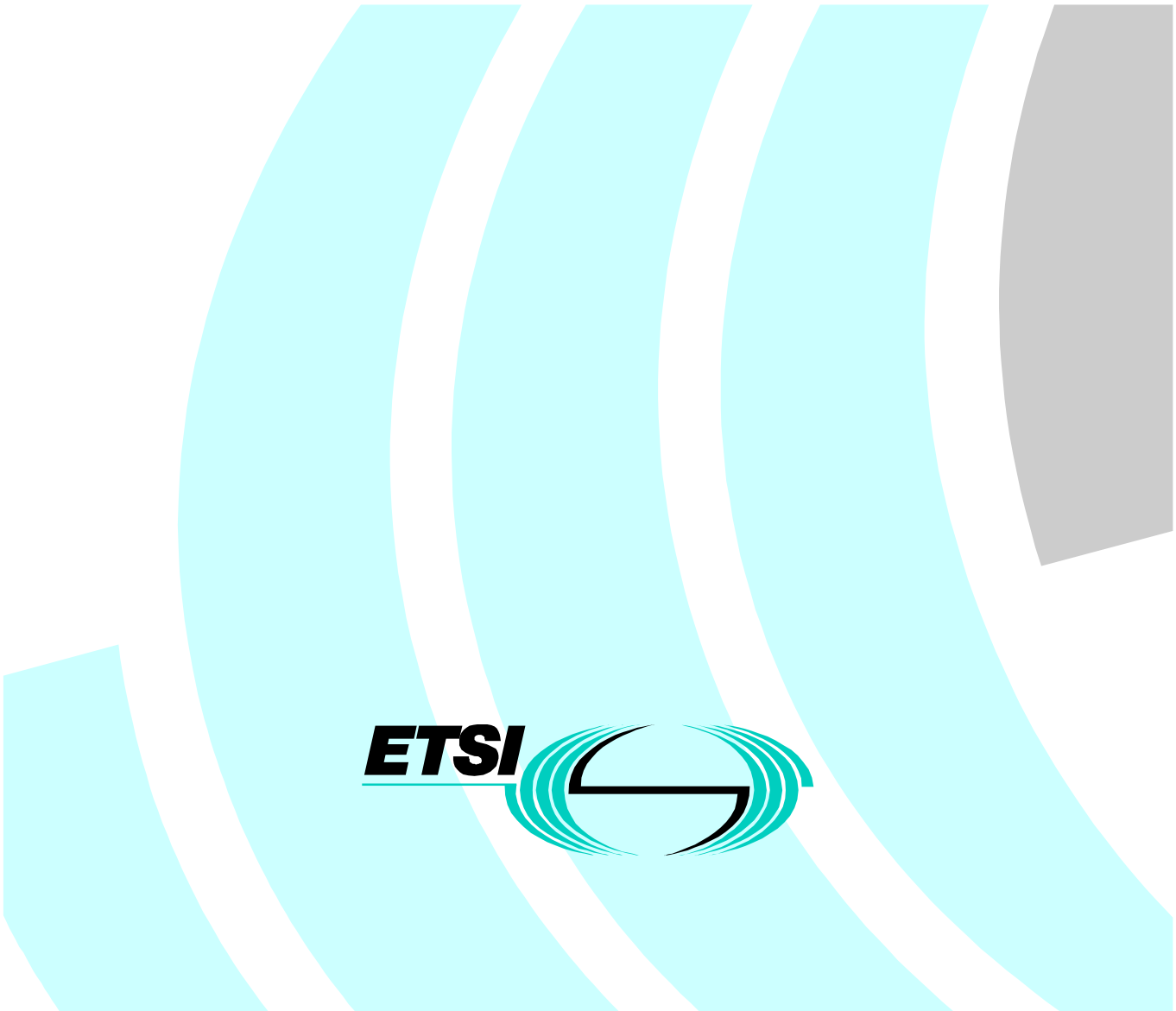
Draft EN 301 363 V1.1.1 (1998-08)

European Standard (Telecommunications series)

Universal Personal Telecommunication (UPT); UPT phase 2; Functional specification of the interface of a UPT Integrated Circuit Card (ICC) and Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN) and Global System for Mobile communications (GSM) terminals (one pass and multiple pass authentication); Conformance test specification



