TS 101 203-3 V1.1.1 (1997-07)

Technical Specification

Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-3; Part 3: Abstract Test Suite (ATS) and Implementation eXtra Information for Testing (IXIT) proforma specification

European Telecommunications Standards Institute

Reference

DTS/PTS-00203-3 (b50r0icr.PDF)

Keywords

Card, testing, ATS, TTCN, ATS_MP FILE,
ATS_GR FILE

ETSI Secretariat

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

X.400

c= fr; a=atlas; p=etsi; s=secretariat

Internet

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

Contents

Intellectual Property Rights

ETSI has not been informed of the existence of any Intellectual Property Right (IPR) which could be, or could become essential to the present document. However, pursuant to the ETSI Interim IPR Policy, no investigation, including IPR searches, has been carried out. No guarantee can be given as to the existence of any IPRs which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by the ETSI Project Pay Terminal and Systems (PTS). The present document was handed over to the CEN Secretariat in order to become an EN through the CEN approval process.
ETSI has produced a set of TSs which are not a copy of any CEN published EN. The TSs are complete and consistent documents with references among themselves. It has been made clear in these TSs that they are contributions to the CEN work for publication as EN (after re-editing the references). Once published by CEN as EN, ETSI will withdraw its TS.

The present document is part 3 of a multi-part document covering Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-3, as identified below:

Part 1: "Implementation Conformance Statement (ICS) proforma specification";

Part 2: "Test Suite Structure and Test Purposes (TSS&TP)";

Part 3: "Abstract Test Suite (ATS) and Implementation eXtra Information for Testing (IXIT)".

Overview of ETSI deliverables on EN 726 family

TS 101 200-1	"EN 726-1: Identification card systems; Telecommunications IC cards and terminals; Part 1: System overview".
TS 101 200-2	"EN 726-2: Identification card systems; Telecommunications IC cards and terminals; Part 2: Security framework".
TS 101 200-3	"EN 726-3: Identification card systems; Telecommunications IC cards and terminals; Part 3: Application independent card requirements".
TS 101 200-4	"EN 726-4: Identification card systems; Telecommunications IC cards and terminals; Part 4: Application independent card related terminal requirements".
TS 101 200-5	"EN 726-5: Identification card systems; Telecommunications IC cards and terminals; Part 5: Payment methods".
TS 101 200-6	"EN 726-6: Identification card systems; Telecommunications IC cards and terminals; Part 6: Telecommunications features".
TS 101 200-7	"EN 726-7: Identification card systems; Telecommunications IC cards and terminals; Part 7: Security module".

Overview of ETSI deliverables on EN 726 conformance testing family

TS 101 203-1	"Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-3; Part 1: Implementation Conformance Statement (ICS) proforma specification".
TS 101 203-2	"Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-3, Part 2: Test Suite Structure and Test Purposes (TSS&TP)".
TS 101 203-3	**"Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-3; Part 3: Abstract Test Suite (ATS) and Implementation eXtra Information for Testing (IXIT) proforma specification".**
TS 101 204-1	"Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-4; Part 1: Implementation Conformance Statement (ICS) proforma specification".
TS 101 204-2	"Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-4, Part 2: Test Suite Structure and Test Purposes (TSS&TP)".
TS 101 204-3	"Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-4; Part 3: Abstract Test Suite (ATS) and Implementation eXtra Information for Testing (IXIT) proforma specification".
TS 101 207-1	"Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-7; Part 1: Implementation Conformance Statement (ICS) proforma specification".
TS 101 207-2	"Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-7, Part 2: Test Suite Structure and Test Purposes (TSS&TP)".
TS 101 207-3	"Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-7; Part 3: Abstract Test Suite (ATS) and Implementation eXtra Information for Testing (IXIT) proforma specification".

1 Scope

The present document specifies the Abstract Test Suite (ATS) and Implementation eXtra Information for Testing (IXIT) proforma for *Application independent card requirements* defined in TS 101 200-3 [1].

ISO/IEC 9646, parts 1 to 5 [2 to 6] are used as the basis for the test methodology.

2 Normative references

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case 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] TS 101 200-3 version 1.2.1: "EN 726-3: Identification card systems; Telecommunications IC cards and terminals; Part 3: Application independent card requirements".

[2] ISO/IEC 9646-1 (1994): "Information technology - Open systems interconnection - Conformance testing methodology and framework - Part 1: General concepts".

[3] ISO/IEC 9646-2: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 2: Abstract Test Suite Specification".

[4] ISO/IEC 9646-3: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 3: The Tree and Tabular Combined Notation (TTCN)".

[5] ISO/IEC 9646-4: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 4: Test realization".

[6] ISO/IEC 9646-5: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 5: Requirements on test laboratories and clients for the conformance assessment process".

