TS 101 207-1 V1.1.1 (1997-07)

Technical Specification

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

European Telecommunications Standards Institute

Reference
DTS/PTS-00207-1 (b6c90icr.PDF)

Keywords
Card, testing, ICS, security

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 4
Foreword 4
1 Scope 5
2 Normative references 5
3 Definitions and abbreviations 6
3.1 Definitions 6
3.2 Abbreviations 6
4 Conformance to this ICS proforma specification 7
Annex A (normative): ICS proforma for the Security Module (SM) 8
A.1 Guidance for completing the ICS proforma 8
A.1.1 Purpose and structure 8
A.1.2 Abbreviations and conventions 9
A.1.3 Instructions for completing the ICS proforma 10
A.2 Identification of the implementation 10
A.2.1 Date of the statement 10
A.2.2 Implementation Under Test (IUT) identification 10
A.2.3 System Under Test (SUT) identification 11
A.2.4 Product supplier 11
A.2.5 Client (if different from product supplier) 11
A.2.6 ICS contact person 12
A.3 Identification of the standards 12
A.4 Global statement of conformance 12
A.5 Security Module (SM) 13
A.5.1 Physical characteristics 13
A.5.2 Electronic signals and transmission protocols 13
A.5.3 Logical model 13
A.5.3.1 Major characteristics 13
A.5.4 General concepts 14
A.5.4.1 General security principles 14
A.5.4.2 Access conditions 14
A.5.4.3 Sequence control 14
A.5.4.4 Configuration 15
A.5.4.5 Security functions 15
A.5.5 Description of the functions 15
A.5.6 Data elements 19
A.5.6.1 Command versus status responses 19
A.5.6.2 Status word coding 21
A.5.7 Contents of the elementary files 22
A.5.7.1 Contents of the EFs 22
A.5.8 Description of the commands 23
A.5.8.1 Mapping principle 23
A.5.8.2 Coding of the commands 23
A.5.9 Downloading of keys from SM to UC 24
Annex B (informative): Bibliography 25
History 26

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 1 of a multi-part document covering Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-7, 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

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

The present document provides the Implementation Conformance Statement (ICS) proforma for the Security Module (SM) defined in TS 101 200-7 [8] in compliance with the relevant requirements, and in accordance with the relevant guidance given in ISO/IEC 9646-7 [12] and ETS 300 406 [10].

The supplier of an implementation that is claimed to conform to the present document is required to complete a copy of the ICS proforma provided in annex A of the present document and is required to provide the information necessary to identify both the supplier and the implementation.

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] EN 27816-1 (1989): "Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics".

[2] EN 27816-2 (1989): "Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and locations of the contacts".

[3] EN 27816-3 (1992): "Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols".

[4] EN 27816-3 (1992)/A1(1993): "Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols. Amendment 1: Protocol type T=1, asynchronous half duplex block transmission protocol".

[5] EN 27816-3 (1992)/A2(1995): "Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols. Amendment 2: Revision of protocol type selection".

[6] ISO/IEC 7816-4 (1995(E)): "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter industry commands for interchange".

[7] 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".

[8] TS 101 200-7 version 1.2.1: "prEN 726-7: Identification card systems; Telecommunications IC cards and terminals; Part 7: Security module".

[9] 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".

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

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

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

3 Definitions and abbreviations

3.1 Definitions

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

- terms defined in ISO/IEC 7816 parts 1 to 3 [1], [2], [3], [4], [5];
- terms defined in TS 101 200-3 [7];
- terms defined in ISO/IEC 9646-1 [11] and in ISO/IEC 9646-7 [12].

In particular, the following terms defined in ISO/IEC 9646-1 [11] 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 Abbreviations

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

AC	Access Condition(s)
AlgoId	Algorithm Identifier
ATC	Abstract Test Case
ATR	Answer To Reset
ATS	Abstract Test Suites
BCD	Binary Code Decimal
CAD	Card Accepting Device (this includes only the mechanics)
CHV	Card Holder Verification
CLA	CLAss
CS	Cyclic Structure
DF	Dedicated File
EF	Elementary File
EW	External World
GR	GRaphical form (TTCN)
IC	Integrated Circuit
ICC	IC Card
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)
PDU	Protocol Data Unit
RC	Return Code
SCS	System Conformance Statement
SM	Security Module
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
UC	User Card

4 Conformance to this ICS proforma specification

If it claims to conform to the present document, the actual ICS proforma to be filled in by a supplier shall be technically equivalent to the text of the ICS proforma given in annex A, and shall preserve the numbering/naming and ordering of the proforma items.