Reference
DEN/NA-064011 (cmc00ico.PDF)

Keywords
CARD, GSM, ISDN, UPT

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet
secretariat@etsi.fr
http://www.etsi.fr
http://www.etsi.org

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.fr/ipr or http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (Telecommunications series) has been produced by the ETSI Technical Committee Network Aspects (NA) and is now submitted for the Public Enquiry phase of the ETSI standards Two-step Approval Procedure.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

1 Scope

The present document provides the test specification for the Universal Personal Telecommunication (UPT) card and the Card Accepting Device (CAD) defined in ETS 300 823 [1].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ETS 300 823 (1997): "Universal Personal Telecommunication (UPT); UPT phase 2; Functional specification of the interface of a UPT Integrated Circuit Card (ICC) and Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN) and Global System for Mobile Communications (GSM) terminals (one pass and multiple pass authentication)".

[2] EN 301 366: "Universal Personal Telecommunication (UPT); UPT phase 2; Functional specification of the interface of a UPT Integrated Circuit Card (ICC) and Card Accepting Devices (CAD); UPT card accepting Dual Tone Multiple Frequency (DTMF) device; Conformance test specification".

[3] ISO 8859-1 (1998): "Information technology; 8-bit single-byte coded graphic character sets; Part 1: Latin alphabet No. 1".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following definitions in addition to the terms defined in ETS 300 823 [1] apply:

Implementation Conformance Statement (ICS): A statement made by the supplier of an implementation or system claimed to conform to a given specification, stating which capabilities have been implemented. The ICS can take several forms: protocol ICS, profile ICS, profile specific ICS, information object ICS, etc.

ICS proforma: A document, in the form of a questionnaire, which when completed for an implementation or system becomes an ICS.

3.2 Symbols

For the purposes of the present document, the symbols of EN 301 366 [2] apply.

3.3 Abbreviations

For the purposes of the present document the following abbreviation in addition to the abbreviations of EN 301 366 [2] apply:

RAND Random challenge sent by the network to be used for authentication.

4 UPT Integrated Circuit Card part

4.1 Test environment

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "PIM" is replaced by "PIM2";
- in subclause 4.4 "DF_{UPT}" is replaced by "DF_{UPT2}".

4.2 Test group hierarchy

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2".

4.3 Test procedure

For this clause, the same text as in EN 301 366 [2] is valid.

4.3.1 Physical characteristics

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2".

4.3.2 Electronic signals and transmission protocols

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2".

4.3.3 Logical model

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2";
- in subclauses 4.3.3.2 and 4.3.3.4 "DF_{UPT}" is replaced by "DF_{UPT2}";
- in subclause 4.3.3.4.2 "EF_{SEQ}" is deleted.

4.3.4 Security services and facilities

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2";
- "DF_{UPT}" is replaced by "DF_{UPT2}";
- the subclauses 4.3.4.1.4 and 4.3.4.1.5 are replaced by the following ones:

4.3.4.1.4 Method of test

Initial conditions:

1) the PIM is connected to a CAD simulator;
2) CHV1 on the PIM is set to '0000';
3) three VERIFY CHV1 attempts and ten UNBLOCK CHV1 attempts remain.

Test procedure:

a) the CAD simulator resets the PIM;
b) the CAD simulator selects DF_{UPT} as defined in subclause 4.4;
c) the CAD simulator sends a VERIFY CHV command with **incorrect** CHV1 '1111' to the PIM;
d) the CAD simulator sends VERIFY CHV command with **incorrect** CHV1 '1111' to the PIM;
e) the CAD simulator sends VERIFY CHV command with **incorrect** CHV1 '1111' to the PIM;
f) the CAD simulator sends a SELECT command to the PIM to select EF_{CT};
g) the CAD simulator sends a READ BINARY;
h) the CAD simulator sends a SELECT command to the PIM to select EF_{PUI};
i) the CAD simulator sends a READ BINARY;
j) the CAD simulator sends a INTERNAL AUTHENTICATION command to the PIM containing the number '12345678';
k) the CAD simulator sends a VERIFY CHV command with correct CHV1 '0000' to the PIM;
l) the CAD simulator sends a SELECT command to the PIM to select EF_{CHV1};
m) the CAD simulator sends an UNBLOCK CHV command to the PIM;
n) the CAD simulator sends a VERIFY CHV command with correct CHV1 '0000' to the PIM.

