TS 101 203-1 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 1: Implementation Conformance Statement (ICS) proforma specification

European Telecommunications Standards Institute

Reference
DTS/PTS-00203-1 (b5090icr.PDF)

Keywords
Card, ICS, testing

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 1 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

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 ICS proforma for *Application independent card requirements* defined in EN 726-3 [1] in compliance with the relevant requirements, and in accordance with the relevant guidance given in ISO/IEC 9646-7 [4] and ETS 300 406 [2].

The supplier of an implementation which is claimed to conform to the present document is required to complete a copy of the ICS proforma provided in annex A 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] 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] ETS 300 406 (April 1995): "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

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

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

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

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

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

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

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

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

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

3 Definitions, symbols and abbreviations

3.1 Definitions

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

- terms defined in TS 101 200-3 [1];
- terms defined in ISO/IEC 9646-1 [3] and in ISO/IEC 9646-7 [4].

In particular, the following terms defined in ISO/IEC 9646-1 [3] 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, as a questionnaire, which when completed for an implementation or system becomes an ICS.

3.2 Symbols

3.2.1 Matrix status and support indication

For the purposes of the present document, the following deviating notation applies:

Item	Function	X	Y	Z
1	A	O		
2	B		O	O
3	C			

The meaning of the cells containing circles is that the combinations indicated by these cells (A-X, B-Y, and B-Z) should be supported. Cells that **do not** contain a circle express a combination that **should not** be supported.

To indicate the support of a combination that is not circled, the corresponding empty cell shall be marked with the symbol: √.

To indicate the absence of support for a mandatory combination, the corresponding circled cell shall be marked with the symbol: ×.

3.2.2 Hexadecimal value notation

For the purposes of the present document, hexadecimal values are enclosed in single quotes, while decimal values are not. A single hexadecimal digit within quotes represents a nibble (4 bits) while two hexadecimal digits within quotes represents a byte (8 bits), e.g. value "12" is a hexadecimal value representing the decimal value 18.

3.3 Abbreviations

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

AC	Access Condition(s)
ALW	ALWays
APDU	Application Protocol Data Unit
ASC	Application Specific Command set
ATC	Abstract Test Case
ATR	Answer To Reset
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
EF_{KEY_MAN}	Elementary File containing management keys
EF_{KEY_OP}	Elementary File containing operational keys
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)
NEV	NEVer
PC	Physical Characteristics
PDU	Protocol Data Unit
PRO	PROtected
RC	Return Code
RFU	Reserved for Future Use
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 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 that conforms to the present document shall:

1) describe an implementation which claims to conform to TS 101 200-3 [1];

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 "Application independent card requirements" (TS 101 200-3)

A.1 Guidance for completing the ICS proforma

A.1.1 Purposes and structure

The purpose of this ICS proforma is to provide a mechanism whereby a supplier of an implementation of the requirements defined in TS 101 200-3 [1] 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 standard
- A.4 Global statement of conformance
- A.5 Capabilities of IC card
  - A.5.1 Physical characteristics
    - A.5.1.1 Format and layout
      - A.5.1.1.1 European application
  - A.5.2 Electronic signals and transmission protocols
  - A.5.3 Logical model
    - A.5.3.1 File identifier
    - A.5.3.2 Elementary files
      - A.5.3.2.1 File restrictions
    - A.5.3.3 Methods for selecting a file
    - A.5.3.4 Invalidation and rehabilitation
  - A.5.4 Security facilities
    - A.5.4.1 File access control
    - A.5.4.2 Keyfile requirements
    - A.5.4.3 CHV file requirements
    - A.5.4.4 Functions versus file access
    - A.5.4.5 Setting of access conditions at file creation
    - A.5.4.6 Security versus access conditions
    - A.5.4.7 Algorithms
  - A.5.5 Description of the functions
  - A.5.6 Description of the commands
    - A.5.6.1 Mapping principles
    - A.5.6.2 General data coding
    - A.5.6.3 Coding of the commands
    - A.5.6.4 Command fields
      - A.5.6.4.1 Types of SELECT
      - A.5.6.4.2 Types of CREATE FILE
      - A.5.6.4.3 Types of EXTEND
      - A.5.6.4.4 Mode of UPDATE RECORD
      - A.5.6.4.5 Mode of READ RECORD
      - A.5.6.4.6 Mode of READ RECORD STAMPED
      - A.5.6.4.7 Type of SEEK
      - A.5.6.4.8 Mode of DECREASE STAMPED
      - A.5.6.4.9 Mode of INCREASE STAMPED

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 [4].

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 (i.e., elements, timers, etc.). It implicitly means "is <item description> supported by the implementation?".

Status column

The following notations, defined in ISO/IEC 9646-7 [4], 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	conditional - the requirement on the capability ("m", "o", "x" or "n/a") depends on the support of other optional or conditional items. "i" is an integer identifying an unique conditional status expression 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 which 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 column gives reference to TS 101 200-3 [1], except where explicitly 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 [4], 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.

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 standard

This ICS proforma applies to the following standard:

TS 101 200-3 [1]: "Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 3: Application independent card requirements".

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 specification. 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 Capabilities of IC card

This subclause contains the ICS proforma tables related to the application independent card requirements.

NOTE: The TS 101 200-3 [1] defines a number of card characteristics including the presence of a number of files. Therefore a card can only conform to the EN 726-3 [1] after an initialization phase which stores the data related to these files on the card.

A.5.1 Physical characteristics

Table A.1: General physical requirements

Item	Physical characteristic	Reference	Status	Support
1	ID-1 card	4	o.1	
1.1	Physical characteristics in accordance with EN 27816-1,2 [8,9]	4	c:m	
2	Format according to ENV 1375-1,2 [5,6]	4	o.1	
3	Temperature range -25°C to +65°C with occasional peaks up to +70°C	4.2	o.2	
4	Temperature range -25°C to +70°C with occasional peaks up to +85°C, if multi-application card suitable for application in portable equipment	4.2	o.2	

o.1: It is mandatory to support exactly one of these items.
o.2: It is mandatory to support exactly one of these items.

