TS 101 203-2 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 2: Test Suite Structure and Test Purposes (TSS&TP)

Reference
DTS/PTS 00203-2 (b50i0icr.PDF)

Keywords
Card, testing, ATS, TSS&TP

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

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

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

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

Overview of ETSI deliverables on EN 726 family

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

Overview of ETSI deliverables on EN 726 conformance testing family

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

1 Scope

The present document provides the Test Suite Structure and Test Purposes (TSS&TP). It applies to the User Card (UC) defined in TS 101 200-3 [11] in compliance with the relevant requirements, and according to the relevant guidance given in ISO/IEC 9646-7 [15] and ETS 300 406 [12].

DISCLAIMER:

The present document provides conformance tests for the TS 101 200-3 [11]. To guarantee usefulness of an IC card it might be necessary to perform additional implementation dependent tests regarding:

- performance aspects;
- quality of security concepts;
- implementation dependent details not described in base standard.

Tests for behaviour of the IUT in case of memory problems are mandatory but it is out of the scope of this document how to create situations of failing memory.

It might be possible to create a failing memory situation by either stressing memory long enough or by using an emulator.

2 Normative references

The present document incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to the present document only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] EN 27816-1 (1989): "Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics(ISO 7816-1; 1987, edition 1)".

[2] EN 27816-2 (1989): "Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and locations of the contacts (ISO 7816-2; 1988, edition 1)".

[3] EN 27816-3 (1992): "Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols (ISO/IEC 7816-3; 1989, edition 1)".

[4] EN 27816-3 (1992): Amendment 1 (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 (ISO/IEC 7816-3; 1989, Amendment 1, 1992)".

[5] EN 27816-3 (1992): Amendment 2 (1995): "Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols. Amendment 2: Revision of protocol type selection (ISO/IEC 7816-3; 1989, Amendment 2, 1994)".

[6] ENV 1375-1 (1994): "Identification card systems - Intersector integrated circuit(s) card additional formats; Part1 ID-000 card size and physical characteristics".

[7] ENV 1375-2 (1994): "Identification card systems - Intersector integrated circuit(s) card additional formats; Part1 ID-00 card size and physical characteristics".

[8] EN 27811 (1989): "Identification cards - Recording Technique".

[9] ENV 1292 (April 1995): "Identification cards - Integrated circuit(s) cards and interface devices - Additional test methods".

[10] GSM 11.10-1 (August 1996): "Digital cellular telecommunication system (Phase 2); Mobile Station (MS) conformance specification; Part1: Conformance Specification".

[11] 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".

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

[13] ETS 300 759-1 (November 1995): "Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM); Part 1: Test Specification for DAM".

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

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

3 Definitions, symbols 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 [11];
- terms defined in ISO/IEC 9646-1 [14] and in ISO/IEC 9646-7 [15].

In particular, the following terms defined in ISO/IEC 9646-1 [14] 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.

oldest record: Record with highest record number. For writing operations it is the next written record (see also TS 101 200-3 [11], subclause 6.2.5).

readable: Any READ command can be performed on that record or file.

writable: Any UPDATE or WRITE command can be performed on that record or file.

3.2 Symbol

For the purposes of the present document, the following symbol applies:

{} Optional data, for example "CLA, INS, P1, P2, P3 {, data}" indicates that data may or may not follow the CLA, INS, P1, P2, P3 bytes.

3.3 Abbreviations

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

AC	Access Condition(s)
ACK	Acknowledge
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
CO	Command
CS	Cyclic Structure
DAM	DECT Authentication Module
DECT	Digital Enhanced Cordless Telecommunications
DF	Dedicated Files
DP	Data structure and pointers
EF	Elementary File
FU	Function
GR	GRaphical form (TTCN)
I/O	Input/Output
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
IV	Invalid behaviour test
IXIT	Implementation eXtra Information for Testing
LFS	Linear Fixed Structure
LM	Logical Model
LVS	Linear Variable Structure
MAC	Message Authentication Code
MF	Master File
MP	Machine Processable form (TTCN)
PC	Physical Characteristics
PDU	Protocol Data Unit
RC	Return Code
RC	Return Code
RST	Reset
SCS	System Conformance Statement
SM	Security Module
SP	electronic Signals and transmission Protocols
SUT	System Under Test
SW	Status Word
TC	Test Case
TP	Test Purposes
TR	TRansparent
TSS	Test Suite Structure
TTCN	Tree and Tabular Combined Notation
UC	User Card
VA	Valid behaviour test
VCC	supply Voltage
VPP	programming Voltage

4 Test environment

This clause specifies several requirements, which shall be met, and a number of rules, which shall be adhered to before testing can proceed.

ISO 9646-1 [14] describes a number of test methods that can be applied for testing. For the purpose of the present document the so called "remote test method" applies. This test method requires only access to the physical interface (the contacts) of the IC card.

4.1 Test equipment

This subclause recommends a minimum specification for each of the items of test equipment referenced in the tests.

4.1.1 Card Accepting Device (CAD) simulator

This item of equipment shall allow T = 0 or T = 1 protocol implementations to take place on ID-1 or ID-000 cards. It shall be able to generate and send any command APDU and receive any of the possible responses. These commands will be generated by translation of the ATS in the future EN to be approved within CEN.

The voltage level for VCC (contact C1) of the IC card shall be adjustable between 0 V and 6,0 V to an accuracy of 0,1 V. The voltage level for I/O (contact C7) when sending data to the IC card shall be adjustable between 0 V and 6,0 V to an accuracy of 0,1 V.

The CAD simulator shall be able to accept an external signal to drive RST (contact C3) of the IC card.