4.3.4.1.5 Test requirement

1) After step e) the status condition returned by the PIM shall be SW1='98', SW2='40' - unsuccessful CHV verification, verify CHV mechanism no longer possible.
2) After steps g), i) and j) the status condition returned by the PIM shall be SW1='98', SW2='04' - access condition not fulfilled.
3) After step k) the status condition returned by the PIM shall be SW1='98', SW2='40' - CHV blocked.

4.3.5 Description of the functions

For this clause, the same text as in EN 301 366 [2] is valid.

4.3.5.1 SELECT function

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2";
- "DF_{UPT}" is replaced by "DF_{UPT2}";
- in subclause 6.5.10.4, m) "EF_{SEQ}" is deleted.

4.3.5.2 READ BINARY function

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2";
- "DF_{UPT}" is replaced by "DF_{UPT2}".

4.3.5.3 UPDATE BINARY function

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2";
- "DF_{UPT}" is replaced by "DF_{UPT2}";
- the subclauses 4.3.5.3.4 and 4.3.5.3.5 are replaced by the following ones:

4.3.5.3.4 Method of test

Initial conditions:

1) the PIM is connected to a CAD simulator;
2) EF_{TV} contains the data string: '11 22';
3) CHV1 is enabled.

Test procedure:

a) the CAD simulator resets the PIM;

b) the CAD simulator sends SELECT commands to the PIM to select EF_{TV} under DF_{UPT};

c) the CAD simulator sends an UPDATE BINARY command using a length of 1 byte, and data string '33' to the PIM;

d) the CAD simulator sends a READ BINARY command to the PIM using a length of 1 byte and an offset of '00 00';

e) the CAD simulator sends a VERIFY CHV command to the PIM;

f) the CAD simulator sends an UPDATE BINARY command using a length of 1 byte, and data string '33' to the PIM;

g) the CAD simulator sends a READ BINARY command using a length of 1 byte to the PIM;

h) the CAD simulator sends an UPDATE BINARY command using a length of 1 byte, and data string '00' to the PIM;

i) the CAD simulator sends a READ BINARY command using a length of 2 bytes to the PIM;

j) the CAD simulator sends an UPDATE BINARY command using an offset of '00 01', a length 1 byte, and data string '44' to the PIM;

k) the CAD simulator sends a READ BINARY command using a length of 2 bytes to the PIM.

4.3.5.3.5 Test requirement

1) After step c) the status condition returned by the PIM shall be SW1='98', SW2='04' - access condition not fulfilled;

2) after step d) the status condition returned by the PIM shall be SW1='98', SW2='04' - access condition not fulfilled;

3) after step g) the data string returned shall be '33';

4) after step i) the data string returned shall be '00 22';

5) after step k) the data string returned shall be '44 00'.

4.3.5.4 READ RECORD function

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2".

4.3.5.5 UPDATE RECORD function

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2".

4.3.5.6 SEEK function

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2".

4.3.5.7 VERIFY CHV function

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2";
- "DF_{UPT}" is replaced by "DF_{UPT2}".

4.3.5.8 CHANGE CHV function

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2".

4.3.5.9 UNBLOCK CHV function

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2";
- "DF_{UPT}" is replaced by "DF_{UPT2}".

4.3.5.10 INTERNAL AUTHENTICATION function

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2";
- "DF_{UPT}" is replaced by "DF_{UPT2}";
- in 2) of subclause 4.3.5.10.2 "(n)" is deleted;
- the subclauses 4.35.10.4 and 4.35.10.5 are replaced by the following ones:

4.3.5.10.4 Method of test

Initial conditions:

1) the PIM is connected to a CAD simulator.