Comments:

A.5.1.1 Format and layout

Table A.2: Area of application

Item	Area	Reference	Status	Support
1	Card to be used in Europe	4.1	o	

A.5.1.1.1 European application

Prerequisite: A.1/1 AND A.2/1 -- ID-1 card and European card

Table A.3: European card

Item	Physical characteristic	Reference	Status	Support
1	Identification number on the card	4.1	o	
2	Card sequence number on the card	4.1	o	
3	Contacts available	4.1	m	
4	Embossing	4.1	o	
4.1	Embossing on same side as contacts	4.1	c:m	
4.2	Number format and layout in accordance with EN 27811 [7]	4.1	c:c3_1	
5	Magnetic stripe	4.1	o	
5.1	Magnetic track on opposite side of contacts	4.1	c:m	

c3_1: IF A.3/1 OR A.3/2 THEN m ELSE n/a -- Identification or Card sequence number

Comments:

A.5.2 Electronic signals and transmission protocols

Table A.4: Electronic signals and transmission protocols

Item	Capability	Reference	Status	Support
1	Electronic signals and transmission protocols in accordance with EN 27816-3 [10], with exception of requirements below	5	m	
2	Supply voltage of 5V ± 10 % is accepted	5.1	m	
3	Supply current equal to or less than 20 mA (excluding spikes).	5.2	m	
4	Card can be used in mobile equipment	5.2	o	
4.1	Supply current equal to or less than 10 mA (excluding spikes).	5.2	c:m	
5	Current spikes always below 40 nAs, 400 ns and 200mA	5.2	m	
6	Programming voltage other than supply voltage	5.3	o	
6.1	Internal generation of programming voltage	5.3	c:m	
7	Duty cycle for asynchronous operation in between 40 % and 60 %	5.4	m	
8	T = 0 protocol	5.5	o.3	
8.1	Extra character guard time indication from terminal to card (TC1 parameter N in ATR) equals 0 or 4	5.5	c:m	
9	T = 1 protocol	5.5	o.3	
9.1	Extra character guard time indication from terminal to card (TC1 parameter N in ATR) equals 0, 4 or 255	5.5	c:m	
10	Low power consumption mode	5.6	o	
10.1	Low power consumption mode indicated in EF_{ICC}	5.6	c:m	

o.3: It is mandatory to support at least one of these items.

Comments:

A.5.3 Logical model

A.5.3.1 File identifier

Table A.5: File identifier

Item	File ID characteristic	Reference	Status	Support
1	File ID is extracted from the CREATE FILE command (note)	6.1	c5_1	
2	Two files under the same parent never have the same ID	6.1	m	

c5_1: IF A.23/3 THEN m ELSE n/a -- CREATE FILE command supported

Comments:

NOTE: The intention of this requirement is to assure that the file ID is chosen by the command issuer, not by the card.

A.5.3.2 Elementary files

Table A.6: File structures

Item	EF type	Reference	Status	Support
1	Transparent EF	6.2.1	m	
1.1	Transparent EFs containing programs	6.2.2	c:o	
2	Linear fixed EF	6.2.3	o	
3	Linear variable EF	6.2.4	o	
4	Cyclic EF	6.2.5	o	
5	EFs containing ASC-set	6.2.6	o	

Comments:

A.5.3.2.1 File restrictions

Table A.7: File restrictions

Item	Restriction	Reference	Status	Support
1	First record defined as record #1	6.2.3,4,5	c7_1	
2	Only oldest record is changed for writing operations (including increase and decrease)	6.2.5	c7_2	
3	Updated record becomes record #1 after increase or decrease operation	6.2.5	c7_2	
4	For writing operation the only way of addressing a record is PREVIOUS	6.2.5	c7_2	
5	Record pointer is set to last written record (#1) after selection of EF	6.2.5	c7_2	
6	Only one ASC-set can be associated to a DF	6.2.6	c7_3	

c7_1: IF A.6/2 OR A.6/3 OR A.6/4 THEN m ELSE n/a -- linear or cyclic EF
c7_2: IF A.6/4 THEN m ELSE n/a -- cyclic EF
c7_3: IF A.6/5 THEN m ELSE n/a -- EFs containing ASC-set

Comments:

A.5.3.3 Methods for selecting a file

Table A.8: Usage of channel mechanism

Item	Method	Reference	Status	Support
1	Channel mechanism supported	6.4	o	
1.1	Remember context for channels	6.4	c:m	
1.2	Exclusive select for files	6.4	c:m	

Comments:

A.5.3.4 Invalidation and rehabilitation

Table A.9: Invalidation and rehabilitation

Item	File ID	Reference	Status	Support
1	Invalidation and rehabilitation supported	6.6	o	
1.1	Availability of functions after invalidation limited to (if functions are supported at all) SELECT, STATUS, DELETE, REHABILITATE, and READ (if file status allows it)	6.6	c:m	

Comments:

A.5.4 Security facilities

A.5.4.1 File access control

The following table contains all access conditions and combinations of them. Supporting any of these automatically implies a support of the relevant security procedure as defined in clause 7 of TS 101 200-3 [1].

Table A.10: File access conditions and combinations

Item	Access condition	Reference	Status	Support
1	ALW (always)	7.1.1, 9.3	m	
1.1	coded as hex "0"	9.3	m	
2	CHV1 (card holder verification)	7.1.1	o	
2.1	coded as hex "1"	9.3	c:m	
3	CHV2 (card holder verification)	7.1.1	o	
3.1	coded as hex "2"	9.3	c:m	
4	PRO (protected)	7.1.1	o	
4.1	coded as hex "3"	9.3	c:m	
5	AUT (authenticated)	7.1.1	o	
5.1	coded as hex "4"	9.3	c:m	
6	CHV1 and PRO	7.1.1	o	
6.1	coded as hex "6"	9.3	c:m	
7	CHV2 and PRO	7.1.1	o	
7.1	coded as hex "7"	9.3	c:m	
8	CHV1 and AUT	7.1.1	o	
8.1	coded as hex "8"	9.3	c:m	
9	CHV2 and AUT	7.1.1	o	
9.1	coded as hex "9"	9.3	c:m	
10	NEV (never)	7.1.1, 9.3	m	
10.1	coded as hex "F"	9.3	m	
NOTE: Access conditions ALW and NEV are mandatory as there are mandatory EFs defined that use these conditions.				