An ICS, which conforms to the present document shall:

1. describe an implementation which claims to conform to TS 101 200-7 [8];

2. be a conforming ICS proforma completed in accordance with the guidance for completion given in clause A.1;

3. include the information necessary to uniquely identify both the supplier and the implementation.

Annex A (normative): ICS proforma for the Security Module (SM)

A.1 Guidance for completing the ICS proforma

A.1.1 Purpose and structure

The purpose of this ICS proforma is to provide a mechanism whereby a supplier of a Security Module (SM) according to TS 101 200-7 [8] may provide information about the implementation in a standardized manner.

The ICS proforma is subdivided into subclauses for the following categories of information:

- A.1 Guidance for completing the ICS proforma
- A.2 Identification of the implementation
- A.3 Identification of the standards
- A.4 Global statement of conformance
- A.5 Security Module (SM)
  - A.5.1 Physical characteristics
  - A.5.2 Electronic signals and transmission protocols
  - A.5.3 Logical model
    - A.5.3.1 Major characteristics
  - A.5.4 General concepts
    - A.5.4.1 General security principles
    - A.5.4.2 Access conditions
    - A.5.4.3 Sequence control
    - A.5.4.4 Configuration
    - A.5.4.5 Security functions
  - A.5.5 Description of the functions
  - A.5.6 Data elements
    - A.5.6.1 Command versus status responses
    - A.5.6.2 Status word coding
  - A.5.7 Contents of the Elementary Files (EFs)
  - A.5.8 Description of the commands
    - A.5.8.1 Mapping principle
    - A.5.8.2 Coding of the commands
  - A.5.9 Downloading of keys from SM to UC

A.1.2 Abbreviations and conventions

The ICS proforma contained in this annex is composed of information in tabular form in accordance with the guidelines presented in ISO/IEC 9646-7 [12].

Item column

The item column contains a number that identifies the item in the table.

Item description column

The item description column describes in free text each respective item (e.g. parameters, timers, etc.). It implicitly means "is <item description> supported by the implementation?".

Status column

The following notations, defined in ISO/IEC 9646-7 [12], are used for the status column:

m	mandatory - the capability is required to be supported.
o	optional - the capability may be supported or not.
n/a	not applicable - in the given context, it is impossible to use the capability.
x	prohibited (excluded) - there is a requirement not to use this capability in the given context.
o.i	qualified optional - for mutually exclusive or selectable options from a set. "i" is an integer which identifies an unique group of related optional items and the logic of their selection which is defined immediately following the table.
ci_j	conditional - the requirement on the capability ("m", "o", "x" or "n/a") depends on the support of other optional or conditional items stated in Table "i" Item "j". The unique conditional status expression that is defined immediately following the table.
c:	conditional relative to higher level - the requirement on the capability ("m", "o", "x" or "c") depends on the support of a higher level item. For example, item 2.1 with status c:m means that the item shall be supported if item 2 is supported. That notation does not apply following a mandatory requirement, although an index may be used to define a dependency. For example item 3 is mandatory, 3.1 is optional. This is indicated only by an "o", although not fulfilling 3 makes 3.1 "n/a".

Reference column

The reference columns give explicit reference to TS 101 200-7 [8], except where stated otherwise.

Support column

The support column shall be filled in by the supplier of the implementation. The following common notations, defined in ISO/IEC 9646-7 [12], are used for the support column:

Y or y	supported by the implementation
N or n	not supported by the implementation
N/A, n/a or -	no answer required (allowed only if the status is n/a, directly or after evaluation of a conditional status)

If this ICS proforma is completed in order to describe a multiple-profile support in a system, it is necessary to be able to answer that a capability is supported for one profile and not supported for another. In that case, the supplier shall enter the unique reference to a conditional expression, preceded by "?" (e.g. ?3). This expression shall be given in the space for comments provided at the bottom of the table. It uses predicates defined in the System Conformance Statement (SCS), each of which refers to a single profile and which takes the value TRUE if and only if that profile is to be used.

EXAMPLE 1: ?3: IF prof1 THEN Y ELSE N

It is also possible to provide a comment to an answer in the space provided at the bottom of the table.

References to items

For each possible item answer (answer in the support column) within the ICS proforma exists a unique reference, used, for example, in the conditional expressions. It is defined as the table identifier, followed by a solidus character "/", followed by the item number in the table. If there is more than one support column in a table, the columns shall be discriminated by letters (a, b, etc.), respectively.

EXAMPLE 2: A.5/4 is the reference to the answer of item 4 in table 5 of annex A.

EXAMPLE 3: A.6/3b is the reference to the second answer (i.e. in the second support column) of item 3 in table 6 of annex A.

Prerequisite line

A prerequisite line takes the form: Prerequisite: <predicate>.

A prerequisite line after a clause or table title indicates that the whole clause or the whole table is not required to be completed if the predicate is FALSE.