[7] TS 101 203-1: "Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-3; Part 1: Implementation Conformance Statement (ICS) proforma specification".

[8] TS 101 203-2: "Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-3, Part 2: Test Suite Structure and Test Purposes (TSS&TP)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following definitions apply:

Abstract Test Suite (ATS): See ISO/IEC 9646-1 [2].

ICS proforma: See ISO/IEC 9646-1 [2].

Implementation Conformance Statement (ICS): See ISO/IEC 9646-1 [2].

Implementation eXtra Information for Testing (IXIT): See ISO/IEC 9646-1 [2].

Implementation Under Test (IUT): See ISO/IEC 9646-1 [2].

IXIT proforma: See ISO/IEC 9646-1 [2].

System Under Test (SUT): See ISO/IEC 9646-1 [2].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AC	Access Condition(s)
ATC	Abstract Test Case
ATR	Answer To Reset
ATS	Abstract Test Suite
BCD	Binary Code Decimal
CAD	Card Accepting Device (this includes only the mechanics)
CHV	Card Holder Verification
CLA	CLAss
CS	Cyclic Structure
DF	Dedicated Files
EF	Elementary Files
GR	GRaphical form (TTCN)
IC	Integrated Circuit
ICS	Implementation Conformance Statement
ID	IDentifier
IFD	Interface Device, used as short form for a terminal including CAD
INS	INStruction
IUT	Implementation Under Test
IXIT	Implementation eXtra Information for Testing
LFS	Linear Fixed Structure
LM	Logical Model
LVS	Linear Variable Structure
MAC	Message Authentication Code
MF	Master File
MP	Machine Processable form (TTCN)
PC	Physical Characteristics
PDU	Protocol Data Unit
RC	Return Code
SCS	System Conformance Statement
SP	Signals and Protocols
SUT	System Under Test
TC	Test Case
TP	Test Purposes
TR	TRansparent
TSS	Test Suite Structure
TTCN	Tree and Tabular Combined Notation

4 General aspects

The Abstract Test Suites (ATS) for TS 101 200-3 [1] implementations uses the remote test method as described in ISO/IEC 9646-2 [3]. This test method needs just one external interface towards the card. This function is provided by the CAD simulator.

Depending on options supported by the Implementation Under Test (IUT) it is possible that only part of the test suite is applicable. A test selection procedure needs to be performed to determine the applicability of a test to a particular IUT. Such selection shall be based on the Implementation Conformance Statement (ICS) and the Implementation eXtra Information for Testing (IXIT). The Abstract Test Cases (ATCs) contained in the present document are a comprehensive reflection of the base standards.

For the various tests a number of files are needed. Ideally the ATS would use any available files on the IUT, but that would require a very detailed inquiry and initializing procedures of file identifiers, locations, access conditions and contents. Instead of that, this IXIT defines a configuration (a detailed data structure) containing a set of files with specific properties and contents. The ATS is able to use this configuration if existing, or create it alternatively. For this reason the client of the test house shall either equip the IUT with this configuration, or support the possibility to create the structure dynamically.

4.1 Test groups and subgroups

The test suite is structured following the rules defined in ISO/IEC 9646-2 [3].

4.2 Preamble

The preamble of each test case consists of the events required to bring the IUT to the appropriate initial state. Examples of such are the creation of files and data. There may be alternate sequences of test steps which can be performed to initialize the IUT. These test steps in the preamble for TC have been chosen carefully, considering the test methodology and the other test co-ordination procedures that are available.

4.3 Test body

The test body is the sequence of actions within a test case that is essential to achieve the test purpose, followed by the verification of the IUTs ending state. Verdicts are assigned to the possible outcomes of the test cases.

4.4 Postamble

At the end of the execution of a test body, the IUT may not be in the "initial state" (a stable state to be used as starting point for testing). A postamble is then required to bring the IUT from the ending state to an "initial state". For efficiency reasons the ATS does not remove created files nor does it undo modifications in files as long as this would not prevent the successful execution of other test cases. Therefore the IUT may contain at the end of the test campaign a file structure that is different from the initial state.

4.5 Instruction on completion of tables

The IXIT proforma request a number of aspects of the System Under Test (SUT) to be revealed. These aspects are questioned in the form of tables that shall be completed.

The meaning of the table columns is defined as follows:

Item	A sequential number used for referencing
Description (e.g. file, type)	A descriptive text of the item under question
Status/suggested value	An indication of requested support. Apart from literal values the following codes apply: o Optional c Conditional Y Yes, available/Yes, can be created N Not available/Cannot be created - Not applicable
Support/value/supported value	A confirmation in the form of a code or value as defined for status
Version	For a keyfile it indicates the current version
Identifier	The file identifier in hexadecimal notation of a DF or EF

Annex A (normative): IXIT proforma

A.1 Identification summary

This clause is to be completed by the test laboratory.