Comments:

A.5.4.2 Keyfile requirements

This subclause applies to any EF_{KEY_MAN} or EF_{KEY_OP}.

Table A.11: Keyfile requirements

Item	Keyfile requirement	Reference	Status	Support
1	Keyfiles store a version number	7.1.2	m	
2	keys are stored together with keylength and algorithm ID	7.1.2	m	
3	After creation of an EF_{KEY_MAN} this file is empty indicated by keylength 0 for the first key.	7.1.2	m	
4	An EF_{KEY_OP} can be created or modified by usage of a key for the relevant EF_{KEY_MAN}.	7.1.2	m	
5	Any EF_{KEY_OP} can be invalidated	7.1.2	c11_1	
6	A higher level EF_{KEY_OP} is used when not existing on current level.	7.1.2	m	
7	A higher level EF_{KEY_OP} is used when invalidated on current level.	7.1.2	c11_1	

c11_1: IF A.23/20 THEN m ELSE n/a -- INVALIDATE command supported

Comments:

A.5.4.3 CHV file requirements

Prerequisite: A.10/2 OR A.10/3 -- Access condition CHV1 or CHV2 supported

Table A.12: CHV file requirements

Item	CHV file requirement	Reference	Status	Support
1	CHV storage	7.1.1	m	
1.1	CHVs stored in EF_{CHV}	7.1.1	o.4	
1.2	Path to CHVs stored in EF_{CHV}	7.1.1	o.4	
2	CHV attempts counter	7.1.3	m	
2.1	CHV attempts counter decrements at incorrect CHV evaluation	7.1.3	m	
2.2	CHV attempts counter reset after correct CHV evaluation	7.1.3	m	
2.3	CHV mechanism blocked when attempts counter reaches zero	7.1.3	m	
3	CHV UNBLOCK attempts counter	7.1.3	m	
3.1	UNBLOCK CHV attempts counter decrements at incorrect UNBLOCK CHV evaluation	7.1.3	m	
3.2	UNBLOCK CHV mechanism blocked when UNBLOCK attempts counter reaches zero	7.1.3	m	
3.3	UNBLOCK CHV attempts counter reset after correct UNBLOCK CHV evaluation	7.1.3	m	
4	CHV UNBLOCK successful usage counter	7.1.3	m	
4.1	UNBLOCK CHV mechanism blocked when successful usage counter reaches zero	7.1.3	m	
4.2	UNBLOCK CHV mechanism cannot be reset when the successful usage counter reached zero.	7.1.3	m	
5	CHV presentation to the card	7.1.3	m	
5.1	Not enciphered	7.1.3	o.5	
5.2	Enciphered.	7.1.3	o.5	

o.4: It is mandatory to support at least one of these items.
o.5: It is mandatory to support at least one of these items.

Comments:

A.5.4.4 Functions versus file access

The TS 101 200-3 [1] defines in subclauses 7.1.4 and 7.2 relations between functions, access conditions and types of files. The table below lists these relationships in general terms. A support for any item automatically expresses conformance to the detailed descriptions in the respective clauses. Any deviation from that should be commented below the table.

Table A.13: Functions versus file access

Item	Relation	Reference	Status	Support
1	Application of functions to files is controlled by access conditions that are set per file for each (group of) function(s) as defined in TS 101 200-3 [1]	7.1.4	m	
2	Application of functions to files is depending on the type of file	7.1.4, table 4	m	
2.1	Application of functions to MF as defined in TS 101 200-3 [1]	7.1.4, table 4	m	
2.2	Application of functions to DF as defined in TS 101 200-3 [1]	7.1.4, table 4	m	
2.3	Application of functions to keyfiles as defined in TS 101 200-3 [1]	7.1.4, table 4	m	
2.4	Application of functions to EF_{CHV} as defined in TS 101 200-3 [1]	7.1.4, table 4	m	
2.5	Application of functions to other EFs as defined in TS 101 200-3 [1]	7.1.4, table 4	m	
2.5.1	Application of functions to EF of linear fixed structure as defined in TS 101 200-3 [1]	7.2, table 5	m	
2.5.2	Application of functions to EF of linear variable structure as defined in TS 101 200-3 [1]	7.2, table 5	m	
2.5.3	Application of functions to transparent EF as defined in TS 101 200-3 [1]	7.2, table 5	m	
2.5.4	Application of functions to cyclic EF as defined in TS 101 200-3 [1]	7.2, table 5	m	

Comments:

A.5.4.5 Setting of access conditions at file creation

The TS 101 200-3 [1] defines in clause 9.3 the way how combinations between access conditions and functions can be supported at file creation. The following tables indicate these combinations for various type of files. If a combination is supported then the coding of the CREATE FILE command shall be according to the TS 101 200-3 [1].

Table A.14: Access conditions for EF creation (excluding keyfiles)

Item	Combination	Reference	Status	Support
1	Selection of functions UPDATE and WRITE (byte 8; bit 7 & 8: 00)	9.3.1	o.6	
2	Selection of functions UPDATE and INCREASE (byte 8; bit 7 & 8: 01)	9.3.1	o.6	
3	Selection of functions DECREASE and WRITE (byte 8; bit 7 & 8: 10)	9.3.1	o.6	
4	Selection of functions DECREASE and INCREASE (byte 8; bit 7 & 8: 11)	9.3.1	o.6	
5	AC for READ/SEEK functions (byte 9; bit 5-8)	9.3.1	o	
6	AC for UPDATE/DECREASE functions (byte 9; bit 1-4)	9.3.1	o	
7	AC for WRITE/INCREASE functions (byte 10; bit 5-8)	9.3.1	o	
8	AC for CREATE RECORD/EXECUTE functions (byte 10; bit 1-4)	9.3.1	o	
9	AC for REHABILITATE function (byte 11; bit 5-8)	9.3.1	o	
10	AC for INVALIDATE function (byte 11; bit 1-4)	9.3.1	o	
11	Keynumber for READ/SEEK functions (byte 14; bit 5-8)	9.3.1	o	
12	Keynumber for UPDATE/DECREASE functions (byte 14; bit 1-4)	9.3.1	o	
13	Keynumber for WRITE/INCREASE functions (byte 15; bit 5-8)	9.3.1	o	
14	Keynumber for CREATE RECORD/EXECUTE functions (byte 15; bit 1-4)	9.3.1	o	
15	Keynumber for REHABILITATE function (byte 16; bit 5-8)	9.3.1	o	
16	Keynumber for INVALIDATE function (byte 16; bit 1-4)	9.3.1	o	

o.6: It is mandatory to support at least one of these items.