Test procedure:

a) the CAD simulator resets the PIM;

b) the CAD simulator selects DF_{UPT} as defined in subclause 4.4;

c) the CAD simulator gains CHV1 security access;

d) the CAD simulator sends a SELECT command to the PIM to select EF_{CT};

e) the CAD simulator sends a READ BINARY;

f) the CAD simulator sends a SELECT command to the PIM to select EF_{PUI};

g) the CAD simulator sends a READ BINARY;

h) the CAD simulator sends a INTERNAL AUTHENTICATION command to the PIM containing the number '12345678';

i) the CAD simulator sends a GET RESPONSE command to the PIM;

j) the CAD simulator resets the PIM;

k) the CAD simulator selects DF_{UPT} as defined in subclause 4.4;

l) the CAD simulator sends a SELECT command to the PIM to select EF_{CT};

m) the CAD simulator sends a READ BINARY;

n) the CAD simulator sends a SELECT command to the PIM to select EF_{PUI};

o) the CAD simulator sends a READ BINARY;

p) the CAD simulator sends a INTERNAL AUTHENTICATION command to the PIM containing the number '12345678';

q) the CAD simulator sends a GET RESPONSE command to the PIM.

4.3.5.10.5 Test requirement

1) After step h) the PIM shall have sent a AC.

2) After step q) the status condition returned by the PIM shall be SW1='98', SW2='04' - access condition not fulfilled, authentication failed.

4.3.6 Description of the commands

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2";
- "DF_{UPT}" is replaced by "DF_{UPT2}";
- the subclause 4.3.6.3.1 is replaced by the following one:

4.3.6.3.1 SELECT command

4.3.6.3.1.1 Definition and applicability

It shall be mandatory for all cards complying with ETS 300 823 [1] to support all functions described therein.

This test applies to both plug-in and ID-1 PIM2 cards.

4.3.6.3.1.2 Conformance requirement

The SELECT command shall provide the response data described in ETS 300 823 [1], subclause 9.3.1.

Reference: ETS 300 823 [1], subclause 9.3.1.

Test Group Reference (TGR): TGR_PIM2_CMD

Test Procedure Reference (TPR): TPR_PIM2_CMD_SEL

4.3.6.3.1.3 Test purpose

To verify that the coding of the SELECT command conforms to the above requirements.

4.3.6.3.1.4 Method of test

Initial conditions:

1) the PIM2 is connected to a CAD simulator.

Test procedure:

a) the CAD simulator resets the PIM2;

b) the CAD simulator sends a SELECT command to the PIM2 to select MF:

- [bytes sent: CLA='A0', INS='A4', P1='00', P2='00', Lc='02', data='3F 00'];
- [bytes received: SW1, $SW2_1$];

c) the CAD simulator sends a GET RESPONSE command to the PIM2:

- [bytes sent: CLA='A0', INS='C0', P1='00', P2='00', Le=$SW2_1$];
- [bytes received: data, SW1, SW2];

d) the CAD simulator selects DF_{UPT2} as defined in subclause 4.4;

e) the CAD simulator sends SELECT commands to the PIM2 to select DF_{SR1}:

- [example bytes sent: CLA='A0', INS='A4', P1='00', P2='00', P3='02', data='7F 70'];
- [bytes received: SW1, $SW2_2$];

f) the CAD simulator sends a GET RESPONSE command to the PIM2:

- [bytes sent: CLA='A0', INS='C0', P1='00', P2='00', Le =$SW2_2$];
- [bytes received: data, SW1, SW2];

g) the CAD simulator sends a SELECT command to the PIM2 to select EF_{PUI}:

- [bytes sent: CLA='A0', INS='A4', P1='00', P2='00', Lc='02', data='6F 07'];
- [bytes received: SW1, $SW2_3$];

h) the CAD simulator sends a GET RESPONSE command to the PIM2:

- [bytes sent: CLA='A0', INS='C0', P1='00', P2='00', Le =$SW2_3$];
- [bytes received: data, SW1, SW2];

i) if EF_{ADN} is present, the CAD simulator sends a SELECT command to the PIM to select EF_{ADN}:

- [bytes sent: CLA='A0', INS='A4', P1='00', P2='00', Lc='02', data='6F 3A'];
- [bytes received: SW1, $SW2_4$];

j) if EF_{ADN} is present, the CAD simulator sends a GET RESPONSE command to the PIM:

- [bytes sent: CLA='A0', INS='C0', P1='00', P2='00', Le =$SW2_4$];
- [bytes received: data, SW1, SW2];

k) the CAD simulator selects the relevant EF_{CHV1} as defined in subclause 4.4;

l) the CAD simulator sends a SELECT command to the PIM2 to re-select EF_{CHV1}:

- [bytes sent: CLA='A0', INS='A4', P1='00', P2='00', Lc='02', data='00 00'];
- [bytes received: SW1, $SW2_5$];

m) the CAD simulator sends a GET RESPONSE command to the PIM2:

- [bytes sent: CLA='A0', INS='C0', P1='00', P2='00', Le =$SW2_5$];
- [bytes received: data, SW1, SW2].

4.3.6.3.1.5 Test requirement

1) After step c) the following shall be true of the response data:

   - bytes 3 and 4 shall contain information about the total memory amount under the MF that is not allocated by any of the DFs or EFs under the MF;
   - bytes 5 and 6 shall contain the file ID for the MF, '3F 00';
   - byte 7 shall contain '01' for MF;
   - byte 8 shall give the access conditions for the MF;
   - byte 12 shall contain the binary code 0000000X, where X gives the invalidation status, which must be 1 otherwise the card has become mute;
   - byte 13 shall give the number of bytes that follow in the response information;
   - byte 14 shall give the current directory characteristics as specified in ETS 300 823 [1];
   - byte 15 shall indicate the correct number of DFs which are a direct child of the MF;
   - byte 16 shall indicate the correct number of EFs which are a direct child of the MF;
   - bytes 19 - 22 shall give information about the CHVs under the MF. For details see ETS 300 823 [1].

2) After step f) the following shall be true of the response data:

   - bytes 3 and 4 shall contain information about the total memory amount under DF_{UPT2} that is not allocated by any of the DFs or EFs under DF_{UPT2};
   - bytes 5 and 6 shall contain the file ID for DF_{UPT2};
   - byte 7 shall contain '02' for DF;
   - byte 8 shall give the access conditions for DF_{UPT2};
   - byte 12 shall contain the binary code 0000000X, where X gives the invalidation status, which must be 1 otherwise the card has become mute;
   - byte 13 shall give the number of bytes that follow in the response information;
   - byte 15 shall indicate the correct number of DFs which are a direct child of DF_{UPT2};
   - byte 16 shall indicate the correct number of EFs which are a direct child of DF_{UPT2};
   - bytes 19 - 22 shall give information about the CHVs under DF_{UPT2}. For details see ETS 300 823 [1].

3) After step h) the following shall be true of the response data:

   - bytes 3 and 4 shall contain information about the file size for EF_{PUI}. The size must be 9;
   - bytes 5 and 6 shall contain the file ID for EF_{PUI} '6F 07';
   - byte 7 shall contain '04' for EF;
   - byte 9 shall give the access conditions for EF_{PUI} described in ETS 300 823 [1], subclause 10.3.2;
   - byte 12: bit 1 shall be 1;
   - byte 13 shall give the number of bytes that follow in the response information;
   - byte 14 gives the structure of the EF and in this case it shall contain '00' indicating transparent structure;
   - byte 15, if present, shall be '00'.

4) If the command GET RESPONSE in step j) is sent, the following shall be true of the response data after step j):

   - bytes 3 and 4 shall contain information about the file size for EF_{ADN};
   - bytes 5 and 6 shall contain the file ID for EF_{ADN}, '6F 3A';
   - byte 7 shall contain '04' for EF;
   - byte 9 shall give the access conditions for EF_{ADN}. Byte 9 shall have the value '11';
   - byte 12: bit 1 shall be 1;
   - byte 13 shall give the number of bytes that follow in the response information;
   - byte 14 gives the structure of the EF and in this case it shall be '01' indicating linear fixed structure;
   - byte 15 shall be 'X+14'.