IXIT number:

....

Test laboratory name:

....

....

Date of issue:

....

Issued to:

....

The test laboratory may include client or contract references in the identification summary.

A.2 Abstract test suite summary

This clause is to be completed by the test laboratory.

System specification:

....

ATS specification:

....

....

Abstract test method(s):

....

....

A.3 Test laboratory

This clause is to be completed by the test laboratory.

Test laboratory identification:

....

....

....

....

Accreditation status of the test service:

....

Accreditation reference:

....

Test laboratory manager:

....

Test laboratory contact:

....

Means of testing:

Means of testing may include any particular facilities such as: executable test suite and test equipment (e.g. card readers).

....

....

....

....

....

Instructions for completion:

The laboratory should include any special instructions necessary for the completion and return of the proforma by the client.

....

....

....

....

....

A.4 Client

This clause is to be completed by the client.

Client identification:

....

....

....

....

Client test manager:

....

Client contact:

....

Test facilities required:

The client should record any particular facilities required for testing, if a range of facilities is provided by the test laboratory.

....

....

....

....

....

A.5 SUT (IC card)

Name:

....

Version:

....

ICS reference for IUT:

....

....

Limitations of the SUT:

The client may provide information explaining if any of the abstract test cases cannot be executed, e.g. non-support for file creation as intended.

....

....

....

....

....

Environmental conditions:

The test laboratory may specify the normal environmental conditions applying to the laboratory to be used for testing (e.g. temperature, humidity). The client should specify any tighter environmental conditions that may be necessary for the correct operation of the SUT.

....

....

A.6 Protocols

In tables A.1 and A.2 the client identifies relevant information concerning any protocol in the SUT on which the IUT may depend.

Table A.1: Protocol used

Item	Protocol name	Status	Support
1	T=0	o.1	
2	T=1	o.1	

o.1: It is mandatory to support at least one of these items.

A.6.1 T=0 protocol

Prerequisite: A.1/1 -- T=0 protocol

The supplier of the implementation shall indicate which options of the T=0 protocol specification are implemented.

No options for T=0 on which IUT or test system depend are foreseen.

A.6.2 T=1 protocol

Prerequisite: A.1/2 -- T=1 protocol

The supplier of the implementation shall indicate which options of the T=1 protocol specification are implemented.

Table A.2: T=1 protocol options

Item	Option	Status/ Suggested value	Support/ Supported value
1	Maximum block size	≥ 32	
2	Chaining mechanism	o	
3	Maximum command data	≥ 64	
4	Maximum command size	≥ 32	
5	WTX request	o	
6	IFS request	o	
7	Error recovery by R-blocks	o	
8	Error recovery by S-blocks	o	

A.7 Base standard identification

This clause is completed by the test laboratory and client in consultation.

Specification reference:..

Version: ....

ICS reference: ....

The ICS reference should reference a completed ICS which is conformant with the ICS proforma contained in TS 101 203-1 [7].

A.8 Implementation options

A.8.1 Configuration

For the purpose of testing a number of different files will be required. The ATS tries to use existing files with the requested properties. However if files with the requested properties do not exist, the ATS will attempt to create these files. If tests should be run that need non-existing files the IUT supplier shall make sure that the files can be created and written as specified. The IUT supplier is allowed to provide more files than specified in this configuration unless otherwise specified in the present document.

Figure A.1 depicts the required configuration (data structure). The following subclauses will list tables that provide details for each of the required files. The IUT supplier is requested to answer a number of questions for each of these files:

- Is the file with the defined properties already available on the IUT?
- If not available, can it be created according to the access conditions of the respective DF or MF?
- What is the file identifier (possibly the proposed file id)?
- In case of a keyfile, what is the current version?
- In case of a keyfile or CHV file, what is the value of the referenced key or the value of the CHV?

Default settings for files:

Unless otherwise specified in the present document, the following default settings apply to the files:

- Access conditions using keys refer to key number 0 (the first key).
- In DFs no CHV1 verification is required before INTERNAL AUTHENTICATION (bit 8 in byte 8 is set to '1').
- Files are not invalidated but can be.

- Files are not readable when invalidated.
- Files require the normal frequency for the authentication algorithm.
- Clock stop is not allowed.

Additional default settings for CHV files:

- CHV files are enabled, but can be disabled.
- CHV files are activated.
- CHV change is allowed.
- CHV is to be presented in clear (not enciphered).
- CHV is coded in BCD format.
- CHV files contain the CHV in stead of the path to the CHV.
- CHV and UNBLOCK CHV counters are at their initial value.