It shall be possible to access all the card contacts either directly or through test points.

4.2 Default data formatting

All numeric data enclosed in double quotes (") in this document is hexadecimal data.

Where "X" is used in place of a hexadecimal digit, X ranges from "0" to "F". For example, the data "6X" ranges from "60" to "6F" inclusive.

Where data is expressed as a group of bytes, it shall be in the following format: "XX XX XX... XX", indicating first byte, second byte, third byte etc. in that order.

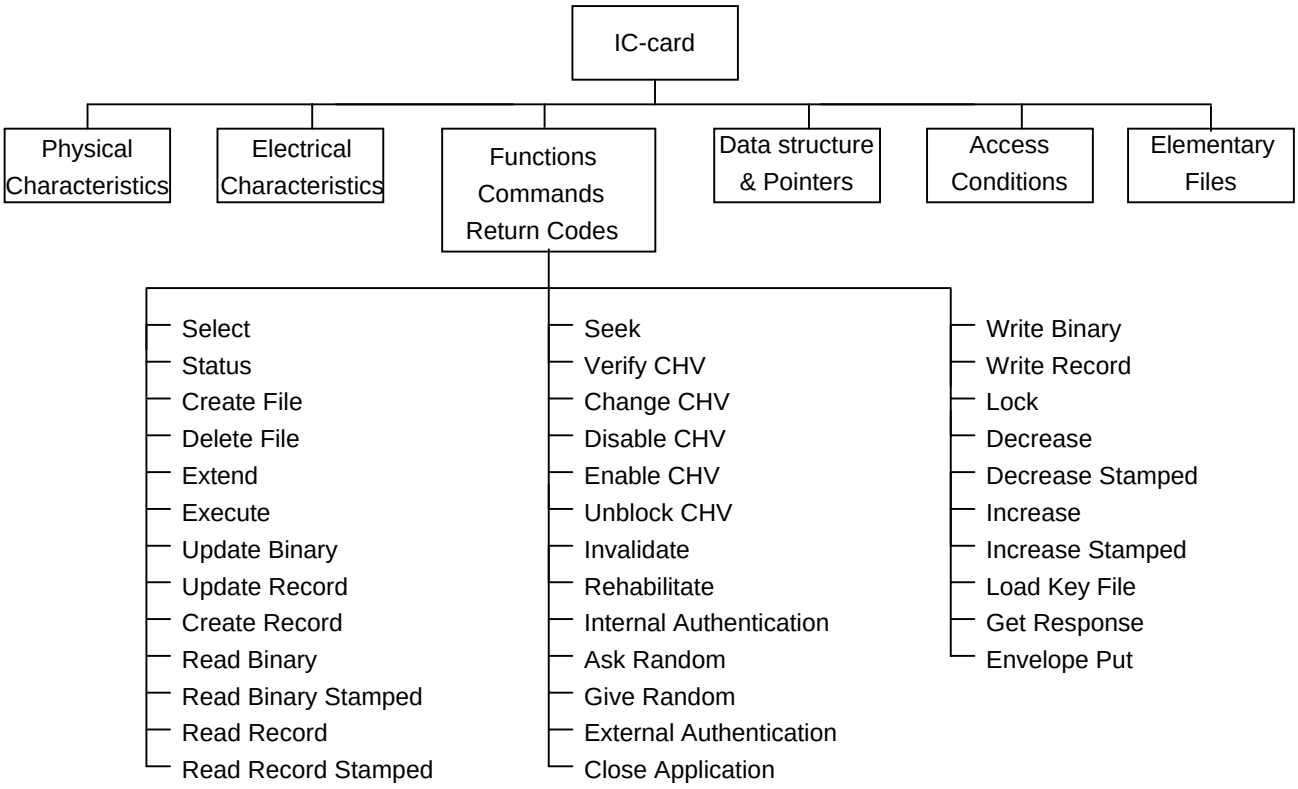
4.3 Test Procedure (TP)

The following statements are applicable to the test procedure clause for all Test Purposes (TP) contained within the present document:

- If there is a sequence control implemented, the commands have to be given in an allowed sequence, unless specified otherwise.
- Positive return codes are the SW1, SW2 = "90 00", "9F XX" or "92 0X".
- Negative return codes are all return codes indicating that an error has occurred.

5 Test suite structure

The following drawing roughly represents the test suite structure for testing the EN 726-3 [11].



6 Test Purposes (TP)

6.1 Introduction

For each test requirement at least one Test Purpose (TP) is defined.

6.1.1 TP naming convention

TPs are numbered, starting at 01, within each group. Groups are organized according to the TSS. Additional references are added to identify the actual Test Suite (TS). See table 1.

Table 1: TP Identifier naming convention scheme

Identifier:	<group>_<subgroup>_<type>_<nn>		
<group>	= major group	PC :	Physical characteristics
		SP :	Electronic signals and transmission protocols
		FU :	Functions
		CO :	Commands
		RC :	Return Codes
		DP :	Data structure and pointers
		AC :	Access Conditions
		EF :	Elementary Files
<subgroup>	= function, file or state	two characters to indicate the function,	
e.g.	SE for SELECT	XX if function independent.	
<type>	= type	one character field representing the type of test	
		VA:	Valid behaviour test
		IV:	Invalid behaviour test
<nn>	= sequential number:	(01-99)	

6.1.2 Source of TP definition

The TPs were developed based on EN 726-3 [11].

6.1.3 TP structure

Each TP has been written in a manner, which is consistent with all other TPs. The intention of this is to make the TPs more readable and checkable. A particular structure has been used and this is illustrated in table 2. This table shall be read in conjunction with any TP. Use a TP as an example to fully understand the table.

