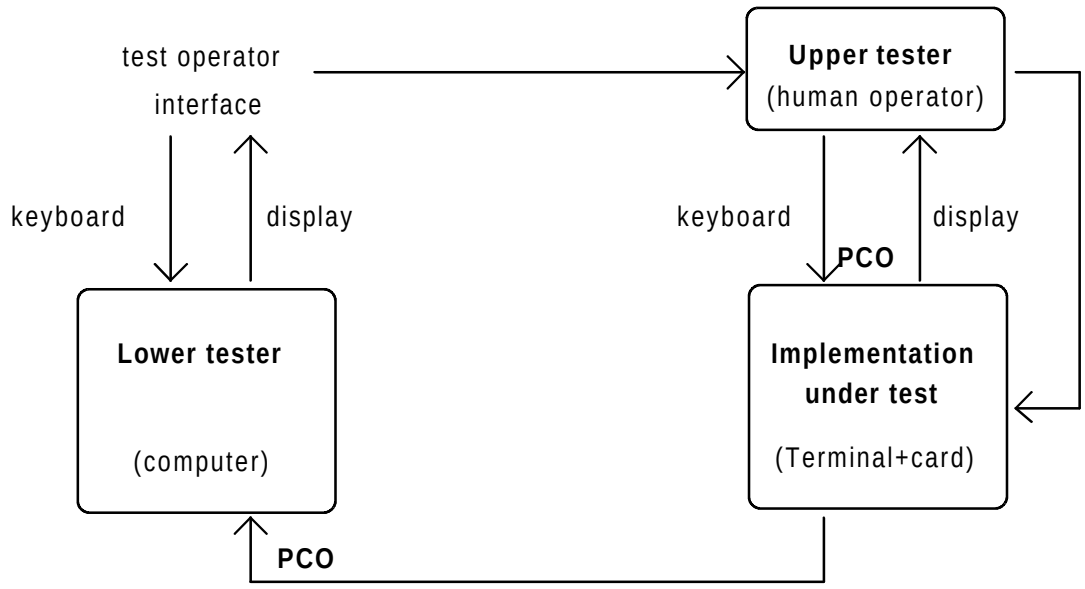

Figure 2: Card reading terminal

The values for CHV are entered via the keyboard of the terminal. The challenge value for authentication is sent to the reference card by the computer.

The output from the terminal is received and analysed.

If a CHV procedure (e.g. unblocking or change) is performed, the result (successful or not successful) may be indicated in a display of the terminal. In any case, the result can be tested by succeeding authentication attempts.

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

6.2 UPT card

In order to test the UPT card, the tester will use a reference terminal.

The PCOs are the keyboard and the display of the reference terminal (interface to the upper tester). This is shown in figure 3.

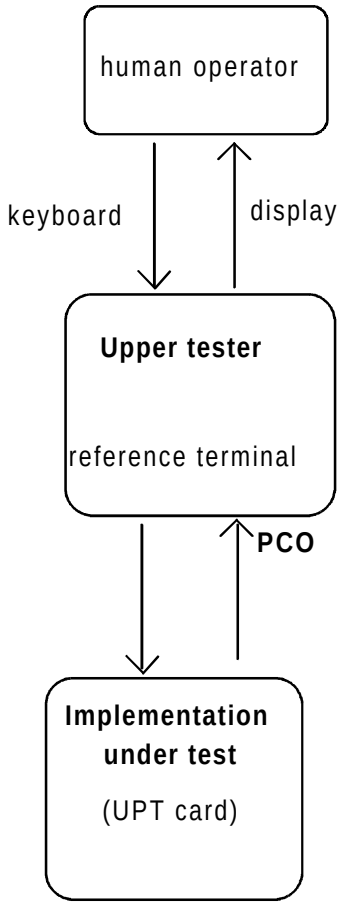

Figure 3: UPT Card

The values for PUI and key can not be entered directly into the UPT card. The card manufacturer shall implement these values according to the requirements of the test laboratory. The interface for this procedure is not standardized.

The values for CHV are entered via the keyboard of the reference terminal. The challenge value for authentication is sent to the card via the terminal.

The output from the card is presented to the display and analysed.

If a CHV procedure (e.g. unblocking or change) is performed, the result (successful or not successful) may be indicated in the display of the terminal. In any case, the result can be tested by succeeding authentication attempts.

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

6.3 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 UPT card (if applicable).