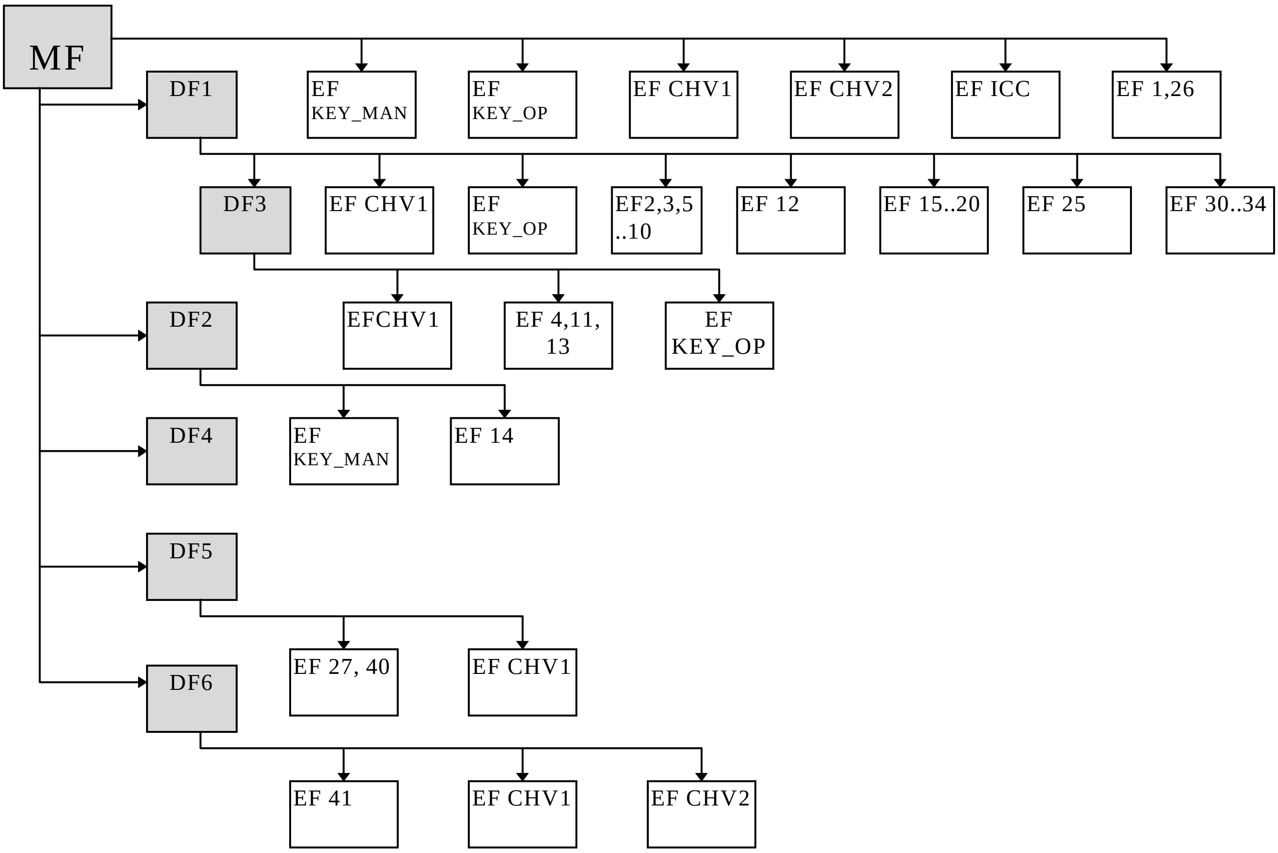

Figure A.1: Required configuration

In stead of completing all subsequent tables the IUT supplier is allowed, if the required configuration is already created, to declare support for all defined files, properties and suggested values in the following table.

Table A.3: Full configuration support

Item	full configuration support	Status	Support
1	The complete required configuration has been created and initialized on the IUT.	o	

A.8.1.1 Dedicated Files (DF)

The following table indicates DFs with specific requested characteristic. If such a DF is available it will be used, otherwise the test suite will try to create it, if that is supported.

The IUT supplier shall indicate for each row whether the described file already exists. If not it shall be indicated whether it can be created. If the file exist or can be created and the actual or preferred value of the file identifier is other than the suggested value, a value shall be provided. A number of tests will be excluded if no support for existence nor creation is given.