Table 2: Structure of a single TP

TP Part	Text	Example
Header	<Identifier> tab <subclause reference in base EN> tab {ICS limitation c<table no>_<line no>{, }}	see table 1 subclause 6.1.1 c9_3.1, c9_3.2
Purpose	Purpose of what to be tested	Check that the CREATE FILE command can be performed successfully to create a transparent EF to be filled with an arbitrary value.
Preconditions	Preconditions concerning file structure and status of the card which have to be fulfilled before test can be performed.	Current DF allows creation of son files
Test	Test itself <command> <command>	 CREATE FILE command READ BINARY
Result	Expected behaviour of the Card	All commands shall have a positive return code and.....

Applicability of tests

All tests described in this part of the standard are normative. In order to comply with the base standard (EN 726-3 [11]) each test covering a mandatory or supported optional capability shall be executed with a successful result. The test verdict shall be assigned according to the test purpose. The preconditions however do not necessarily express the only scenario in which a test purpose can be verified. Different scenarios leading to an unambiguous verification of the test purpose could be considered to confirm efficient test execution.

6.1.4 Test strategy

As the base standard contained no explicit requirements for testing, the TPs were generated as a result of an analysis of the base standard and ICS.

6.1.5 Valid behaviour test

This type of test is used whenever it shall be proved, that an implementation complies with the standard. The reaction on invalid stimuli or states is not the objective of this type of test.

6.1.6 Invalid behaviour test

Herewith all kind of error conditions are tested. This includes invalid or inopportune or exceptional commands, parameters, states or sequences. The tests verify whether the implementation shows robustness against invalid stimuli and that the returned Status Words (SW) comply with the standard.

6.2 IC card

6.2.1 Physical characteristics

The EN 726-3 [11] does not focus on physical characteristics. It does, however, point out a number of details that are similar to or slightly different from those defined in referenced standards. As a general precondition it is assumed that adequate tests to verify the physical characteristics of the card have been performed according to requirements of the relevant standards, and that detailed documentation of the results is available.

The following test purposes therefore request examination of this documentation to verify that the card meets the requirements of EN 726-3 [11].

PC_XX_VA_01 subclause 4 c1_1

Purpose
Check that the physical characteristics of the ID-1 card are in accordance with EN 27816-1, 2 [1], [2].

Preconditions
- None

Test
Apply test from ETSI test specification for DAM (ETS 300 759-1 [13]), subclause 6.1.1.1, (according to EN 27816-1 [1] and EN 27816-2 [2]).

Result
Test shall have results as described in the referenced specification.

PC_XX_VA_02 subclause 4 c1_2

Purpose
Check that the format of the card is in accordance with ENV 1375-1, 2 [6], [7].

Preconditions
- None

Test
Apply test from ETSI test specification for DAM (ETS 300 759-1 [13]), subclause 6.1.1.2, (according to ENV 1375-1, 2 [6] [7]).

Result
Test shall have results as described in the referenced specification.

PC_XX_VA_03 subclause 4.2c1_3

Purpose
Check that the card is functional in the temperature range -25°C to +65°C with occasional peaks up to +70°C.

Preconditions
- None

Test
Apply test from ETSI test specification for DAM (ETS 300 759-1 [13]), subclause 6.1.2, (making a correction for the different temperature range).

Result
Test shall have results as described in the referenced specification.

PC_XX_VA_04 subclause 4.2c1_4

Purpose
Check that the card is functional in the temperature range -25°C to +70°C with occasional peaks up to +85°C.

Preconditions
- None

Test

Apply test from ETSI test specification for DAM (ETS 300 759-1 [13]), subclause 6.1.2

Result

Test shall have results as described in the referenced specification.

PC_XX_VA_05 subclause 4.1c2_1, c3_4

Purpose

Check that the embossing is on the same side as contacts.

Preconditions

- None

Test

Check according to drawings in ISO 7816-2 [2] annex B.

Result

Test shall have results as described in the referenced specification.

PC_XX_VA_06 subclause 4.1c2_1, c3_1, c3_4

Purpose

Check that the number format and layout of embossed identification number are in accordance with EN 27811 [8].

Preconditions

- None

Test

Check according to drawings in EN 27811 [8].

Result

Test shall have results as described in the referenced specification.

PC_XX_VA_07 subclause 4.1c2_1, c3_2, c3_4

Purpose

Check that the number format and layout of embossed card sequence number are in accordance with EN 27811 [8].

Preconditions

- None

Test

Check according to drawings in EN 27811 [8].

Result

Test shall have results as described in the referenced specification.

PC_XX_VA_08 subclause 4.1c2_1, c3_5

Purpose

Check that the magnetic track is on the opposite side of contacts.

Preconditions

- None

Test

Check according to drawings in EN 27816-2 [2] annex B.

Result

Test shall have results as described in the referenced specification.

6.2.2 Electronic signals and transmission protocols

The EN 726-3 [11] does not focus on electrical signals and transmission protocols characteristics. It does however point out a number of details that are similar to or slightly different from those defined in referenced standard EN 27816-3 [3]. As a general precondition it is assumed that adequate tests to verify the electronic signals and transmission protocols of the card have been performed, and that detailed documentation of the results is available.

The following test purposes therefore request examination of this documentation to verify that the card meets the requirements of EN 726-3 [11].

SP_XX_VA_01 subclause 5 c4_1

Purpose

Check that the electronic signals are in accordance with EN 27816-3 [3] (with exception of requirements verified by other test in this group).