5) After step m) the following shall be true of the response data:

   - bytes 3 and 4 shall be '00 17';
   - bytes 5 and 6 shall contain the file ID for EF_{CHV1}, '00 00';
   - byte 7 shall contain '04' for EF;
   - byte 9 shall give the access conditions for EF_{CHV1}. Byte 9 shall have the value 'FF';
   - byte 12: bit 1 shall be 1, bit 2 shall be 1 and bit 3 shall be 0;
   - byte 13 shall give the number of bytes that follow and shall be coded '07';
   - byte 14 gives the structure of the EF and in this case it shall be '00' indicating transparent structure;
   - byte 15 shall indicate the number of remaining CHV attempts and shall be in the range '00' to '03';
   - byte 16 shall be '01' indicating CHV verification;
   - byte 17 bits 1, 2 and 3 shall be 0;
   - bytes 18 and 20 shall be 'FF';
   - byte 19 shall indicate the number of remaining UNBLOCK CHV attempts and shall be in the range '00' to '0A'.

4.3.7 Contents of the EFs

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2";
- "DF_{UPT}" is replaced by "DF_{UPT2}";
- the subclause 4.3.7.3 is replaced by the following one:

4.3.7.3 Contents of the EFs at the UPT application level

4.3.7.3.1 Definition and applicability

The following Elementary Files are required on the UPT card at the UPT application level in order for a UPT session to be carried out. For each of these EFs, the correct access conditions, data items and coding need to be in place.

- EF_{CT} - CT value;
- EF_{PUI} - PUI;
- EF_{PST} (optional) - allocated and activated/disactivated services;
- EF_{TV} - time-out value;
- EF_{MTV} (optional) - maximum time-out value.

This test applies to both plug-in and ID-1 UPT cards.

4.3.7.3.2 Conformance requirement

1) The ASCII coding of the data items shall be in accordance with ISO 8859-1 [3].
2) EFs, records or data items having an unassigned value shall have their bytes and bits set to 'FF' and 1, respectively.
3) After the administrative phase, all data items shall have a defined value or have their bits set to 1.
4) All implemented EFs file a have size greater than zero shall contain all mandatory items.
5) Optional data items shall be filled with 'F', or if located at the end of the EF need not exist.
6) EF_{CT} shall contain the following data item for byte 1:
   - CT.
7) EF_{PUI} shall contain the following data items for bytes 1 to 9:
   - Length of PUI
   - PUI.
8) EF_{PST} (optional) shall contain the following data items for bytes 1 to 4:
   - services number 1 to number 14.
9) EF_{TV} shall contain the following data items for bytes 1 to 2:
   - Number of minutes.
10) EF_{MTV} (optional) shall contain the following data items for bytes 1 to 2:
   - Number of minutes.

Reference: ETS 300 823 [1], subclause 10.3.

Test Group Reference (TGR): TGR_PIM2_CEF_UPT.

Test Procedure Reference (TPR): TPR_PIM2_CEF_UPT.

4.3.7.3.3 Test purpose

To verify that the PIM2 conforms to the above requirements.

4.3.7.3.4 Method of test

Initial conditions:

1) the PIM2 is connected to a CAD simulator.

Test procedure:

a) the CAD simulator resets the PIM2;

b) the CAD simulator selects DF_{UPT2} as defined in subclause 4.4;

c) the CAD simulator sends a SELECT command to the PIM2 to select EF_{CT};

d) the CAD simulator sends a GET RESPONSE command to the PIM2;

e) the CAD simulator sends READ BINARY commands to the PIM2 to read all available data bytes;

f) the CAD simulator sends a SELECT command to the PIM2 to select EF_{PUI};

g) the CAD simulator sends a GET RESPONSE command to the PIM2;

h) the CAD simulator sends a READ BINARY command to the PIM2 to read all available data bytes;

i) the CAD simulator sends a SELECT command to the PIM2 to select EF_{PST};

j) the CAD simulator sends a GET RESPONSE command to the PIM2;

k) the CAD simulator sends a READ BINARY command to the PIM2 to read all available data bytes;

l) the CAD simulator sends a SELECT command to the PIM2 to select EF_{TV};

m) the CAD simulator sends a GET RESPONSE command to the PIM2;

n) the CAD simulator sends a READ BINARY command to the PIM2 to read all available data bytes;

o) the CAD simulator sends a SELECT command to the PIM2 to select EF_{MTV};

p) the CAD simulator sends a GET RESPONSE command to the PIM2;

q) the CAD simulator sends a READ BINARY command to the PIM2 to read all available data bytes.