Table A.4: Dedicated Files (DF)

		Existence		Creation		Identifier		Size
Item	**File and properties**	**Status**	**Support**	**Status**	**Support**	**Suggested**	**Chosen**	
1	MF	Y		N		'3F00'		
2	DF1 with AC = ALW for all functions, containing no other special files than those defined in table 6	Y/N		Y/N/-		'8001'		
3	DF2 with AC = CHV1 on INVALIDATE REHABILITATE and DELETE FILE AC = PRO (key 1) on CREATE FILE containing no son files	Y/N		Y/N/-		'8002'		
4	DF3 with AC = ALW for all functions, except for EXTEND (PRO) containing no other special files than those defined in table 6; not more than 254 bytes available for EXTEND	Y/N		Y/N/-		'8003'		
5	DF4 with AC = PRO on DELETE, containing no son files	Y/N		Y/N/-		'8004'		
6	DF5 AC = PRO with non existing key on DELETE VERIFY CHV before IA	Y/N		Y/N		'8005'		
6	DF6 AC = PRO for CREATE FILE and DELETE with non existing key number for DELETE	Y/N		Y/N		'8006'		

In order to allow files to be created in the MF and other DFs additional info shall be provided in the following table. If no keys are required the table need not to be completed.

Table A.5: Access Conditions (AC) of the MF and related key

Item	**Property**	**Suggested**	**Support / Chosen**
1	Access Condition for CREATE FILE in MF	PRO	
1.1	Key number in EF_{KEY_MAN}	0	
2	Access Condition for DELETE FILE in MF	PRO	
2.1	Key number in EF_{KEY_MAN}	0	

A.8.1.2 Special Elementary Files (EF)

This subclause deals with special Elementary Files like CHV and key files. Each of the items in the following table contain a requirement for a special EF with specific requirements. If such an EF is supported (it exists), it will be used in the test. Otherwise the test system will try to create it, if allowed by the creation support column. As the creation of special files can be operating system dependent it is requested whether the creation of these files is allowed and their usage is conform the base standard. If the file does not exist and creation is not allowed the respective tests cannot be performed.

Table A.6: Availability of special Elementary Files (EF)

		Existence		Creation		Version	
Item	**File**	**Status**	**Support**	**Status**	**Support**	**Suggested**	**Support**
1	EF$_{CHV1}$ in MF which can be disabled, enabled, blocked and unblocked	Y/N		Y/N/-		-	
2	EF$_{CHV2}$ in MF which can be blocked and unblocked	Y/N		Y/N/-		-	
3	EF$_{KEY\_MAN}$ in MF	Y/N		Y/N/-		1	
4	EF$_{KEY\_OP}$ in MF with AC = CHV1 on INVALIDATE and REHABILITATE; AC = CHV1+PRO on LOAD KEY FILE and UPDATE	Y/N		Y/N/-		1	
5	EF$_{ICC}$ in MF	Y/N		Y/N/-		-	
6	EF$_{ID}$ in MF	Y/N		Y/N/-		-	
7	EF$_{LAN}$ in MF	Y/N		Y/N/-		-	
8	EF$_{NAM}$ in MF	Y/N		Y/N/-		-	
9	EF$_{KEY\_OP}$ in DF1 with AC = PRO on LOAD KEY FILE	Y/N		Y/N/-		1	
10	EF$_{CHV1}$ in DF1	Y/N		Y/N/-		-	
11	EF$_{CHV1}$ in DF3 which requires an enciphered CHV representation.	Y/N		Y/N/-		-	
12	EF$_{KEY\_OP}$ in DF3 AC = PRO on LOAD KEY FILE and key does not exist	Y/N		Y/N/-		1	
13	EF$_{KEY\_MAN}$ in DF2 which contains no keys	Y/N		Y/N/-		1	
14	EF$_{CHV1}$ in DF5 not allowed to be disabled	Y/N		Y/N/-		-	
15	EF$_{CHV1}$ in DF6 not allowed to be enabled	Y/N		Y/N/-		-	
16	EF$_{CHV2}$ in DF6 not activated	Y/N		Y/N/-		-	

In order verify the card capabilities a number of keys is required. The following tables request the values of keys and codes (CHVs) in the key files of the MF and DF1 and DF3. All keys and codes in existing EFs that are related to actual access conditions need to be provided. Whenever two CHV files in one DF exist the corresponding CHVs shall be different. Additionally an algorithm ID shall be given for each key. The usage of the algorithms may involve various modes of operation depending on their application. The semantics of the modes of operation shall be agreed between the IUT supplier and the test house. An example mode of operation could be 'Authentication for TESA-7'. If there are additional keys in the table, they can be added in a separate table. At least one key number shall be specified without key to be there, to test IUT behaviour in case of a missing key number.