Preconditions

- None

Test

Apply test from ETSI test specification for DAM (ETS 300 759-1 [13]), subclauses 6.2.1. to 6.2.4. with the exception of the below mentioned tests using the values of EN 27816-3 [3].

Result

Test shall have results as described in the referenced specification.

SP_XX_VA_02 subclause 5 c4_1,c4_8

Purpose

Check that the transmission protocol is in accordance with EN 27816-3 [3].

Preconditions

- None

Test

Apply the scenarios of ENV 1292 [9]

Result

The scenarios shall operate as shown.

SP_XX_VA_03 subclause 5 c4_1,c4_9

Purpose

Check that the transmission protocol is in accordance with EN 27816-3 [4].

Preconditions

- None

Test

Apply the scenarios of EN 27816-3 [4].

Result

The scenarios shall operate as shown.

SP_XX_VA_04 subclause 5.1c4_2

Purpose

Check that a supply voltage VCC of 5 V ± 10 % is accepted.

Preconditions

- None

Test

Apply test from test specification for DAM (ETS 300 759-1 [13]), subclause 6.2.1.1.

Result

Test shall have results as described in the referenced specification.

SP_XX_VA_05 subclause 5.2 c4_3

Purpose

Check that the current consumption (excluding spikes) is ≤ 20 mA at any frequency accepted by the card.

Preconditions

- None

Test

Apply test from ETSI test specification for DAM (ETS 300 759-1 [13]), subclause 6.2.1.2 (taking alternative limit into account).

Result

Test shall have results as described in the referenced specification.

SP_XX_VA_06 subclause 5.2c4_4

Purpose

Check that the current consumption is ≤ 10 mA (excluding spikes).

Preconditions

- None

Test

Apply test from ETSI test specification for DAM (ETS 300 759-1 [13]), subclause 6.2.1.2.

Result

Test shall have results as described in the referenced specification.

SP_XX_VA_07 subclause 5.2 c4_5

Purpose

To check that current spikes are always below 40 nAs, 400 ns and 200 mA.

Preconditions

- None

Test

Apply test from GSM standard 11.10 [10]], subclause 27.17.2.

Result

Test shall have results as described in the referenced specification.

SP_XX_VA_08 subclause 5.3c4_6

Purpose

To check for internal generation of programming voltage.

Preconditions

- None

Test

Check the documentation delivered by the manufacturer that the card either does not use VPP contact or requires the same voltage as for VCC.

Result

Test shall have results as described in the referenced specification.

SP_XX_VA_09 subclause 5.4 c4_7

Purpose

To check that the duty cycle for asynchronous operation is in between 40 % and 60 %.

Preconditions

- None

Test

Apply test from ETSI test specification for DAM (ETS 300 759-1 [13]), subclause 6.2.3.1.

Result

Test shall have results as described in the referenced specification.

SP_XX_VA_10 subclause 5.5c4_8

Purpose

Extra character guard time indication from terminal to card (TC1 parameter N in ATR) equals 0 or 4.

Preconditions

- None

Test

Read parameter in ATR.

Result

The value of TC1 shall be 0 or 4.

SP_XX_VA_11 subclause 5.5c4_9

Purpose

Extra character guard time indication from terminal to card (TC1 parameter N in ATR) equals 0, 4 or 255.

Preconditions

- None

Test

Read parameter in ATR.

Result

The value of TC1 shall be 0, 4 or 255.

6.2.3 Functions, commands and return codes

Functions

Communication between terminals and user cards can be performed via 34 different functions. A function typically involves a signal (command) from the terminal to the IC card and a corresponding signal (response) from the IC card to the terminal. See figure 1. The processing of the function on the IC card can result in a change of data inside the IC card (e.g. a pointer or file contents).

The result (successful or not) of the function is reported in the response that is sent from IC card to terminal and verified by issuing additional commands.

Scenario:

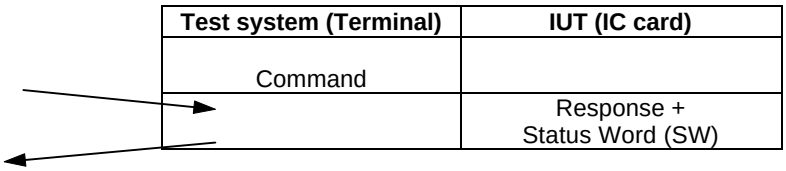


Figure 1: Scenario for testing functions

This subclause focuses on the actions that shall be performed by the function, e.g. does the function actually do what it is intended to do. The next subclauses will focus on the commands and return codes, which is more related to coding variations of the data exchanged between terminal and IC card.

Testing of the functions is performed by the following steps:

1. Make sure that pre-conditions are fulfilled. This may be done by preambles that store the required data on the IC card or initialize the required state. A default pre-condition is to make sure that Access Conditions related to the test are fulfilled.

2. Issue a command with correct parameters; If no explicit values for the fields are given then an average or logical value is presumed.

3. Check for correct response data (if relevant for the function) and a positive return code (status condition returned by the IC card = hex "90 00");

4. If data should be changed inside the IC card:

5. Issue commands and check response data to verify the result of the original function;

6. Perform a postamble to undo the internal IC card data changes caused by the test.

Commands

Testing the commands is very similar to the testing of functions. For every function a command is available, but there are two more commands used for transparent transport of data.

This subclause merely focuses on valid variations of command fields. The testing scenario is the same as for functional testing. A command is sent and the result is checked to evaluate its success.