A.1.3 Instructions for completing the ICS proforma

The supplier of the implementation shall complete the ICS proforma in each of the spaces provided. In particular, an explicit answer shall be entered, in each of the support boxes provided, using the notation described in subclause A.1.2.

If necessary, the supplier may provide additional comments in space at the bottom of the tables, or separately on sheets of paper.

More detailed instructions are given at the beginning of the different subclauses of the ICS proforma.

A.2 Identification of the implementation

Identification of the Implementation Under Test (IUT) and the system in which it resides (the System Under Test (SUT)) should be filled in so as to provide as much detail as possible regarding version numbers and configuration options.

The product supplier information and client information should both be filled in if they are different.

A person who can answer queries regarding information supplied in the ICS should be named as the contact person.

A.2.1 Date of the statement

.....

A.2.2 Implementation Under Test (IUT) identification

IUT name:

.....

.....

IUT version:

.....

A.2.3 System Under Test (SUT) identification

SUT name:

.....

Hardware configuration:

.....

Operating system:

.....

A.2.4 Product supplier

Name:

.....

Address:

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

A.2.5 Client (if different from product supplier)

Name:

.....

Address:

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

A.2.6 ICS contact person

(A person to contact if there are any queries concerning the content of the ICS)

Name:

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

.....

A.3 Identification of the standards

This ICS proforma applies to the following standard:

TS 101 200-7 [8]: "Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 7: Security Module".

A.4 Global statement of conformance

Are all mandatory capabilities implemented? (Yes/No) .....

NOTE: Answering "No" to this question indicates non-conformance to the standard specifications. Non-supported mandatory capabilities are to be identified in the ICS, with an explanation of why the implementation is non-conforming, on pages attached to the ICS proforma.

A.5 Security Module (SM)

A.5.1 Physical characteristics

Table A.1: Physical characteristics

Item	Physical characteristics	Reference	Status	Support
1	The SM format is an IC card	5	o	
1.1	Physical characteristics in accordance with TS 101 200-3 [7], clause 4.	4	c:m	

Comments:

A.5.2 Electronic signals and transmission protocols

Table A.2: Electrical characteristics

Item	Electrical characteristics	Reference	Status	Support
1	Electrical characteristics in accordance with TS 101 200-3 [7], clause 5.	5	c2_1	
2	T=0 transmission protocol is supported	5	c2_2	

c2_1: IF A.1/1 THEN m -- SM is an IC card
c2_2: IF A.1/1 THEN o -- SM is an IC card

Comments:

A.5.3 Logical model

A.5.3.1 Major characteristics

Table A.3: Major characteristics

Item	Major characteristics	Reference	Status	Support
1	Permanent secrets (master keys)	6	m	
2	Temporary secrets (diversified keys)	6	m	
3	Balance	6	o	
4	Other options	6	o	
4.1	No interference with basic contents	6	c:m	

Comments:

A.5.4 General concepts

Some of the requirements in this clause are not testable by means of an ATS, therefore the manufacturer should give a statement on the fulfilling of these requirements.

A.5.4.1 General security principles

Table A.4: Security principles

Item	Security principle	Reference	Status	Support
1	SM operation or data from the SM does not compromise the security of the system	7.1	m	
2	Cryptographic keys are managed in a way that security of system using the SM is not compromised	7.1	m	
3	The SM contains several keysets	7.1	o	

The SM provider should be responsible for the life cycle.

Comments:

A.5.4.2 Access conditions

Table A.5: Access conditions

Item	Access condition	Reference	Status	Support
1	ACs implemented	7.1.1	o	
1.1	ACs are implemented in accordance with TS 101 200-3 [7]	7.1.1	c:c2_1	
2	Usage of keys restricted	7.1.1	o	
3	Key diversification is available for function not according to TS 101 200-3 [7]	7.1.1	o	
3.1	The limits of the usage of the keys is kept inside the SM	7.1.1	c:m	

Comments:

A.5.4.3 Sequence control

Table A.6: Sequence control

Item	Sequence control	Reference	Status	Support
1	Sequence control implemented	7.1.2	o	
1.1	The result is according to TS 101 200-7 [8], if the command is allowed	7.1.2	c:m	
1.2	The result is "command out of sequence", if the command is not allowed	7.1.2	c:m	

Comments:

A.5.4.4 Configuration

Table A.7: System layout

Item	Layout	Reference	Status	Support
1	The card - terminal interface is not affected by the type of implementation of the SM	7.3	m	

Comments:

A.5.4.5 Security functions

Table A.8: Security functions

Item	Security functions	Reference	Status	Support
1	The SM is logically and physically protected against attacks aimed at exposing or abusing secrets during the whole life cycle of the SM	7.4	m	
2	The provided functions are independent of transmission protocols	7.4	m	
3	The SM uses the same keys and algorithm as the UC	7.4	m	
3.1	The SM is based on symmetric algorithms	7.4	m	
3.2	The SM is based on diversified keys	7.4	m	

Comments:

A.5.5 Description of the functions

Table A.9: Functions without MAC

Item	Function	Reference	Status	Support
1	SELECT KEYSET	8.1.1	m	
1.1	The SM selects a keyset with the key file version given by the UC, if the UC is following TS 101 200-3 [7]	8.1.1	m	
2	DIVERSIFY KEYSET	8.1.2	m	
2.1	Keys (diversified and master) are protected against being read out	8.1.2	m	
2.2	DIVERSIFY KEYSET has to be preceded by SELECT KEYSET	8.1.2	m	
2.3	The diversified keyset is kept in the SM and is valid until the DIVERSIFY KEYSET with the same master keyset takes place.	8.1.2	m	
3	ASK PARAMETER	8.1.3	m	
3.1	The parameter is valid only until the next function requires a challenge, if the command is not VERIFY MAC	8.1.3	m	
3.2	Multiple counter exist	8.1.3	o.1	
3.2.1	The counter associated with the selected keyset is used	8.1.3	c:m	
3.3	Only one common counter is used	8.1.3	o.1	

o.1: It is mandatory to support one of these options

Comments:

Table A.10: Functions used to compute MAC/CRYPTOGRAM

Item	Function	Reference	Status	Support
1	COMPUTE LOAD KEY	8.2.1	o	
1.1	The SM performs an enciphering of the key of the selected keyset	8.2.1	c:m	
1.2	The enciphered key, the contents of the data field and the challenge given by the UC is used to provide a cryptogram	8.2.1	c:m	
1.3	A GIVE RANDOM is to be used to transmit the random number from the UC	8.2.1	c:m	
1.4	The SELECT KEYSET function is to be executed before	8.2.1	c:m	
1.4.1	It is checked that the relevant keyfile contains diversified keys	8.2.1	c:m	
2	COMPUTE MAC	8.2.2	o	
2.1	COMPUTE MAC is used to calculate the MAC for functions of the UC, where the AC is PRO.	8.2.2	c:m	
2.2	A GIVE RANDOM is to be used to transmit the random number from the UC	8.2.2	c:m	
2.3	The SELECT KEYSET function is to be executed before	8.2.2	c:m	
2.3.1	It is checked that the relevant keyfile contains diversified keys	8.2.2	c:m	
3	COMPUTE CRYPTOGRAM	8.2.3	o	
3.1	COMPUTE CRYPTOGRAM is used to calculate the cryptogram for the EXTERNAL AUTHENTICATION command.	8.2.3	c:m	
3.2	A GIVE RANDOM is to be used to transmit the random number from the UC	8.2.3	c:m	
3.3	The SELECT KEYSET function is to be executed before	8.2.3	c:m	
3.3.1	It is checked that the relevant keyfile contains diversified keys	8.2.3	c:m	
4	DECREASE(SM)	8.3.4	o	
4.1	The SM checks if the indicated key is allowed to perform this function	8.3.4	c:m	
4.2	A GIVE RANDOM is to be used to transmit the random number from the UC	8.3.4	c:m	
4.3	The SELECT KEYSET function is to be executed before	8.3.4	c:m	
4.3.1	It is checked that the relevant keyfile contains diversified keys	8.3.4	c:m	
4.4	A check is done, whether the file to be decreased is selected.	8.3.4	c:m	
4.5	The result is the value of the SM file decreased by the value of the input parameter and a MAC for the INCREASE (UC) command.	8.3.4	c:m	

5	COMPUTE MAC EW	8.2.4	o	
5.1	COMPUTE MAC EW is used to add a cryptogram to data given to the SM.	8.2.4	c:m	
5.2	An ASK PARAMETER is to be used to get a challenge.	8.2.4	c:m	
5.3	It is checked that EF_{KEY_OP} (SM) is selected.	8.2.4	c:m	
5.4	It is checked that for the selected key the flag "AUTHENTICATION ALLOWED" is set.	8.2.4	c:m	
5.5	A chaining of COMPUTE MAC EW commands is allowed	8.2.4	c:o	

c10_1: IF A.4/4 THEN m -- several keysets are supported

Comments:

Table A.11: Functions used to verify MAC/CRYPTOGRAM

Item	Function	Reference	Status	Support
1	VERIFY MAC	8.3.1	o	
1.1	The SM checks if the indicated key is allowed to perform this function	8.3.1	c:m	
1.2	An ASK PARAMETER is to be used to obtain the random number to be transmitted to the UC	8.3.1	c:m	
1.3	The SELECT KEYSET function is to be executed before	8.3.1	c:m	
1.3.1	It is checked that the relevant keyfile contains diversified keys	8.3.1	c:m	
2	UPDATE(SM)	8.3.2	o	
2.1	The MAC in the input parameters is checked, before an update is performed.	8.3.2	c:m	
2.1	The SM checks if the indicated key is allowed to perform this function	8.3.2	c:m	
2.2	An ASK PARAMETER is to be used to obtain the random number to be transmitted to the UC	8.3.2	c:m	
2.3	The SELECT KEYSET function is to be executed before	8.3.2	c:m	
2.3.1	It is checked that the relevant keyfile contains diversified keys	8.3.2	c:m	
2.4	A check is done, whether the file to be updated is selected.	8.3.2	c:m	

3	INCREASE(SM)	8.3.3	o	
3.1	The SM checks if the indicated key is allowed to perform this function	8.3.3	c:m	
3.2	An ASK PARAMETER is to be used to obtain the random number to be transmitted to the UC	8.3.3	c:m	
3.3	The SELECT KEYSET function is to be executed before	8.3.3	c:m	
3.3.1	It is checked that the relevant keyfile contains diversified keys	8.3.3	m	
3.4	A check is done, whether the file to be increased is selected	8.3.3	c:m	
3.5	The input parameter are checked, before an update is performed	8.3.3	c:m	
3.6	The result is the value of the SM file increased by the value of the input parameter	8.3.3	c:m	
4	VERIFY CRYPTOGRAM	8.3.5	o	
4.1	An ASK PARAMETER is to be used to obtain the random number to be transmitted to the UC	8.3.5	c:m	
4.2	The SELECT KEYSET function is to be executed before	8.3.5	c:m	
4.2.1	It is checked that the relevant keyfile contains diversified keys	8.3.5	c:m	

Comments:

Table A.12: Functionality on SM - EW interface

Item	Functionality	Reference	Status	Support
1	The functions and the set of commands are in accordance with EN726-3 [7]	8.5	c2_1	

Comments:

Table A.13: General functionality

Item	Functionality	Reference	Status	Support
1	The SM handles information to link the keys with their respective functions.	8.6	m	
1.1	Relevant key qualifier	8.6	m	
1.2	master key	8.6	m	
1.3	Algorithm ID	8.6	m	
1.4	Algorithm	8.6	m	
1.5	Diversified key	8.6	m	
1.6	Functions allowed to use this key	8.6	m	
1.7	Access conditions to change this set of information	8.6	m	
2	The usage of keys is restricted	8.7	m	
2.1	COMPUTE MAC (EXECUTE)	8.7	c13_1	
2.2	COMPUTE MAC (DECREASE)	8.7	c13_1	
2.3	VERIFY MAC (READ BINARY STAMPED)	8.7	c13_2	
2.4	VERIFY MAC (READ RECORD STAMPED)	8.7	c13_2	

2.5	VERIFY CRYPTOGRAM (INTERNAL AUTHENTICATION)	8.7	c13_3	
2.6	UPDATE (SM)	8.7	c13_4	
2.7	INCREASE (SM)	8.7	c13_5	
2.8	DECREASE (SM)	8.7	c13_6	
2.9	COMPUTE MAC EW	8.7	c13_7	

c13_1: IF A.10/2 THEN m -- COMPUTE MAC is supported
c13_2: IF A.11/1 THEN m -- VERIFY MAC is supported
c13_3: IF A.11/4 THEN m -- VERIFY CRYPTOGRAM is supported
c13_4: IF A.11/2 THEN m -- UPDATE (SM) is supported
c13_5: IF A.11/3 THEN m -- INCREASE (SM) is supported
c13_6: IF A.10/4 THEN m -- DECREASE (SM) is supported
c13_7: IF A.10/5 THEN m -- COMPUTE MAC EW is supported

Comments:

A.5.6 Data elements

A.5.6.1 Command versus status responses

For consistency of an application using different types of SMs the responses to different functions shall have the same meaning.