Comments:

Table A.15: Access conditions for DF creation

Item	Combination	Reference	Status	Support
1	CHV1 to be verified before INTERNAL AUTHENTICATION	9.3.2	o.7	
2	CHV1 need not to be verified before INTERNAL AUTHENTICATION	9.3.2	o.7	
3	AC for DELETE function (byte 10; bit 5-8)	9.3.2	o	
4	AC for CREATE/EXTEND FILE functions (byte 10; bit 1-4)	9.3.2	o	
5	AC for REHABILITATE function (byte 11; bit 5-8)	9.3.2	o	
6	AC for INVALIDATE function (byte 11; bit 1-4)	9.3.2	o	
7	Keynumber for DELETE function (byte 15; bit 5-8)	9.3.2	o	
8	Keynumber for CREATE/EXTEND FILE functions (byte 15; bit 1-4)	9.3.2	o	
9	Keynumber for REHABILITATE function (byte 16; bit 5-8)	9.3.2	o	
10	Keynumber for INVALIDATE function (byte 16; bit 1-4)	9.3.2	o	

o.7: It is mandatory to support at least one of these items.

Comments:

Table A.16: Access conditions for keyfile creation (EF_{KEY_MAN} or EF_{KEY_OP})

Item	Combination	Reference	Status	Support
1	AC for LOAD KEY FILE function (byte 9; bit 5-8)	9.3.3	o	
2	AC for UPDATE function (byte 9; bit 1-4)	9.3.3	o	
3	AC for REHABILITATE function (byte 11; bit 5-8)	9.3.3	o	
4	AC for INVALIDATE function (byte 11; bit 1-4)	9.3.3	o	
5	Keynumber for LOAD KEY FILE function (byte 14; bit 5-8)	9.3.3	o	
6	Keynumber for UPDATE function (byte 14; bit 1-4)	9.3.3	o	
7	Keynumber for REHABILITATE function (byte 16; bit 5-8)	9.3.3	o	
8	Keynumber for INVALIDATE function (byte 16; bit 1-4)	9.3.3	o	

Comments:

A.5.4.6 Security versus access conditions

Table A.17: Security and access conditions

Item	Relation	Reference	Status	Support
1	Fulfilment of access conditions CHV and AUT is remembered until end of application/session	7.5	m	
2	For AC = PRO cryptogram expected at end of command	7.6.1	c17_1	
2.1	Cryptogram expected to contain input of random, header (INS, P1, P2, Lc) and data	7.6.1	c:m	
2.2	Command accepted and executed only when cryptogram correct	7.6.1	c:m	
3	Cryptogram returned in STAMPED functions.	7.6.2	m	
3.1	Cryptogram input depending on MODE	7.6.2	o	
4	For AC = AUT cryptogram expected during authentication	7.6.3	c17_2	
4.1	Key and cryptogram taken from relevant keyfile.	7.6.3	c:m	
5	Cryptogram returned for internal authentication	7.6.3	c17_3	
5.1	Key and cryptogram taken from relevant keyfile.	7.6.3	c:m	

c17_1: IF A.10.4 OR A.10.6 OR A.10.7 THEN m ELSE n/a -- AC PRO (with or without CHV) supported
c17_2: IF A.10.5 OR A.10.8 OR A.10.9 THEN m ELSE n/a -- AC AUT (with or without CHV) supported
c17_3: IF A.19.22 THEN m ELSE n/a -- INTERNAL AUTHENTICATION supported

Comments:

A.5.4.7 Algorithms

The TS 101 200-3 [1] lists a number of security algorithms. For these algorithms identifiers have been reserved that should be used to identify them. The support of any of these algorithms automatically implies the support of its application to security facilities (authentication, protected, stamped, key load) as defined in subclause 7.6.5 of the TS 101 200-3 [1]. However the use of other non-proprietary algorithms is not restricted. If any of such algorithms are supported it shall be marked under item 6 "Other". Additionally the name(s), ID(s) and security facilities of these algorithms shall be indicated in the comments field below the table.

Table A.18: Algorithms and IDs

Item	Algorithm and IDs	Reference	Status	Support
1	DSAA	7.6.5	o	
1.1	ID = "1"	7.6.5	c:m	
2	COMP NAT	7.6.5	o	
2.1	ID = "2"	7.6.5	c:m	
3	USA4	7.6.5	o	
3.1	ID = "3"	7.6.5	c:m	
4	TESA-7	7.6.5	o	
4.1	ID = "4"	7.6.5	c:m	
5	COMP 128	7.6.5	o	
5.1	ID = "40"	7.6.5	c:m	
6	Proprietary	7.6.5	o	
6.1	ID = "70" - "7F"	7.6.5	c:m	
7	Other	7.6.5	o	

Comments:

A.5.5 Description of the functions

The following table contains all functions. Supporting any of these automatically implies a support of the relevant application procedures and constraints as defined in clause 8 of TS 101 200-3 [1]. The support of any function can be dependent on the chosen profile as defined in table A.38 of the present document.