Testing of the commands is performed by the following steps:

1. Make sure that pre-conditions are fulfilled. This may be done by preambles that store the required data on the IC card or initialize the required state. A default pre-condition is to make sure that Access Conditions related to the test are fulfilled.

2. Issue a command with correct parameters.

3. Check for correct response data (if relevant for the function) and a positive return code (status condition returned by the IC card = hex "90 00").

If data should be changed inside the IC card:

4. Issue commands and check response data to verify whether the field values were correctly interpreted by the IUT.

5. Perform a postamble to undo the internal IC card data changes caused by the test.

Return codes
According to EN 27816-3 [3] two status bytes, SW1 and SW2, are returned after each command, the coding of theses status bytes is given in subclause 9.4 of EN 726-3 [11]. The following tests are to be used to ensure that the UC is able to respond with the specified status words.

6.2.3.1 SELECT (SE)

6.2.3.1.1 Function

FU_SE_VA_01 subclause 8.1c19_1, c23_1, c24_1

Purpose
Check that the SELECT function can be performed for a downward selection by file id (according to file qualifier) of a DF.

Preconditions
- DF to be selected contains at least one EF;

- DF pointer is in DF above the DF to be selected;

Test
Select the DF and then try to select the EF within the selected DF.

Result
Both commands shall have a positive return code.

FU_SE_VA_02 subclause 8.1 c19_1, c23_1, c23_10, c24_1

Purpose
Check that the SELECT function can be performed for a downward selection by file id (according to file qualifier) of an EF.

Preconditions
- Readable transparent EF exists;

- DF pointer is in DF that contains that EF;

Test
Select the EF and try to read one bytes from it.

Result
Both commands shall have a positive return code.

FU_SE_VA_03 subclause 8.1 c19_1, c23_1, c23_10, c24_1

Purpose
Check that the SELECT function can be performed for a horizontal selection by file id (according to file qualifier) of an EF.

Preconditions
- Readable transparent EF exists;

- EF pointer is on other EF under the same DF;

Test

Select the EF and try to read one byte from it.

Result

Both commands shall have a positive return code.

FU_SE_VA_04 subclause 8.1 c19_1, c23_1, c24_1

Purpose

Check that the SELECT function can be performed for a horizontal selection by file id (according to file qualifier) of a DF.

Preconditions

- DF to be selected contains at least one EF;
- File pointer is on EF within a DF above DF to select;

Test

Select the DF and then try to select the EF within the selected DF.

Result

Both commands shall have a positive return code.

FU_SE_VA_05 subclause 8.1 c19_1, c23_1, c24_1

Purpose

Check that the SELECT function can be performed for a upward selection by file id (according to file qualifier) of a DF.

Preconditions

- DF to be selected contains at least one EF;
- DF pointer is on DF under DF to be selected;

Test

Select the DF and then try to select the EF within the selected DF.

Result

Both commands shall have a positive return code.

FU_SE_VA_06 subclause 8.1 c19_1, c23_1, c23_10, c24_6

Purpose

Check that the SELECT function can be performed for a absolute (from MF) selection by path of an EF.

Preconditions

- Readable transparent EF exists in DF other than MF;
- DF pointer is in DF other than MF or DF above EF to be selected;

Test

Select the EF and try to read one bytes from it.

Result

Both commands shall have a positive return code.

FU_SE_VA_07 subclause 8.1 c19_1, c23_1, c23_10, c24_7

Purpose

Check that the SELECT function can be performed for a relative (from current DF) selection by path of an EF.

Preconditions

- Readable transparent EF exists in a DF at least two levels below MF;

- DF pointer is in DF (other than MF) which is in the path of the EF to be selected;

Test

Select the EF and try to read one bytes from it.

Result

Both commands shall have a positive return code.

FU_SE_VA_08 subclause 8.1 c19_1, c23_1, c24_5

Purpose

Check that the SELECT function can be performed for a selection by application identifier of a DF.

Preconditions

- DF to be selected is registered by application id within EFdir;
- DF to be selected contains at least one EF;
- DF pointer is on DF other than DF to be selected;

Test

Select the DF and then try to select the EF within the selected DF.

Result

Both commands shall have a positive return code.

FU_SE_VA_09 subclause 8.1c19_1, c23_1, c24_1, c23_3, c23_4

Purpose

Check that the SELECT function returns correctly the number of son DFs.

Preconditions

- DF selected contains known number of son DFs;

Test

Select the DF to check the number of son DFs. Then create another DF within it and select the DF again to check the number of son DFs. Then delete a son DF and select the DF again to check the number of son DFs.

Result

All commands shall have a positive return code. And the number of son DFs shall always be in accordance with the actual number of sons.

FU_SE_VA_10 subclause 8.1 c19_1, c23_1, c23_10, c24_1, c23_3, c23_4

Purpose

Check that the SELECT function returns correctly the number of son EFs.

Preconditions

- DF selected contains known number of son EFs;

Test

Select the DF to check the number of son EFs. Then create another EF within it and select the DF again to check the number of son EFs. Then delete a son EF and select the DF again to check the number of son EFs.

Result

All commands shall have a positive return code. And the number of son EFs shall always be in accordance with the actual number of sons.

6.2.3.1.2 Command

The coding of the SELECT command is the following:

Table 3: Return codes for the SELECT command

CLA	Class byte
INS	"A4"
P1	Selection control
P2	Type of selection
L_c field	Length of data field
Data field	File Id, Path or Application identifier
L_e field	Maximum length of data expected in response

CO_SE_VA_01 subclause 9.1 c23_1, c24_2

Purpose
Check that the SELECT command can be performed for a downward selection by file id (select son DF) of a DF.