The PCO at the lower tester is the keyboard of the terminal simulator and the display of the terminal simulator. The PCO at the upper tester might be a standardized software interface or a human operator interface. The testing architecture is shown in figure 4.

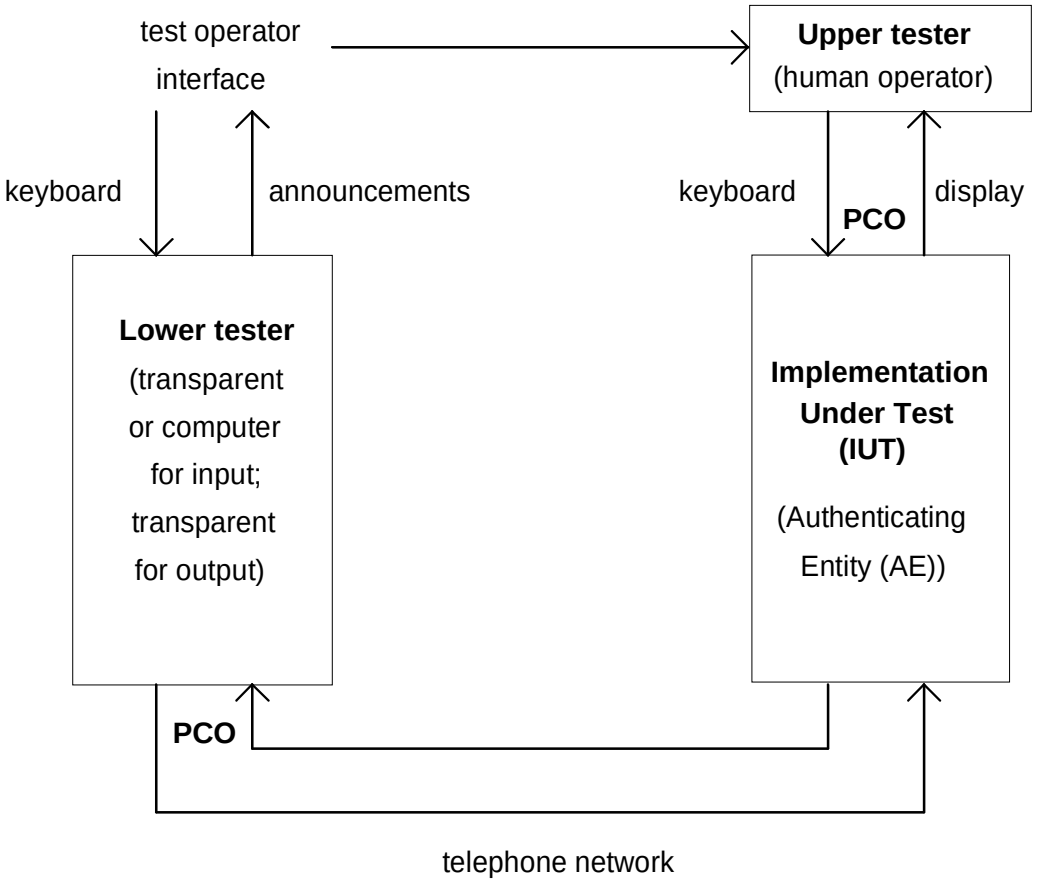

Figure 4: Authenticating Entity

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.

The values for PUI key 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 request for authentication is entered via the keyboard after CHV.

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

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 UPT card reading terminal

The following test cases of the UPT card reading terminal are specified:

- CHV;
- two-pass strong authentication;
- timer.

7.1.1 CHV

T C 1:	Fulfils the test purpose THVCA1.
Test steps:	1) Insert the UPT reference card in the terminal. 2) Perform a correct CHV. 3) Read the response on the terminal display.
Expected result after step 3:	Successful CHV.

T C 2:	Fulfils the test purpose THVBV1.
Test steps:	1) Insert the UPT reference card in the terminal. 2) Perform a correct CHV. 3) Perform a change CHV procedure with a value different from the old one. 4) Remove the UPT reference card. 5) Reinsert the UPT reference card. 5) Perform CHV with the old value. 6) Perform CHV with the new value.
Expected result after step 6:	Unsuccessful CHV.
Expected result after step 7:	Successful CHV.