Table A.19: Functions

Item	Function	Reference	Status	Support
1	SELECT	8.1	m	
2	STATUS	8.2	o	
3	CREATE FILE	8.3	o	
4	DELETE FILE	8.4	o	
5	EXTEND	8.5	o	
6	EXECUTE	8.6	o	
7	UPDATE BINARY	8.7	o	
8	UPDATE RECORD	8.8	o	
9	CREATE RECORD	8.9	o	
10	READ BINARY	8.10	m	
11	READ BINARY STAMPED	8.11	o	
12	READ RECORD	8.12	o	
13	READ RECORD STAMPED	8.13	o	
14	SEEK	8.14	o	
15	VERIFY CHV	8.15	o	
16	CHANGE CHV	8.16	o	
17	DISABLE CHV	8.17	o	
18	ENABLE CHV	8.18	o	
19	UNBLOCK CHV	8.19	o	
20	INVALIDATE	8.20	o	
21	REHABILITATE	8.21	o	
22	INTERNAL AUTHENTICATION	8.22	o	
23	ASK RANDOM	8.23	o	
24	GIVE RANDOM	8.24	o	
25	EXTERNAL AUTHENTICATION	8.25	o	
26	CLOSE APPLICATION	8.26	o	
27	WRITE BINARY	8.27	o	
28	WRITE RECORD	8.28	o	
29	LOCK	8.29	o	
30	DECREASE	8.30	o	
31	DECREASE STAMPED	8.31	o	
32	INCREASE	8.32	o	
33	INCREASE STAMPED	8.33	o	
34	LOAD KEYFILE	8.34	o	
NOTE: The functions SELECT and READ BINARY are considered mandatory in order to allow access to the mandatory files.				

Comments:

A.5.6 Description of the commands

A.5.6.1 Mapping principles

Table A.20: APDU mapping principles and parameters

Item	APDU format/parameter	Reference	Status	Support
1	Command APDU according to ISO 7816-4 [11]	9.1.1	m	
2	Response APDU according to ISO 7816-4 [11]	9.1.2	m	
3	CLA in the range A0-A3	9.2	m	

Comments:

Table A.21: Class byte coding

Item	class byte	Reference	Allowed values	Supported values
1	Class byte value	9.2	"00"-"FF" (note 1)	(note 2)

Comments:

NOTE 1: For telecommunication purposes class byte values in the range "A0" - "A3" are preferred.

NOTE 2: A range can be indicated in case multiple values are supported.

A.5.6.2 General data coding

Table A.22: General coding of data in commands

Item	data	Reference	Status	Support
1	RFU bytes and bits set to 0 unless specified otherwise.	9.2	m	
2	Data fields left justified and padded with 1s.	9.2	m	

Comments:

A.5.6.3 Coding of the commands

The following table contains the commands that correspond to the functions declared before. Supporting any of these automatically implies a support of the coding of the command and its fields (including instruction code) and data field as defined in clause 9 of TS 101 200-3 [1].

Table A.23: Coding of the commands

Item	Command	Reference	Status	Support
1	SELECT	9.2.1	m	
2	STATUS	9.2.2	o	
3	CREATE FILE	9.2.3	o	
4	DELETE FILE	9.2.4	o	
5	EXTEND	9.2.5	o	
6	EXECUTE	9.2.6	o	
7	UPDATE BINARY	9.2.7	o	
8	UPDATE RECORD	9.2.8	o	
9	CREATE RECORD	9.2.9	o	
10	READ BINARY	9.2.10	m	
11	READ BINARY STAMPED	9.2.11	o	
12	READ RECORD	9.2.12	o	
13	READ RECORD STAMPED	9.2.13	o	
14	SEEK	9.2.14	o	
15	VERIFY CHV	9.2.15	o	
16	CHANGE CHV	9.2.16	o	
17	DISABLE CHV	9.2.17	o	
18	ENABLE CHV	9.2.18	o	
19	UNBLOCK CHV	9.2.19	o	
20	INVALIDATE	9.2.20	o	
21	REHABILITATE	9.2.21	o	
22	INTERNAL AUTHENTICATION	9.2.22	o	
23	ASK RANDOM	9.2.23	o	
24	GIVE RANDOM	9.2.24	o	
25	EXTERNAL AUTHENTICATION	9.2.25	o	
26	CLOSE APPLICATION	9.2.26	o	
27	WRITE BINARY	9.2.27	o	
28	WRITE RECORD	9.2.28	o	
29	LOCK	9.2.29	o	
30	DECREASE	9.2.30	o	
31	DECREASE STAMPED	9.2.31	o	
32	INCREASE	9.2.32	o	
33	INCREASE STAMPED	9.2.33	o	
34	LOAD KEYFILE	9.2.34	o	
35	GET RESPONSE	9.2.35	c23_1	
36	ENVELOPE PUT	9.2.36	c23_1	

c23_1: IF A. 4/8 THEN o ELSE n/a -- T = 0 protocol supported

Comments:

A.5.6.4 Command fields

A.5.6.4.1 Types of SELECT

The following table indicates the various types of select. Supporting any of these options implies supporting the coding as defined in subclause 9.2.1 of TS 101 200-3 [1].

Prerequisite: A.23/1 -- SELECT command supported

Table A.24: Type of SELECT

Item	Type	Reference	Status	Support
1	Select by file qualifier	9.2.1	o.8	
2	Select son DF	9.2.1	o.8	
3	Select EF under current DF	9.2.1	o.8	
4	Select parent DF	9.2.1	o.8	
5	Select absolute DF (Application Id)	9.2.1	o.8	
6	Select by path from MF	9.2.1	o.8	
7	Select by path from current DF	9.2.1	o.8	

o.8:It is mandatory to support at least one of these items.

Comments:

A.5.6.4.2 Types of CREATE FILE

The following table indicates the various types of data initialization after file creation. Supporting any of these options implies supporting the coding as defined in subclause 9.2.3 of TS 101 200-3 [1].