Preconditions
- DF to be selected contains at least one EF;
- DF pointer is in DF above the DF to be selected;

Test
Select the DF and then try to select the EF within the selected DF.

Result
Both commands shall have a positive return code.

CO_SE_VA_02 subclause 9.1 c23_1, c24_3

Purpose
Check that the SELECT command can be performed for a downward selection by file id (select son EF) of an EF.

Preconditions
- EF exists;
- DF pointer is in DF that contains that EF;

Test
Select the EF.

Result
Command shall have a positive return code and the response data shall be correct.

CO_SE_VA_03 subclause 9.1 c23_1, c24_1, c24_4

Purpose
Check that the SELECT command can be performed for an upward selection by file id (select parent DF) of a DF.

Preconditions
- DF to be selected contains at least one EF;
- No EF is selected;
- DF pointer is on DF under DF to be selected;

Test

Select the DF and then try to select the EF within the selected DF.

Result

Both commands shall have a positive return code.

CO_SE_VA_04 subclause 9.1 c23_1, c24_1, c24_4

Purpose

Check that the SELECT command can be performed for an upward selection by file id (select parent DF) of a DF, if there is an EF selected in current EF.

Preconditions

- DF to be selected contains at least one EF;
- Current DF contains EF which is selected;
- DF pointer is on DF under DF to be selected;

Test

Select the DF and then try to select the EF within the newly selected DF.

Result

Both commands shall have a positive return code.

CO_SE_VA_05 subclause 9.1 c23_1, c24_6

Purpose

Check that the SELECT command can be performed for an EF having a large size path.

Preconditions

- EF exists in maximum DF level supported by ICC;
- DF pointer is in DF other than MF or DF above EF to be selected;

Test

Select the EF using the absolute (from MF) selection by path.

Result

Command shall have a positive return code and the response data shall be correct.

CO_SE_VA_06 subclause 9.1 c23_1, c24_6

Purpose

Check that the SELECT command can be performed to select an EF_{CHV1}.

Preconditions

- EF_{CHV1} exists;
- DF pointer is in DF above EF to be selected;

Test

Select the EF.

Result

Command shall have a positive return code and the response data shall be correct.

CO_SE_VA_07 subclause 9.1 c23_1, c24_6

Purpose

Check that the SELECT command can be performed to select an EF_{CHV2}.

Preconditions

- EF_{CHV2} exists;
- DF pointer is in DF above EF to be selected;

Test

Select the EF.

Result

Command shall have a positive return code and the response data shall be correct.

CO_SE_VA_08 subclause 9.1 c23_1, c24_6

Purpose

Check that the SELECT command can be performed to select an EF_{KEY_OP}.

Preconditions

- EF_{KEY_OP} exists;
- DF pointer is in DF above EF to be selected;

Test

Select the EF.

Result

Command shall have a positive return code and the response data shall be correct.

CO_SE_VA_09 subclause 9.1 c23_1, c24_6

Purpose

Check that the SELECT command can be performed to select an EF_{KEY_MAN}.

Preconditions

- EF_{KEY_MAN} exists;
- DF pointer is in DF above EF to be selected;

Test

Select the EF.

Result

Command shall have a positive return code and the response data shall be correct.

CO_SE_VA_10 subclause 9.1 c23_1, c24_6

Purpose

Check that the SELECT command can be performed for an EF while just 4 bytes response are requested.

Preconditions

- EF exists;
- DF pointer is in DF above EF to be selected;

Test

Select the EF.

Result

Command shall have a positive return code and the response data shall be correct.

CO_SE_VA_11 subclause 9.1 c23_1, c24_6

Purpose

Check that the SELECT command can be performed for an EF while L_e is specified with "00".

Preconditions

- EF exists;
- DF pointer is in DF above EF to be selected;

Test

Select the EF.

Result

Command shall have a positive return code and complete response data shall be received.

6.2.3.1.3 Return codes

Table 4: Return codes for the SELECT command

Return Code	Error description
94 04	- File ID not found
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" qualifier P1 ≠ "01" son DF P1 ≠ "02" son EF P1 ≠ "03" parent P1 ≠ "04" application identifier P1 ≠ "08" path from MF P1 ≠ "09" path from current DF
67 XX	- L_c ≠ empty P1 = "03","08" L_c ≠ "01.."10" P1 = "04" L_c ≠ "even" P1 = "00","01","02","08","09"
92 40	- no test is foreseen for this status word
90 00	- Normal ending (ACK) of the command
9F XX	- Length "XX" of the response data

RC_SE_VA_01 subclause 9.4.6 c19_1, c4_9

Purpose

Check that SELECT returns "90 00", if used correctly.

Preconditions

- MF exists.

Test

Reset the UC and present a SELECT command to select the MF by using P1 = 00 and the qualifier being the MF-ID.

Result

The expected status word is "90 00".

RC_SE_VA_02 subclause 9.4.6 c19_1, c4_8

Purpose

Check that SELECT returns "9F XX", if used correctly.

Preconditions

- MF exists.

Test

Reset the UC and present a SELECT command to select the MF by using P1 = 00 and the qualifier being the MF-ID.

Result

The expected status word is "9F XX".

RC_SE_IV_01 subclause 9.4.6 c19_1

Purpose

Check that SELECT returns "94 04", if the select File-ID does not exist.

Preconditions

- Not existing File-ID known.

Test

Reset the UC and present a SELECT command to select the File by using P1 = 00 and the qualifier being the File-ID.

Result

The expected status word is "94 04".