Table A.7: Key values and secret codes

		Key value or secret code	
Item	**file and key**	**Suggested**	**Chosen**
1	CHV1 in MF	'1234'	
1.1	UNBLOCK CHV	'3456'	
2	CHV2 in MF	'5678'	
2.1	UNBLOCK CHV	'7890'	
3	relevant key in $\text{EF}_{\text{KEY\_MAN}}$ in MF	16 bytes counting up '00 .. 1F'	
3.1	Algorithm ID	TESA-7 ('04')	
3.2	number of relevant key for Internal Authentication in $\text{EF}_{\text{KEY\_MAN}}$ in MF	-	
3.3	relevant key for Internal Authentication in $\text{EF}_{\text{KEY\_MAN}}$ in MF	16 bytes counting up '00 .. 1F'	
3.4	Algorithm ID of relevant key for Internal Authentication in $\text{EF}_{\text{KEY\_MAN}}$ in MF	TESA-7 ('04')	
3.5	not present key number	'A'	
4	relevant key in $\text{EF}_{\text{KEY\_OP}}$ in MF	16 bytes counting up '20 .. 3F'	
4.1	Algorithm ID	TESA-7 ('04')	
4.2	number of relevant key for Internal Authentication in $\text{EF}_{\text{KEY\_OP}}$ in MF	-	
4.3	relevant key for Internal Authentication in $\text{EF}_{\text{KEY\_OP}}$ in MF	16 bytes counting up '00 .. 1F'	
4.4	Algorithm ID of relevant key for Internal Authentication in $\text{EF}_{\text{KEY\_OP}}$ in MF	TESA-7 ('04')	
5	relevant key in $\text{EF}_{\text{KEY\_OP}}$ in DF1	16 bytes counting up '20 .. 3F'	
5.1	Algorithm ID	TESA-7 ('04')	
5.2	number of relevant key for Internal Authentication in $\text{EF}_{\text{KEY\_OP}}$ in DF1	-	
5.3	relevant key for Internal Authentication in $\text{EF}_{\text{KEY\_OP}}$ in DF1	16 bytes counting up '00 .. 1F'	
5.4	Algorithm ID of relevant key for Internal Authentication in $\text{EF}_{\text{KEY\_OP}}$ in DF1	TESA-7 ('04')	
5.5	not present key number	'A'	
6	CHV1 in DF1 (enciphered)	'4321'	
6.1	UNBLOCK CHV (enciphered)	'6543'	
7	CHV1 in DF3	'8765'	
7.1	UNBLOCK CHV	'0987'	
8	CHV1 in DF5	'8765'	
9	CHV1 in DF6	'8765'	
10	CHV2 in DF6	'8765'	
10.1	UNBLOCK CHV	'0987'	

Table A.8: Values of EF_{ICC}

Item	Data	Value
1	Clockstop	
2	IC card serial number	
3	IC card manufacturing references	
4	Card personlizer ID	
5	Embedder/ IC assembler ID	
6	IC identifier	
7	Card profile	
8	Type of Selection	

Table A.9: Values of EF_{ID}

Item	Data	Value
1	Identification number	
2	Date of activation	
3	Card expiry date	
4	Card sequence number	
5	Country Code	

Table A.10: Values of EF_{LAN}

Item	Data	Value
1	First language preference	
2	Second language preference	
3	Third language preference	
4	Fourth language preference	

Table A.11: Values of EF_{NAM}

Item	Data	Value
1	Card Holder Name	

A.8.1.3 Linear Fixed Structure (LFS) Elementary Files (EF)

The following table indicates linear fixed structure (LFS) EFs with specific requested characteristics. If such an EF is available it will be used, otherwise the test suite will try to create it.

Table A.12: Linear Fixed Structure Elementary Files

		Existence		Creation		Identifier	
Item	**File**	**Status**	**Support**	**Status**	**Support**	**Suggested**	**Support**
1	EF15; an LFS EF with AC = AUT on UPDATE and WRITE; AC = CHV1 on CREATE RECORD and READ Record size is 5	Y/N		Y/N/-		'300F'	
2	EF16; an LFS EF with AC = PRO on WRITE, INVALIDATE, REHABILITATE, UPDATE and WRITE, while its record size is 5	Y/N		Y/N/-		'3010'	
3	EF17; an LFS EF with AC = PRO on UPDATE, WRITE and READ while the referenced key does not exist	Y/N		Y/N/-		'3011'	
4	EF18; an LFS EF with AC = ALW on all functions, while record size = 5 and it has 255 records. The file can be invalidated and extended; not readable when invalidated	Y/N		Y/N/-		'3012'	
5	EF19; an LFS EF with AC = ALW on all functions, while record size = 30; not readable when invalidated	Y/N		Y/N/-		'3013'	
6	EF20; an LFS EF with AC = ALW on all functions, which has 5 records of size = 4	Y/N		Y/N/-		'3014'	

A.8.1.4 Linear Variable Structure (LVS) Elementary Files (EF)

The following table indicates Linear Variable Structure (LVS) EFs with specific requested characteristics. If such an EF is available it will be used, otherwise the test suite will try to create it.