Table A.14: Status responses

Item	Responses	Reference	Status	Support
1	SELECT KEYSET	9.3.1	m	
1.1	SW = '98 AD'	9.3.1	c14_2	
1.2	SW = '94 04'	9.3.1	o	
1.3	SW = '6E XX'	9.3.1	o	
1.4	SW = '6D XX'	9.3.1	o	
1.5	SW = '6F XX'	9.3.1	m	
1.6	SW = '6B XX'	9.3.1	o	
1.7	SW = '67 XX'	9.3.1	o	
1.8	SW = '90 00'	9.3.1	m	
2	DIVERSIFY KEYS	9.3.1	m	
2.1	SW = '98 AD'	9.3.1	c14_2	
2.2	SW = '94 00'	9.3.1	o	
2.3	SW = '94 08'	9.3.1	o	
2.4	SW = '6E XX'	9.3.1	o	
2.5	SW = '6D XX'	9.3.1	o	
2.6	SW = '6F XX'	9.3.1	m	
2.7	SW = '6B XX'	9.3.1	o	
2.8	SW = '67 XX'	9.3.1	o	
2.9	SW = '90 00'	9.3.1	m	
3	ASK PARAMETER	9.3.1	m	
3.1	SW = '98 AD'	9.3.1	c14_2	
3.2	SW = '94 02'	9.3.1	o	
3.3	SW = '6E XX'	9.3.1	o	
3.4	SW = '6D XX'	9.3.1	o	
3.5	SW = '6F XX'	9.3.1	m	
3.6	SW = '6B XX'	9.3.1	o	
3.7	SW = '67 XX'	9.3.1	o	
3.8	SW = '90 00'	9.3.1	m	
4	COMPUTE CRYPTOGRAM	9.3.1	o	
4.1	SW = '98 AD'	9.3.1	c:c14_2	
4.2	SW = '98 35'	9.3.1	c:o	
4.3	SW = '6E XX'	9.3.1	c:o	
4.4	SW = '6D XX'	9.3.1	c:o	
4.5	SW = '6F XX'	9.3.1	c:m	

4.6	SW = '6B XX'	9.3.1	c:o	
4.7	SW = '67 XX'	9.3.1	c:o	
4.8	SW = '90 00'	9.3.1	c:m	
4.9	SW = '9F XX'	9.3.1	c:c14_1	
5	VERIFY CRYPTOGRAM	9.3.1	o	
5.1	SW = '98 AD'	9.3.1	c:c14_2	
5.2	SW = '98 04'	9.3.1	c:o	
5.3	SW = '98 35'	9.3.1	c:o	
5.4	SW = '6E XX'	9.3.1	c:o	
5.5	SW = '6D XX'	9.3.1	c:o	
5.6	SW = '6F XX'	9.3.1	c:m	
5.7	SW = '6B XX'	9.3.1	c:o	
5.8	SW = '67 XX'	9.3.1	c:o	
5.9	SW = '90 00'	9.3.1	c:m	
6	COMPUTE MAC	9.3.1	o	
6.1	SW = '98 AD'	9.3.1	c:c14_2	
6.2	SW = '98 35'	9.3.1	c:o	
6.3	SW = '6E XX'	9.3.1	c:o	
6.4	SW = '6D XX'	9.3.1	c:o	
6.5	SW = '6F XX'	9.3.1	c:m	
6.6	SW = '6B XX'	9.3.1	c:o	
6.7	SW = '67 XX'	9.3.1	c:o	
6.8	SW = '90 00'	9.3.1	c:m	
6.9	SW = '9F XX'	9.3.1	c:c14_1	
7	COMPUTE MAC EW	9.3.1	o	
7.1	SW = '98 AD'	9.3.1	c:c14_2	
7.2	SW = '98 35'	9.3.1	c:o	
7.3	SW = '6E XX'	9.3.1	c:o	
7.4	SW = '6D XX'	9.3.1	c:o	
7.5	SW = '6F XX'	9.3.1	c:m	
7.6	SW = '6B XX'	9.3.1	c:o	
7.7	SW = '67 XX'	9.3.1	c:o	
7.8	SW = '90 00'	9.3.1	c:m	
7.9	SW = '9F XX'	9.3.1	c:c14_1	
8	VERIFY MAC	9.3.1	o	
8.1	SW = '98 AD'	9.3.1	c:c14_2	
8.2	SW = '98 04'	9.3.1	c:o	
8.3	SW = '98 35'	9.3.1	c:o	
8.4	SW = '6E XX'	9.3.1	c:o	
8.5	SW = '6D XX'	9.3.1	c:o	
8.6	SW = '6F XX'	9.3.1	c:m	
8.7	SW = '6B XX'	9.3.1	c:o	
8.8	SW = '67 XX'	9.3.1	c:o	
8.9	SW = '90 00'	9.3.1	c:m	
9	UPDATE (SM)	9.3.1	o	
9.1	SW = '98 AD'	9.3.1	c:c14_2	
9.2	SW = '98 04'	9.3.1	c:o	
9.3	SW = '98 35'	9.3.1	c:o	
9.4	SW = '92 0X'	9.3.1	c:o	
9.5	SW = '92 40'	9.3.1	c:o	
9.6	SW = '94 00'	9.3.1	c:o	
9.7	SW = '94 08'	9.3.1	c:o	
9.8	SW = '6E XX'	9.3.1	c:o	
9.9	SW = '6D XX'	9.3.1	c:o	
9.10	SW = '6F XX'	9.3.1	c:m	
9.11	SW = '6B XX'	9.3.1	c:o	
9.12	SW = '67 XX'	9.3.1	c:o	
9.13	SW = '90 00'	9.3.1	c:m	