Prerequisite: A.23/3 -- CREATE FILE command supported

Table A.25: Type of CREATE FILE

Item	Type	Reference	Status/ allowed value range	Support/ Supported value range
1	Data space initialized with a given one byte value. (P1 = value, P2 bit 1 = 0)	9.2.3	o.9	
1.1	Value range allowed for P1	9.2.3	"00"-"FF"	
2	Data space not initialized. (P1 = 0, P2 bit 1 = 1)	9.2.3	o.9	
3	Data space formatted with records with a given one byte value during creation. (P1 = value, P2 bit 2 = 0)	9.2.3	c25_1	
4	Data space not formatted during creation. (P1 = 0, P2 bit 2 = 1)	9.2.3	c25_1	

o.9:It is mandatory to support at least one of these items.
o.10: It is mandatory to support at least one of these items.
c25_1: IF A. 6/2 OR A. 6/4 THEN o.10 ELSE n/a -- Linear fixed or cyclic structure

Comments:

A.5.6.4.3 Types of EXTEND

The following table indicates the various types of data initialization after file extension. Supporting any of these options implies supporting the coding as defined in subclause 9.2.5 of TS 101 200-3 [1].

Prerequisite: A.23/5 -- EXTEND command supported

Table A.26: Type of EXTEND

Item	Type	Reference	Status/ allowed value range	Support/ Supported value range
1	Data space initialized with a given one byte value. (P1 = value, P2 bit 1 = 0)	9.2.5	o.11	
1.1	Value range allowed for P1	9.2.5	"00"-"FF"	
2	Data space not initialized. (P1 = 0, P2 bit 1 = 1)	9.2.5	o.11	
3	Data space formatted with records with a given one byte value during creation. (P1 = value, P2 bit 2 = 0)	9.2.5	c26_1	
4	Data space not formatted during creation. (P1 = 0, P2 bit 2 = 1)	9.2.5	c26_1	

o.11: It is mandatory to support at least one of these items.
o.12: It is mandatory to support at least one of these items.
c26_1: IF A. 6/2 OR A. 6/4 THEN o.12 ELSE n/a -- Linear fixed or cyclic structure

Comments:

A.5.6.4.4 Mode of UPDATE RECORD

The following table indicates the various types of indicating records in the UPDATE RECORD command. Supporting any of these options implies supporting the coding as defined in subclause 9.2.8 of TS 101 200-3 [1].

Prerequisite: A.23/8 -- UPDATE RECORD command supported

Table A.27: Mode of UPDATE RECORD

Item	Mode	Reference	Status	Support
1	First mode (P2 = "00")	9.2.8	o.13	
2	Last mode(P2 = "01")	9.2.8	o.13	
3	Next mode(P2 = "02")	9.2.8	o.13	
4	Previous mode(P2 = "03")	9.2.8	o.13	
5	Absolute mode(P2 = "04")	9.2.8	o.13	
6	Current mode(P2 = "04", P1 = "00")	9.2.8	o.13	

o.13: It is mandatory to support at least one of these items.

Comments:

A.5.6.4.5 Mode of READ RECORD

The following table indicates the various types of indicating records in the READ RECORD command. Supporting any of these options implies supporting the coding as defined in subclause 9.2.12 of TS 101 200-3 [1].

Prerequisite: A.23/12 -- READ RECORD command supported

Table A.28: Mode of READ RECORD

Item	Mode	Reference	Status	Support
1	First mode (P2 = "00")	9.2.12	o.14	
2	Last mode(P2 = "01")	9.2.12	o.14	
3	Next mode(P2 = "02")	9.2.12	o.14	
4	Previous mode(P2 = "03")	9.2.12	o.14	
5	Absolute mode(P2 = "04")	9.2.12	o.14	
6	Current mode(P2 = "04", P1 = "00")	9.2.12	o.14	
7	Reading to end of file at once by setting field Le = 0	9.2.12	o	

o.14: It is mandatory to support at least one of these items.

Comments:

A.5.6.4.6 Mode of READ RECORD STAMPED

The following table indicates the various types of indicating records in the READ RECORD STAMPED command. Supporting any of these options implies supporting the coding as defined in subclause 9.2.13 of TS 101 200-3 [1].

Prerequisite: A.23/13 -- READ RECORD STAMPED command supported

Table A.29: Mode of READ RECORD STAMPED

Item	Mode	Reference	Status	Support
1	First mode (P2 = "00")	9.2.13	o.15	
2	Last mode(P2 = "01")	9.2.13	o.15	
3	Next mode(P2 = "02")	9.2.13	o.15	
4	Previous mode(P2 = "03")	9.2.13	o.15	
5	Absolute mode(P2 = "04")	9.2.13	o.15	
6	Current mode(P2 = "04", P1 = "00")	9.2.13	o.15	
7	Reading to end of file at once by setting field Le = 0	9.2.12	o	

o.15: It is mandatory to support at least one of these items.

Comments:

A.5.6.4.7 Type of SEEK

The following table indicates the various types of SEEK. Supporting any of these options implies supporting the coding as defined in subclause 9.2.14 of TS 101 200-3 [1].

Prerequisite: A.23/14 -- SEEK command supported

Table A.30: Type of SEEK

Item	Type	Reference	Status	Support
1	Forward from beginning	9.2.14	o.16	
2	Backward from the end	9.2.14	o.16	
3	Forward from next location	9.2.14	o.16	
4	Backward from next location	9.2.14	o.16	
5	No response data returned	9.2.14	o.17	
6	Record number returned as response data	9.2.14	o.17	
7	Seek offset in P1	9.2.14	o	

o.16: It is mandatory to support at least one of these items.
o.17: It is mandatory to support at least one of these items.

Comments:

A.5.6.4.8 Mode of DECREASE STAMPED

The following table indicates the modes for the DECREASE STAMPED command. Supporting any of these options implies supporting the meaning and coding as defined in subclause 9.2.31 of TS 101 200-3 [1].

Prerequisite: A.23/31 -- DECREASE STAMPED command supported

Table A.31: Mode of DECREASE STAMPED

Item	Mode	Reference	Status	Support
1	No header included (P1 = "00")	9.2.31	o.18	
2	Header of DECREASE STAMPED command included (P1 = "01")	9.2.31	o.18	
3	Header of INCREASE STAMPED command included (P1 = "02")	9.2.31	o.18	
4	Header of DECREASE command included (P1 = "03")	9.2.31	o.18	
5	Header of INCREASE command included (P1 = "04")	9.2.31	o.18	

o.18: It is mandatory to support at least one of these items.