RC_SE_IV_02 subclause 9.4.6 c19_1

Purpose

Check that SELECT returns "6B XX" if the parameter P1 ≠ "00", P1 ≠ "01", P1 ≠ "02", P1 ≠ "03", P1 ≠ "04", P1 ≠ "08" and P1 ≠ "09".

Preconditions

- MF exists.

Test

Reset the UC and present a SELECT command to select the MF by using a not allowed parameter P1 and the qualifier being the MF-ID.

Result

The expected status word is "6B XX".

RC_SE_IV_03 subclause 9.4.6 c19_1

Purpose

Check that SELECT returns "67 XX", if the L_c is not allowed.

Preconditions

- MF exists.

Test

Reset the UC and present a SELECT command to select the MF with P1 = 0 and the qualifier being the MF-ID, plus additional bytes, so that L_c will not be equal to 2.

Result

The expected status word is "67 XX".

6.2.3.2 STATUS (ST)

6.2.3.2.1 Function

FU_ST_VA_01 subclause 8.2 c19_2, c23_2

Purpose

Check that the STATUS function can be performed for the MF.

Preconditions

- MF selected; No EF is selected:

Test

Perform the STATUS command.

Result

The command shall have a positive return code and the response data shall be in accordance with the MF characteristics.

FU_ST_VA_02 subclause 8.2 c19_2, c23_2

Purpose

Check that the STATUS function can be performed for a DF.

Preconditions

- DF other than MF selected: No EF is selected:

Test

Perform the STATUS command.

Result

The command shall have a positive return code and the response data shall be in accordance with the DF characteristics.

FU_ST_VA_03 subclause 8.3 c19_2, c23_2

Purpose

Check that the STATUS function can be performed for a DF, while an EF is selected.

Preconditions

- DF other than MF selected; Any EF selected:

Test

Perform the STATUS command.

Result

The command shall have a positive return code and the response data shall be in accordance with the DF characteristics.

6.2.3.2.2 Command

The coding of the Status command is the following:

Table 5: Return codes for the STATUS command

CLA	Class byte
INS	"F2"
P1	"00"
P2	"00"
L_c field	Empty
Data field	Empty
L_e field	Maximum length of data expected in response

CO_ST_VA_01 subclause 9.2 c23_1, c23_2

Purpose

Check that the STATUS command can be performed while just 10 bytes response are requested.

Preconditions

- DF selected;

Test

Perform the STATUS command with L_e="0A".

Result

STATUS shall return the first 10 bytes of a correct response.

6.2.3.2.3 Return codes

Table 6: Return codes for the STATUS command

Return Code	Error description
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" and P2 ≠ "00"
67 XX	- no test is foreseen for this status word
92 40	- no test is foreseen for this status word
90 00	- Normal ending (ACK) of the command

RC_ST_VA_01 subclause 9.4.6 c19_2

Purpose

Check that STATUS returns "90 00", if used correctly.

Preconditions

- None.

Test

Reset the UC and present a STATUS command.

Result

The expected status word is "90 00".

RC_ST_IV_01 subclause 9.4.6 c19_2

Purpose

Check that STATUS returns "6B XX" if the parameter P1 ≠ "00" or P2 ≠ "00".

Preconditions

- MF exists.

Test

Reset the UC and present a STATUS command with P1 ≠ "00" or P2 ≠ "00".

Result

The expected status word is "6B XX".

6.2.3.3 CREATE FILE (CF)

6.2.3.3.1 Function

FU_CF_VA_01 subclause 8.3 c19_3, c23_3, c23_1, c6_1

Purpose

Check that the CREATE FILE function can be performed successfully to create an EF.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create an transparent EF. Check by means of the SELECT command whether the EF has been created.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command was performed shall be in accordance with the data provided by the CREATE FILE command.

FU_CF_VA_02 subclause 8.3 c19_30, c23_3, c23_1

Purpose

Check that the CREATE FILE function can be performed successfully to create a DF.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create a DF. Check by means of the SELECT command whether the DF has been created.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command was performed shall be in accordance with the data provided by the CREATE FILE command.

6.2.3.3.2 Command

The coding of the CREATE FILE command is the following:

Table 7: Return codes for the CREATE FILE command

CLA	Class byte
INS	"E0"
P1	initialization value
P2	Type of creation
L_c field	Length of data field
Data field	Data sent to the card (+cryptogram)
L_e field	Empty

CO_CF_VA_01 subclause 9.3 c23_3, c23_1, c6_2

Purpose

Check that the CREATE FILE command can be performed successfully to create a linear fixed structure EF.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create a linear fixed structure EF. Check by means of the SELECT command whether the EF has been created.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command was performed shall be in accordance with the data provided by the CREATE FILE command.

CO_CF_VA_02 subclause 9.3 c23_3, c23_1, c6_3

Purpose

Check that the CREATE FILE command can be performed successfully to create a linear variable structure EF.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create a linear variable structure EF. Check by means of the SELECT command whether the EF has been created.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command was performed shall be in accordance with the data provided by the CREATE FILE command.

CO_CF_VA_03 subclause 9.3 c23_3, c23_1, c6_5

Purpose

Check that the CREATE FILE command can be performed successfully to create an EF to contain an ASC.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create an EF to contain an ASC. Check by means of the SELECT command whether the EF has been created.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command was performed shall be in accordance with the data provided by the CREATE FILE command.

CO_CF_VA_04 subclause 9.3 c23_3, c23_1, c6_1_1

Purpose

Check that the CREATE FILE command can be performed successfully to create a transparent EF to contain a program.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create a transparent EF to contain a program. Check by means of the SELECT command whether the EF has been created.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command was performed shall be in accordance with the data provided by the CREATE FILE command.