10	INCREASE (SM)	9.3.1	o	
10.1	SW = '98 AD'	9.3.1	c14_2	
10.2	SW = '98 04'	9.3.1	c:o	
10.3	SW = '98 35'	9.3.1	c:o	
10.4	SW = '92 40'	9.3.1	c:o	
10.5	SW = '94 00'	9.3.1	c:o	
10.6	SW = '94 08'	9.3.1	c:o	
10.7	SW = '6E XX'	9.3.1	c:o	
10.8	SW = '6D XX'	9.3.1	c:o	
10.9	SW = '6F XX'	9.3.1	c:m	
10.10	SW = '6B XX'	9.3.1	c:o	
10.11	SW = '67 XX'	9.3.1	c:o	
10.12	SW = '90 00'	9.3.1	c:m	
10.13	SW = '9F XX'	9.3.1	c:c14_1	
11	DECREASE (SM)	9.3.1	o	
11.1	SW = '98 AD'	9.3.1	c14_2	
11.2	SW = '98 35'	9.3.1	c:o	
11.3	SW = '92 40'	9.3.1	c:o	
11.4	SW = '94 00'	9.3.1	c:o	
11.5	SW = '94 08'	9.3.1	c:o	
11.6	SW = '6E XX'	9.3.1	c:o	
11.7	SW = '6D XX'	9.3.1	c:o	
11.8	SW = '6F XX'	9.3.1	c:m	
11.9	SW = '6B XX'	9.3.1	c:o	
11.10	SW = '67 XX'	9.3.1	c:o	
11.11	SW = '90 00'	9.3.1	c:m	
11.12	SW = '9F XX'	9.3.1	c:c14_1	
12	COMPUTE LOAD KEY	9.3.1	c10_1	
12.1	SW = '98 AD'	9.3.1	c:c14_2	
12.2	SW = '98 35'	9.3.1	c:o	
12.3	SW = '6E XX'	9.3.1	c:o	
12.4	SW = '6D XX'	9.3.1	c:o	
12.5	SW = '6F XX'	9.3.1	c:m	
12.6	SW = '6B XX'	9.3.1	c:o	
12.7	SW = '67 XX'	9.3.1	c:o	
12.8	SW = '90 00'	9.3.1	c:m	
12.9	SW = '9F XX'	9.3.1	c:c14_1	

c14_1: IF A.2/2 THEN o -- T=0 protocol is supported
c14_2: IF A.6/1 THEN o -- sequence control is implemented

Comments:

A.5.6.2 Status word coding

Table A.15: Coding

Item	Coding	Reference	Status	Support
1	AC (CHV, MAC, Cryptogram) not fulfilled = '9804'	9.3.1.1	m	
2	No ASK PARAMETER/GIVE RANDOM before = '9835'	9.3.1.1	m	
3	Command out of sequence = '98AD'	9.3.1.1	c14_2	
4	Update successful, after X retries = '920X'	9.3.1.2	m	
5	Update impossible = '9240'	9.3.1.2	m	
6	No EF selected = '9400'	9.3.1.3	m	
7	Out of range = '9402'	9.3.1.3	m	
8	File ID not found = '9404'	9.3.1.3	m	
9	File type inconsistent = '9408'	9.3.1.3	m	
10	Wrong CLA given = '6EXX'	9.3.1.4	m	
11	Wrong INS given = '6DXX'	9.3.1.4	m	

12	Command aborted = '6FXX'	9.3.1.4	m	
13	Incorrect parameter P1, P2 = '6BXX'	9.3.1.4	m	
14	Incorrect parameter P3 = '67XX'	9.3.1.4	m	
15	Normal ending = '9000'	9.3.1.5	m	
16	Length 'XX' of response data = '9FXX'	9.3.1.5	c14_1	

Comments:

A.5.7 Contents of the elementary files

Prerequisite: A.1/1 is supported (SM is an IC Card).