T C 3:	Fulfils the test purpose THVBV2.
Test steps:	1) Insert the UPT reference card in the terminal. 2) Perform a correct unblocking CHV. 3) Remove the UPT reference card. 4) Perform CHV with an incorrect value. 5) Perform CHV with a correct value.
Expected result after step 4:	Unsuccessful CHV.
Expected result after step 5:	Successful CHV.

7.1.2 Two-pass strong authentication

T C 4:	Fulfils the test purposes TTIBV1, TTIBV2 and TSACA1.
Test steps:	1) Insert the UPT reference card in the terminal. 2) Perform a successful CHV. 3) Initiate the two-pass strong authentication procedure. 4) Record the output data. 5) Before T - 1 second, send a challenge to the UPT card. 6) Record the output data. 7) After T + 1 second, send a challenge to the UPT card. 8) Record the output data.
Expected result after step 4:	PUI and CT shall be sent, all values shall be correct.
Expected result after step 6:	PUI, CT and AC shall be sent, all values shall be correct.
Expected result after step 8:	No authentication data shall be sent by the terminal.

7.1.3 Timer

In subclause 7.1.2, TC 4 fulfils the test purposes TTIBV1 and TTIBV2.

T C 5:	Fulfils the test purposes TTIBI1 and TTIBV3.
Test steps:	1) Change T value to a value greater than T_{MAX}. 2) Perform a successful CHV. 3) Record the output data. 4) After the old T value - 1 second, send a challenge to the terminal. 5) Record the output data. 6) After the old T value + 1 second, send a challenge to the terminal. 7) Record the output data. 8) Change T value to a value greater than T_{MAX}. 9) Perform a successful CHV. 10) Record the output data. 11) After the old T value - 1 second, send a challenge to the terminal. 12) Record the output data. 13) After the old T value + 1 second, send a challenge to the terminal. 14) Record the output data.
Expected result after step 1:	Change of T refused.
Expected result after step 5:	PUI, CT and AC shall be sent, all values shall be correct.
Expected result after step 7:	No authentication data shall be sent by the terminal.
Expected result after step 8:	Change of T refused.
Expected result after step 12:	PUI, CT and AC shall be sent, all values shall be correct.
Expected result after step 14:	No authentication data shall be sent by the terminal.

7.2 UPT card

The following test cases of the UPT card are specified:

- CHV;
- two-strong authentication;
- timer.

7.2.1 CHV

T C 6:	Fulfils the test purposes CHVBV1 and CHVBI1.
Test steps:	1) Insert the card in the reference terminal. 2) Perform an incorrect CHV. 3) Record the response from the card. 4) Perform an internal authentication in the card using RAND as input parameter. 5) Record the response from the card. 6) Perform a correct CHV. 7) Record the response from the card. 8) Perform an internal authentication in the card using RAND as input parameter. 9) Record the response from the card.
Expected result after step 3:	Unsuccessful CHV.
Expected result after step 5:	Error message.
Expected result after step 7:	Successful CHV.
Expected result after step 9:	AC shall be received.

In subclause 7.2.2, TC 8 fulfils the test purpose CHVCA3.

T C 7:	Fulfils the test purpose CHVBI2.
Test steps:	1) Insert the card in the reference terminal. 2) Perform an incorrect CHV. 3) Record the response from the card. 4) Perform an incorrect CHV. 5) Record the response from the card. 6) Perform a correct CHV. 7) Record the response from the card. 8) Perform an incorrect CHV. 9) Record the response from the card. 10) Perform an incorrect CHV. 11) Record the response from the card. 12) Perform an incorrect CHV. 13) Record the response from the card. 13) Remove and reinsert the card. 15) Perform a correct CHV. 16) Record the response from the card.
Expected result after step 3:	Unsuccessful CHV.
Expected result after step 5:	Unsuccessful CHV.
Expected result after step 7:	Successful CHV.
Expected result after step 9:	Unsuccessful CHV.
Expected result after step 11:	Unsuccessful CHV.
Expected result after step 13:	Card blocked.
Expected result after step 16:	Card blocked.

7.2.2 Two-pass strong authentication

T C 8:	Fulfils the test purposes CSABV1 and CSABV2 and CHVCA3.
Test steps:	1) Read out PUI from the card and record it. 2) Read out CT from the card and record it. 3) Perform an internal authentication in the card using RAND as input parameter. 4) Record the response from the card. 5) Reset the card. 6) Perform an internal authentication in the card using RAND as input parameter. 7) Record the response from the card.
Expected result after step 1:	The stated value of PUI is received.
Expected result after step 2:	The stated value of CT is received.
Expected result after step 4:	Correct value of AC is received.
Expected result after step 7:	Error message is received.