Table A.13: Linear Variable Structure Elementary Files

		Existence		Creation		Identifier	
Item	**File**	**Status**	**Support**	**Status**	**Support**	**Suggested**	**Support**
1	EF25; an LVS EF with AC = ALW on all functions, which is readable, can be extended and has 2 or more records	Y/N		Y/N/-		'3019'	
2	EF26; an LVS EF with AC = CHV1 on read	Y/N		Y/N/-		'301A'	
3	EF27; an LVS EF with AC = CHV1 on read	Y/N		Y/N/-		'301B'	

A.8.1.5 Cyclic Structure (CS) Elementary Files (EF)

The following table indicates cyclic structure (CS) EFs with specific requested characteristics. If such an EF is available it will be used, otherwise the test suite will try to create it.

Table A.14: Cyclic Structure Elementary Files

		Existence		Creation		Identifier	
Item	**File**	**Status**	**Support**	**Status**	**Support**	**Suggested**	**Support**
1	EF30; a CS EF with AC = PRO on INCREASE and DECREASE while the referenced key does not exist	Y/N		Y/N/-		'301E'	
2	EF31; a CS EF with AC = ALW for all functions which can be invalidated and extended. It is updatable, readable and non-empty. Its has 4 records of size 5	Y/N		Y/N/-		'301F'	
3	EF32; a CS EF with AC = ALW for all functions. It has 4 records of size 5	Y/N		Y/N/-		'3020'	
4	EF33; a CS EF with AC = PRO for INCREASE and DECREASE. It has 4 records of size 5	Y/N		Y/N/-		'3021'	
5	EF34; a CS EF with AC = CHV1 for INCREASE and DECREASE. It has 4 records of size 5	Y/N		Y/N/-		'3022'	

A.8.1.6 Transparent structure (TR) Elementary Files (EF)

The following table indicates TRansparent (TR) EFs with specific requested characteristics. If such an EF is available it will be used, otherwise the test suite will try to create it.

Table A.15: Transparent Elementary Files

		Existence		Creation		Identifier	
Item	**File**	**Status**	**Support**	**Status**	**Support**	**Suggested**	**Support**
1	EF1; a TR EF with AC = PRO on READ, UPDATE, WRITE and EXECUTE while the referenced key does not exist	Y/N		Y/N/-		'3001'	
2	EF2; a TR EF with AC = CHV1 on READ	Y/N		Y/N/-		'3002'	
3	EF3; a TR EF with AC = CHV2 on READ	Y/N		Y/N/-		'3003'	
4	EF4; a TR EF with AC = ALW on READ	Y/N		Y/N/-		'3004'	
5	EF5; a TR EF with AC = AUT on READ	Y/N		Y/N/-		'3005'	
6	EF6; a TR EF with AC = CHV1/AUT on READ; AC = CHV1/PRO on UPDATE	Y/N		Y/N/-		'3006'	
7	EF7; a TR EF with AC = NEV on READ; AC = PRO on UPDATE	Y/N		Y/N/-		'3007'	
8	EF8; a TR EF which is invalidated and contains a program	Y/N		Y/N/-		'3008'	
9	EF9; a TR EF which can be invalidated, deleted, extended and updated. It is readable when invalidated. Its size is > 3 bytes.	Y/N		Y/N/-		'3009'	
10	EF10; a TR EF which can be updated. Its size is > 300 bytes.	Y/N		Y/N/-		'300A'	
11	EF11; a TR EF with AC = ALW on READ; AC = CHV1 on UPDATE	Y/N		Y/N/-		'300B'	
12	EF12; a TR EF with AC = CHV2/AUT on READ; AC = CHV2/PRO on UPDATE	Y/N		Y/N/-		'300C'	
13	EF13; a TR EF with AC = CHV1 on READ	Y/N		Y/N/-		'300D'	
14	EF14; a TR EF with AC = CHV1 on READ	Y/N		Y/N/-		'300E'	

A.8.1.7 Elementary Files (EF) containing programs

The following table indicates EFs containing programs with specific requested characteristics. If such an EF is available it will be used, otherwise the test suite will try to create it.

Table A.16: EFs containing programs

		Existence		Creation		Identifier	
Item	**File**	**Status**	**Support**	**Status**	**Support**	**Suggested**	**Support**
1	EF40 AC = PRO on EXECUTE with non existing key	Y/N		Y/N/-		'300F'	
2	EF41 AC = PRO on EXECUTE	Y/N		Y/N/-		'3010'	

A.8.2 File Identifiers (ID)

Table A.17: File Identifiers

Item	Limitation	Suggested value	Supported value
1	Highest allowed file identifier	'FFFE'	
2	Unused file identifier	'3030'	

A.8.3 Size limitations

Table A.18: Size limitations

Item	Limitation	Suggested value	Supported value
1	Maximum level of nested DFs within the file structure on the IC card	> 8	
2	Maximum size of EFs or DFs to be created	> 300	

A.8.4 Keyfile version handling

When loading the first key in a keyfile by means of the LOAD KEY FILE command a version number should be indicated. The success of this command may depend on the value of this field.