A.5.7.1 Contents of the EFs

Table A.16: File requirements

Item	EF	Reference	Status	Support
1	Masterfile according to ISO/IEC 7816-4 [6]	A.4.1	m	
2	EF_{ICC} according to TS 101 200-3 [7] subclause 10.4, for the support of optional data elements refer to ICS for EN 726-3 (TS 101 203-1[9])	A.4.2	m	
3	EF_{DIR} according to TS 101 200-3 [7] subclause 6.3	A.4.3	o	
4	EF_{KEY_MAN} (SM) according to TS 101 200-3 [7] subclause 10.6	A.4.4	m	
5	EF_{KEY_OP} (SM) according to TS 101 200-3 [7] subclause 10.7	A.4.5	o	
6	DFx according to TS 101 200-3 [7] subclause 9.2.3	A.4.6	m (note)	
7	EF_{KEY_MAN} (UC)X	A.4.7	o	
7.1	Unavailable Master keys are coded with AlgoId of 'FF'	A.4.7	m	
8	EF_{KEY_OP} (UC)X	A.4.7	m	
8.1	The structure is the mirror of the relevant EF_{KEY} of the UC	A.4.7	m	
8.2	Unavailable Master keys are coded with AlgoId of 'FF'	A.4.7	m	
9	$EF_{KEYTABLE}$	A.4.8	m	
9.1	One $EF_{KEYTABLE}$ per EF_{DIK}	A.4.8	m	
9.2	Only the relevant key is allowed for the linked functions	A.4.8	m	
10	EF_{AMOUNT} (SM)	A.4.9	o	
11	EF_{DIK_MAN} (UC)	A.4.10	o	
11.1	Unavailable Master keys are coded with AlgoId of 'FF'	A.4.10	m	
12	EF_{DIK_OP} (UC)	A.4.10	m	
12.1	The structure is the mirror of the relevant EF_{KEY} of the UC	A.4.10	m	
12.2	Unavailable Master keys are coded with AlgoId of 'FF'	A.4.10	m	
NOTE: At least one DF is mandatory.				

Comments:

A.5.8 Description of the commands

Prerequisite: A.1/1 is supported (SM is an IC card).

A.5.8.1 Mapping principle

NOTE: If the SM is not an IC card additional information is needed to fulfil A.7.

Table A.17: APDU mapping principles and parameters

Item	APDU format/parameter	Reference	Status	Support
1	The command header consists of the CLA, INS, P1, P2 and Lc elements	A.5.1	m	
2	The command trailer consists of the Le element	A.5.1	m	
3	CLA coded as defined in TS 101 200-3 [7] subclause 9.2	A.5.2	m	

Comments:

A.5.8.2 Coding of the commands

If conformance with one of the commands is declared, that requires implicitly that the command is coded according to the standard.

Table A.18: Coding of the commands

Item	Command	Reference	Status	Support
1	SELECT KEYSET	A.5.2.1	m	
1.1	Support of KEYSET in MF	A.5.2.1, A.3	o	
1.2	Support of KEYSET in DF	A.5.2.1, A.3	m	
2	DIVERSIFY KEYSET	A.5.2.2	m	
2.1	2 sets of EF_{DIK}	A.7	c10_1	
3	ASK PARAMETER	A.5.3.1	m	
3.1	Multiple counters	A.5.3.1	o.2	
3.2	Single counter with back tracking mechanism	A.5.3.1	o.2	
4	COMPUTE LOAD KEY	A.5.4.1	o	
4.1	2 sets of EF_{DIK}	A.7	c:c10_1	
5	COMPUTE MAC	A.5.4.2	o	
6	COMPUTE CRYPTOGRAM	A.5.4.3	o	
7	VERIFY MAC	A.5.5.1	o	
8	UPDATE (SM)	A.5.5.2	o	
9	VERIFY CRYPTOGRAM	A.5.5.3	o	
10	INCREASE (SM)	A.5.6.1, 6	o	
11	DECREASE (SM)	A.5.6.2, 6	o	
12	COMPUTE MAC EW	A.5.4.4	o	

o.2: Only one of these options shall be selected.

Comments:

A.5.9 Downloading of keys from SM to UC

Table A.19: Functions for downloading of keys

Item	Functions	Reference	Status	Support
1	Loading of keys in an empty EF_{KEY_MAN} of the UC	A.7.1	c2_2	
2	Changing of already existing keys in the EF_{KEY_MAN} of the UC	A.7.2	c2_2	
3	Changing of already existing keys in the EF_{KEY_OP} of the UC	A.7.3	c2_2	

Comments:

Annex B (informative): Bibliography

- EN 27811-1 (1989): "Identification cards - Recording technique - Part 1: Embossing".
- EN 27811-3 (1989): "Identification cards - Recording technique - Part 3: Location of embossed character on ID-1 cards".
- ISO/IEC 10202: "Financial Transaction cards: Security Architecture of financial transaction systems using Integrated Circuit Cards - Part 4: Secure Application Module".

History

Document history		
V1.1.1	July 1997	Publication

ISBN 2-7437-1351-8
Dépôt légal : Juillet 1997