Comments:

A.5.6.4.9 Mode of INCREASE STAMPED

The following table indicates the modes for the DECREASE STAMPED command. Supporting any of these options implies supporting the meaning and coding as defined in subclause 9.2.33 of TS 101 200-3 [1].

Prerequisite: A.23/33 -- INCREASE STAMPED command supported

Table A.32: Mode of INCREASE STAMPED

Item	Mode	Reference	Status	Support
1	No header included (P1 = "00")	9.2.33	o.19	
2	Header of DECREASE STAMPED command included (P1 = "01")	9.2.33	o.19	
3	Header of INCREASE STAMPED command included (P1 = "02")	9.2.33	o.19	
4	Header of DECREASE command included (P1 = "03")	9.2.33	o.19	
5	Header of INCREASE command included (P1 = "04")	9.2.33	o.19	

o.19: It is mandatory to support at least one of these items.

Comments:

A.5.6.5 Status conditions returned by the card

A.5.6.5.1 Support and coding of the status words

The following table lists all status conditions that could be returned by the card. The support of each status condition shall be indicated. The support for each of the codes is optional, as there is no mandatory relation between commands and response codes. They do however relate to commands (and therefore profiles) as listed in table A.34. The support of any of these codes automatically implies the support of the meaning defined for that code in TS 101 200-3 [1] subclause 9.4.6.

Table A.33: Status words by context

Item	Context of status condition	Reference	Status	Support
1	Security management	9.4.1	o	
1.1	98 02	9.4.1	c:o	
1.2	98 04	9.4.1	c:o	
1.3	98 08	9.4.1	c:o	
1.4	98 10	9.4.1	c:o	
1.5	98 35	9.4.1	c:o	
1.6	98 40	9.4.1	c:o	
1.7	98 50	9.4.1	c:o	
2	Memory management	9.4.2	o	
2.1	92 0X	9.4.2	c:o	
2.2	92 10	9.4.2	c:o	
2.3	92 20	9.4.2	c:o	
2.4	92 40	9.4.2	c:o	
3	Referencing management	9.4.3	o	
3.1	94 00	9.4.3	c:o	
3.2	94 02	9.4.3	c:o	
3.3	94 04	9.4.3	c:o	
3.4	94 08	9.4.3	c:o	
4	Application independent errors	9.4.4	m	
4.1	6E XX	9.4.4	o	
4.2	6D XX	9.4.4	o	
4.3	6F XX	9.4.4	c33_1	
4.4	6B XX	9.4.4	o	
4.5	67 XX	9.4.4	o	
5	Correctly executed commands	9.4.5	m	
5.1	90 00	9.4.5	m	
5.2	9F XX	9.4.5	c: c33_2	

c33_1: IF THE IUT CAN REACH AN ERROR STATE NOT COVERED BY ANY OF THE SUPPORTED CODES THEN m ELSE n/a

c33_2: IF A.4/8 THEN o ELSE n/a

Comments:

A.5.6.5.2 Commands versus possible status responses

The questions in the following subclause concern status conditions that are returned by the card following the receipt and processing of commands. They apply to all of the specified commands, listed in table A.23. The support for each of the codes is optional as the TS 101 200-3 [1] does not impose a mandatory support for combinations of errors and functions. However, if error codes are supported, they shall relate to the meaning as defined in TS 101 200-3 [1] in subclause 9.4.6. Furthermore the IUT shall be able to report both success and failure of any command using appropriate status responses.

In table A.34 the applied notation is different from the normal convention. There is a column for each of the relevant errors. The cells that that have been circled express an optional status to support the error for that command. It is assumed that an implementation just supports these combinations, therefore the person to complete this ICS is requested just to indicate the differences. To complete this table a supporting mark √ should be put in those cells that are supported although they are not circled. An exclusion mark × should be put in those cells that are circled, but not supported. No additions shall be made to this table if the implementation conforms exactly to this table.

Table A.34: Status responses to commands

		security							memory					reference					appl. indep.						ok	
Item	**Command**	**9802**	**9804**	**9808**	**98100**	**98350**	**98400**	**98500**		**9200X**	**92100**	**92200**	**92400**		**94000**	**94002**	**94004**	**94008**		**6EXX**	**6DXX**	**6FXX**	**6BXX**	**67XX**		**90000**	**9FXX**
1	ASK RANDOM												O							O	O	O	O	O		O	
2	CHANGE CHV	O	O	O	O	O	O			O			O							O	O	O	O	O		O	
3	CLOSE APPLICATION												O				O	O		O	O	O	O	O		O	
4	CREATE FILE	O	O		O	O				O	O	O	O							O	O	O	O	O		O	
5	CREATE RECORD	O	O		O	O				O	O		O		O	O		O		O	O	O	O	O		O	
6	DECREASE	O	O		O	O		O					O		O			O		O	O	O	O	O		O	O
7	DECREASE STAMPED	O	O		O	O		O					O		O			O		O	O	O	O	O		O	O
8	DELETE FILE	O	O		O	O				O			O				O			O	O	O	O	O		O	
9	DISABLE CHV	O	O	O	O	O	O			O			O							O	O	O	O	O		O	
10	ENABLE CHV	O	O	O	O	O	O			O			O							O	O	O	O	O		O	
11	ENVELOPE PUT												O							O	O	O	O	O		O	
12	EXECUTE	O	O		O	O							O		O			O		O	O	O	O	O		O	O
13	EXTEND	O	O		O	O				O	O		O					O		O	O	O	O	O		O	
14	EXTERNAL AUTHENTICATION	O	O		O	O				O			O							O	O	O	O	O		O	
15	GET RESPONSE												O							O	O	O	O	O		O	O
16	GIVE RANDOM												O							O	O	O	O	O		O	
17	INCREASE	O	O		O	O		O		O			O		O			O		O	O	O	O	O		O	O
18	INCREASE STAMPED	O	O		O	O		O		O			O		O			O		O	O	O	O	O		O	O
19	INTERNAL AUTHENTICATION	O	O		O								O					O		O	O	O	O	O		O	O
20	INVALIDATE	O	O		O	O				O			O							O	O	O	O	O		O	
21	LOAD KEYFILE	O	O		O	O				O			O		O			O		O	O	O	O	O		O	
22	LOCK	O	O		O	O				O			O				O			O	O	O	O	O		O	
23	READ BINARY		O		O								O		O	O		O		O	O	O	O	O		O	O
24	READ BINARY STAMPED	O	O		O	O							O		O	O		O		O	O	O	O	O		O	O
25	READ RECORD		O		O								O		O	O	O	O		O	O	O	O	O		O	O
26	READ RECORD STAMPED	O	O		O	O							O		O	O	O	O		O	O	O	O	O		O	O
27	REHABILITATE	O	O		O	O				O			O							O	O	O	O	O		O	
28	SEEK		O		O								O		O		O	O		O	O	O	O	O		O	O
29	SELECT												O				O			O	O	O	O	O		O	O
30	STATUS												O							O	O	O	O	O		O	
31	UNBLOCK CHV	O	O	O	O	O	O			O			O							O	O	O	O	O		O	
32	UPDATE BINARY	O	O		O	O				O			O		O	O		O		O	O	O	O	O		O	
33	UPDATE RECORD	O	O		O	O				O			O		O	O	O	O		O	O	O	O	O		O	
34	VERIFY CHV	O	O	O	O	O	O			O			O							O	O	O	O	O		O	
35	WRITE BINARY	O	O		O	O				O			O		O	O		O		O	O	O	O	O		O	
36	WRITE RECORD	O	O		O	O				O			O		O	O	O	O		O	O	O	O	O		O	