7.2.3 Timer

T C 9:	Fulfils the test purpose CTICA1.
Test steps:	1) Read out T from the card and record it.
Expected result:	T shall be equal to the stated value.

T C 10:	Fulfils the test purpose CTICA2.
Test steps:	1) Read out T_{MAX} from the card and record it.
Expected result:	T_{MAX} shall be equal to the stated value.

T C 11:	Fulfils the test purposes CTIBI1 and CTIBI2.
Test steps:	1) Insert the card in the reference terminal. 2) Try to change the value of T. 3) Try to change the value of T_{MAX}. 4) Perform a successful CHV. 5) Try to change the value of T.
Expected result after step 2:	Error message.
Expected result after step 3:	Error message.
Expected result after step 5:	Change accepted.

7.3 AE

In this subclause, the data shall be sent to the AE according to the correct syntax specified in ETS 300 391-1 [3].

The following major functions shall be tested:

- the PUI check;
- two-pass strong authentication;
- SAPIN check;
- OCPIN check;
- PIN change check.

7.3.1 PUI check

T C 12:	Fulfils the test purpose APCCA1.
Test steps:	1) Send invalid PUI to the AE in a two-pass strong authentication attempt.
Expected result:	No challenge is sent back from the AE.

T C 13:	Fulfils the test purpose APCCA2.
Test steps:	1) Send a blacklisted PUI to the AE in a two-pass strong authentication attempt.
Expected result:	No challenge is sent back from the AE.

7.3.2 Two-pass strong authentication

T C 14:	Fulfils the test purpose ASABV2.
Test steps:	1) Send a valid and not blacklisted PUI and a valid CT to the AE. 2) Record the challenge sent back by the AE. 3) Send the response calculated using the right key and the challenge. 4) Record the output.
Expected result after step 4:	Successful authentication.

T C 15:	Fulfils the test purpose ASABI1.
Test steps:	1) Send a valid and not blacklisted PUI and a valid CT to the AE. 2) Record the challenge sent back by the AE. 3) Send the response calculated using the wrong key, and the correct PUI. 4) Record the output.
Expected result after step 4:	Authentication failure.

T C 16:	Fulfils the test purpose ASABV1.
Test steps:	1) Send valid and not blacklisted PUIs and a valid CT to the AE. 2) Record the challenges sent back by the AE.
Expected result after step 2:	The analysis of these challenges does not give any information for the next ones.

7.3.3 SAPIN check

T C 17:	Fulfils the test purpose ASVBV1.
Test steps:	1) Send a correct value of SAPIN.
Expected result:	The AE allows the completion of the call.

T C 18:	Fulfils the test purpose ASVBI1.
Test steps:	1) Send an incorrect value of SAPIN.
Expected result:	The AE does not allow the completion of the call.

7.3.4 OCPIN check

T C 19:	Fulfils the test purpose AOVBV1.
Test steps:	1) Send a correct value of OCPIN.
Expected result:	The AE allows the user to proceed.

T C 20:	Fulfils the test purpose AOVBI1.
Test steps:	1) Send an incorrect value of OCPIN.
Expected result:	The AE does not allow the user to proceed.

7.3.5 Change PIN check

T C 21:	Fulfils the test purpose APCBI2.
Test steps:	1) Perform a successful weak authentication. 2) Perform the change PIN procedure with the OCPIN value. 3) Disconnect. 4) Perform the weak authentication procedure with OCPIN value. 5) Perform the weak authentication with the same values as in step 1. 6) Perform a successful weak authentication. 7) Perform the change PIN procedure with the SAPIN value. 8) Disconnect. 9) Perform the weak authentication procedure with SAPIN. 10) Perform the weak authentication with the same values as in step 1.
Expected result after step 2:	Change PIN refused.
Expected result after step 4:	Authentication failure.
Expected result after step 5:	Successful authentication.
Expected result after step 7:	Change PIN refused.
Expected result after step 9:	Authentication failure.
Expected result after step 10:	Successful authentication.

History

Document history			
August 1996	Public Enquiry	PE 112:	1996-08-19 to 1996-12-13
July 1997	Vote	V 9739:	1997-07-29 to 1997-09-26
October 1997	First Edition		

ISBN 2-7437-1764-5
Dépôt légal : Octobre 1997