Prerequisite: LOAD KEY FILE command supported

Table A.19: Keyfile version handling

Item	Physical characteristic	Status	Support
1	Version number does not affect success of command	o	
2	Command shall include current version number	o	
3	Command shall include increased version number	o	
4	Version management is handled differently	o	

A.8.5 CHV limitations

Table A.20: CHV limitations

Item	Limitation	Suggested value	Supported value
1	CHV retry counter	3	
2	Successful UNBLOCK CHV procedures	100	

A.8.6 Memory behaviour

Table A.21: Specific memory failures

Item	Memory failure	Supported (Y/N)
1	Is it possible to activate and deactivate the internal retry routine	
2	Is it possible to activate and deactivate a memory failure	

A.8.7 Supported CLA bytes

Table A.22: Supported Class

Item	Supported	Byte value
1	Class	

A.8.8 Unsupported CLA and INS bytes

Table A.23: Unsupported Class (CLA) and Instruction (INS)

Item	Unsupported	Byte value
1	Class	
2	Instruction	

Annex B (normative): Abstract Test Suite (ATS)

This ATS has been produced using the Tree and Tabular Combined Notation (TTCN) according to ISO/IEC 9646-3 [4].

The ATS was developed on a separate TTCN software tool and therefore the TTCN tables are not completely referenced in the contents table. The ATS itself contains a Test Suite Overview Part which provides additional information and references.

The ATS specializes the tests that were defined in the TSS&TP document (TS 101 203-2 [8]) by means of a formal language (TTCN). But not all test purposes were suitable to be expressed formally, therefore the following test groups have been excluded from the ATS:

- PC: Physical Characteristics;
- SP: (electronic) Signals and Protocols.

The actual execution of these test shall be based on the textual description within the TSS&TP document (TS 101 203-2) [8].

Additionally there are tests that need dedicated implementation procedures that are not provided within the ATS. Examples of these are tests that require the IUT to be in a state having memory problems. In these situations empty test steps are provided that can be specialized by the test house in order to fulfil the precondition.

Naming conventions:

- Test case names correspond to the test purpose names in the TSS&TP document (TS 101 203-2 [8]).
- IXIT parameters start with "PX_".
- Constraint names start with "S_" for SEND constraints, and "R_" for RECEIVE constraints.
- Constraint names additionally contain an abbreviation of the command, e.g.: "SE_" for SELECT.

B.1 The TTCN Graphical form (TTCN.GR)

The TTCN.GR representation of this ATS is contained in a Word document (GR900329.DOC) which can be found on the diskette which is attached to the last page of the present document.

B.2 The TTCN Machine Processable form (TTCN.MP)

The TTCN.MP representation corresponding to this ATS is contained in an ASCII file (MP900329.MP) which can be found on the diskette which is attached to the last page of the present document.

NOTE: According to ISO/IEC 9646-3 [4], in case of a conflict in interpretation of the operational semantics of TTCN.GR and TTCN.MP, the operational semantics of the TTCN.GR representation takes precedence.

Annex C (informative): Bibliography

- ETS 300 406 (April 1995): "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

- ISO/IEC 9646-7 (1995): "Information technology - Open systems interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

- ENV 1375-1 "Identification card systems - Intersector integrated circuit(s) and additional formats - Part 1: ID-000 card size and physical characteristics".

- ENV 1375-2 "Identification card systems - Intersector integrated circuit(s) and additional formats - Part 2: ID-00 card size and physical characteristics".

- EN 27811-1 "Identification card systems - Recording technique - Part 1: Embossing".

- EN 27816-1: "Identification cards - Integrated circuit(s) cards with cards contacts - Part 1: Physical characteristics".

- EN 27816-2: "Identification cards - Integrated circuit(s) cards with cards contacts - Part 2: Dimensions and location of the contacts".

- EN 27816-3: "Identification cards - Integrated circuit(s) cards with cards contacts - Part 3: Electronic signals and transmission protocols".

- ISO/IEC 7816-4: "Identification cards; Integrated circuit(s) cards with contacts; Part 4: Interindustry commands for interchange".

- ISO/IEC 7816-5: "Identification cards; Integrated circuit(s) cards with contacts; Part 5: Numbering system and registration procedure for application identifiers".

History

Document history		
V1.1.1	July 1997	Publication

ISBN 2-7437-1533-2
Dépôt légal : Juillet 1997