Comments:

A.5.7 Contents of special elementary files

Table A.35: General capabilities

Item	Capability	Reference	Status	Support
1	ASCII coding in accordance with ISO 8859-1	10	m	
2	Parity bit (bit 8) in ASCII characters set to "0" indicates no parity	10	m	
3	Optional data not at the end of a file is set to "FF"	10	m	

Comments:

A.5.7.1 Contents of the EFs at the MF level

The following table contains a list of EFs that shall or may be available in the card. The support of any of these files automatically implies the support of the indicated Access Condition and presence and coding of each mandatory element as defined in TS 101 200-3 [1].

Table A.36: EFs at the MF level

Item	EF	Reference	Status	Support
1	EF_{CHV}	10.1	o	
2	EF_{DIR}	10.2	o	
3	EF_{IC}	10.3	o	
4	EF_{ICC}	10.4	m	
5	EF_{ID}	10.5	m	
6	EF_{KEY_MAN}	10.6	m	
7	EF_{KEY_OP}	10.7	o	
8	EF_{LANG}	10.8	o	
9	EF_{NAME}	10.9	o	

Comments:

A.5.7.1.1 Optional data elements in EF_{ICC}

The support of any of the optional data elements automatically implies the support of its coding as defined in TS 101 200-3 [1].

Table A.37: Optional data elements in EF_{ICC}

Item	Data element	Reference	Status	Support
1	IC identifier	10.4	o	
2	Card Profile	10.4	o	
3	Type of selection (note)	10.4	o	

Comments:

NOTE: If the indication of type of selection is supported its value should match the actual supported selection types.

A.5.7.1.1.1 Profiles indicated in EF_{ICC}

This subclause indicates the supported profiles. If a profile is supported the associated commands and features described in clause 10.4 of TS 101 200-3 [1] should be supported likewise.

Prerequisite: A.37.2 -- Profile indicated in EF_{ICC}

Table A.38: Profiles

Item	Profile	Reference	Status	Support
1	0	10.4	o.20	
2	1	10.4	o.20	
3	2	10.4	o.20	
4	3	10.4	o.20	
5	4	10.4	o.20	
6	99	10.4	o.20	

o.20: It is mandatory to support at least one of these items.

Comments:

A.5.7.1.2 Optional data elements in EF_{ID}

The support of any of the optional data elements automatically implies the support of its coding as defined in TS 101 200-3 [1].

Table A.39: Optional data elements in EF_{ID}

Item	Data element	Reference	Status	Support
1	Date of activation	10.5	o	
2	Card expiry date	10.5	o	
3	Card sequence number	10.5	o	
4	Country code	10.5	o	

Comments:

A.5.7.1.3 Optional data elements in EF_{LANG}

The support of any of the optional data elements automatically implies the support of its coding as defined in TS 101 200-3 [1].

Table A.40: Optional data elements in EF_{LANG}

Item	Data element	Reference	Status	Support
1	First language preference	10.8	o	
2	Second language preference	10.8	o	
3	Third language preference	10.8	o	
4	Fourth language preference	10.8	o	

Comments:

A.5.7.1.4 Optional data elements in EF_{NAME}

The support of the optional data element automatically implies the support of its coding as defined in TS 101 200-3 [1].

Table A.41: Optional data elements in EF_{NAME}

Item	Data element	Reference	Status	Support
1	Card holder name	10.9	o	

Comments:

A.5.8 Design and manufacturing related security aspects

Table A.42: Security aspects in design and manufacturing

Item	Security aspect	Reference	Status	Support
1	Semiconductor design prevents reading secured and protected data	12.1.1	m	
2	Secure memory structure distributes coherent information over chip	12.1.1	o	
3	Operating systems ensures security and protection	12.1.1	m	
3.1	Unauthorized file access is prohibited	12.1.1	m	
3.2	Access conditions shall be fulfilled to get access	12.1.1	m	
3.3	File loading cannot corrupt other files	12.1.1	m	
4	Secure manufacturing process with physical access control and protection, event logging and logical protection of cryptographic information	12.1.2, 12.1.3, 12.1.4	m	

Comments:

Annex B (informative): Bibliography

- EN 726-4 (December 1994): "Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 4: Application independent card related terminal requirements".
- prEN 726-7 (May 1995): "Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 7: Security module".
- ISO 8859-1 (1987): "Information processing - 8-bit single byte coded graphic character sets, Part 1: Latin alphabet No.1".
- ISO 7811-3 (1985): "Identification cards - Recording technique - Part 3: Location of embossed character on ID-1 cards".
- 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 2-7437-1579-0
Dépôt légal : Juillet 1997