4.3.7.3.5 Test requirement

After steps e), h), k), n) and q) the data read shall conform to the requirements above.

5 UPT Card Accepting Device part

5.1 Test environment

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "PIM" is replaced by "PIM2";
- the following subclause is added:

5.1.1.2 Network item

This item of equipment (a real network connection or a net simulator) must be able to send a random number RAND of 8 bytes after receiving an authentication request from the CAD during the two pass strong authentication by the CAD-Network interface.

5.2 Test group hierarchy

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "OPSA" is replaced by "TPSA".

5.3 Test procedure

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

"PIM" is replaced by "PIM2".

5.3.1 Physical characteristics

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2".

5.3.2 Electrical tests

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2".

5.3.3 Low level protocol tests

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2".

5.3.4 Application protocol

For this clause, the same text as in EN 301 366 [2] is valid with the following modifications:

- "ETS 300 477" is replaced by "ETS 300 823 [1]";
- "PIM" is replaced by "PIM2";
- "DF_{UPT}" is replaced by "DF_{UPT2}";
- the subclause 5.3.4.4.1 is replaced by the following one:

5.3.4.4.1 Two pass strong authentication

5.3.4.4.1.1 Definition and applicability

This procedure is used by the PIM2 to authenticate itself to the network.

5.3.4.4.1.2 Conformance requirement

1) The CAD shall send the commands in the sequence described in ETS 300 823 [1], subclause 11.4.1 and in the right format described in ETS 300 823 [1], clause 9.

Reference: ETS 300 823 [1], clause 9 and subclause 11.4.1.

Test Group Reference (TGR): TGR_CAD_APP_SEC_TPSA.

Test Procedure Reference (TPR): TPR_ CAD_APP_SEC_TPSA.

5.3.4.4.1.3 Test purpose

To verify that the CAD conform to the above requirements.

5.3.4.4.1.4 Method of test

Initial condition

1) the CAD is connected to a PIM2 simulator and powered on;
2) a successful PIM2 initialization procedure and a successful CHV1 procedure is completed;
3) the content of EF_{CT} is '01';
4) the content of EF_{PUI} is '01 12 FF FF FF FF FF FF FF';
5) the CAD is connected to a Network item, see subclause 5.1.1.2.

Test procedure

a) the procedure is initiated by the tester by the corresponding MMI interaction;
b) the PIM2 simulator sends the status bytes corresponding to the received command "select EF_{CT}";
c) the PIM2 simulator sends the data ('01') and the status bytes corresponding to the received command "read";
d) the PIM2 simulator sends the status bytes corresponding to the received command "select EF_{PUI}";
e) the PIM2 simulator sends the data ('01 12 FF FF FF FF FF FF FF') and the status bytes corresponding to the received command "read";
f) the Network item sends a random number RAND to the CAD;
g) if the CAD has sent the right command "internal authentication" (described below) the PIM2 simulator sends the status bytes '90 00' (if the received command was right);
h) if the CAD has sent the right command "get response" (described below) the PIM2 simulator sends the data '11 22 11 22 11 22 11 22' and the status bytes '90 00' (if the received command was right);

5.3.4.4.1.5 Test requirement

1) After step a) the CAD shall send the command SELECT to select EF_{CT};
2) After step b) the CAD shall send the command READ BINARY with P1='00', P2='00' and Le='01';
3) After step c) the CAD shall send the command SELECT to select EF_{PUI};
4) After step d) the CAD shall send the command READ BINARY with P1='00', P2='00' and Le='09';
5) If the CAD has sent an authentication request to the Network item, the CAD shall send the command INTERNAL AUTHENTICATION with P1='00', P2='00', Le='08' and data = RAND after step f);
6) After step g) the CAD shall send the command GET RESPONSE.

6 List of Test Procedure Reference

For this clause, the same text as in EN 301 366 [2] is valid .

History

Document history			
V1.1.1	July 1998	Public Enquiry	PE 9849: 1998-08-07 to 1998-12-04