CO_CF_VA_05 subclause 9.3 c23_3, c23_1, c6_5

Purpose

Check that the CREATE FILE command can be performed successfully to create a DF to contain an ASC file.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create a DF to contain an ASC file. Check by means of the SELECT command whether the EF has been created.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command was performed shall be in accordance with the data provided by the CREATE FILE command.

CO_CF_VA_06 subclause 9.3 c23_3, c23_1, c6_1, c23_10

Purpose

Check that the CREATE FILE command can be performed successfully to create a transparent EF to be filled with an arbitrary value.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create a transparent EF to fill with an arbitrary value. Check by means of the SELECT command whether the EF has been created and by means of a READ BINARY whether the contents of the file matches the given value.

Result

All commands shall have a positive return code and the data returned by the card after the SELECT and READ BINARY commands are performed shall be in accordance with the data provided by the CREATE FILE command.

CO_CF_VA_07 subclause 9.3 c23_3, c23_1, c6_2, c23_12

Purpose

Check that the CREATE FILE command can be performed successfully to create a linear fixed EF to be filled with records with an arbitrary value.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create a linear fixed EF to fill with an arbitrary value.

Check by means of the SELECT command whether the EF has been created and by means of a READ RECORD command whether the number of records and contents of the file match.

Result

All commands shall have a positive return code and the data returned by the card after the SELECT and READ RECORD commands are performed shall be in accordance with the data provided by the CREATE FILE command.

CO_CF_VA_08 subclause 9.3 c23_3, c23_1, c6_4, c23_12

Purpose

Check that the CREATE FILE command can be performed successfully to create a cyclic EF to be filled with records with an arbitrary value.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create a cyclic EF to fill with an arbitrary value.

Check by means of the SELECT command whether the EF has been created and by means of a READ RECORD command whether the number of records and contents of the file match.

Result

All commands shall have a positive return code and the data returned by the card after the SELECT and READ RECORD commands are performed shall be in accordance with the data provided by the CREATE FILE command.

CO_CF_VA_09 subclause 9.3 c23_3, c23_1, c6_1

Purpose

Check that the CREATE FILE command can be performed successfully to create a large transparent EF.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create a large transparent EF.

Check by means of the SELECT command whether the EF has been created.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command is performed shall be in accordance with the data provided by the CREATE FILE command.

CO_CF_VA_10 subclause 9.3 c23_3, c23_1, c6_1

Purpose

Check that the CREATE FILE command can be performed successfully to create an EF with highest possible file ID.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create a transparent EF with highest possible file ID.

Check by means of the SELECT command whether the EF has been created.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command is performed shall be in accordance with the data provided by the CREATE FILE command.

CO_CF_VA_11 subclause 9.3 c23_3, c23_1, c6_1

Purpose

Check that the CREATE FILE command can be performed successfully to create an EF with lowest possible file ID.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create a transparent EF with lowest possible file ID.

Check by means of the SELECT command whether the EF has been created.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command is performed shall be in accordance with the data provided by the CREATE FILE command.

CO_CF_VA_12 subclause 9.3 c23_3, c23_1, c6_1, c9_1

Purpose

Check that the CREATE FILE command can be performed successfully to create an invalidated EF.

Preconditions

- Current DF allows creation of son files;

- Invalidation/Rehabilitation is an applicable feature of the Card operating system.

Test

Perform a CREATE FILE command to create an invalidated transparent EF.

Check by means of the SELECT command whether the EF has been created.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command is performed shall be in accordance with the data provided by the CREATE FILE command.

CO_CF_VA_13 subclause 9.3 c23_3, c23_1, c6_1, c9_1

Purpose

Check that the CREATE FILE command can be performed successfully to create an EF that is not readable when invalidated.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create a transparent EF that is not readable when invalidated.

Check by means of the SELECT command whether the EF has been created.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command is performed shall be in accordance with the data provided by the CREATE FILE command.

CO_CF_VA_14 subclause 9.3 c23_3, c23_1, c6_1, c24_5

Purpose

Check that the CREATE FILE command can be performed successfully to create a DF having an Application Identifier.

Preconditions

- Current DF allows creation of son files;

Test

Perform a CREATE FILE command to create a DF having an Application Identifier.

Check by means of the SELECT (using the Application Id) command whether the DF has been created.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command is performed shall be in accordance with the data provided by the CREATE FILE command.

6.2.3.3.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 8: Return codes for the CREATE FILE command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
92 0X	- Update successful but after using internal retry routine X times
92 10	- Insufficient memory space available
92 20	- File ID is already available in this parent directory
92 40	- Update impossible (memory problem)
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" or P2 ≠ "00"
67 XX	- L_c < "12" + X or L_c > "21" + X
90 00	- Normal ending (ACK) of the command

RC_CF_VA_01 subclause 9.4.6 c19_3

Purpose

Check that CREATE FILE returns "90 00" if used correctly.

Preconditions

- The AC for CREATE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.

Test

Present a CREATE FILE command with an ID of a not existing file and a valid cryptogram.

Result

The expected status word is "90 00".

RC_CF_IV_01 subclause 9.4.6 c19_3

Purpose

Check that CREATE FILE returns "98 02" if the key associated with the AC CREATE does not exist.

Preconditions

- The AC for CREATE is PRO.
- The key associated with the AC CREATE does not exist.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.

Test

Present a CREATE FILE command with an ID of a not existing file and any cryptogram.

Result

The expected status word is "98 02".

RC_CF_IV_02 subclause 9.4.6 c19_3

Purpose

Check that CREATE FILE returns "98 04" if the AC for CREATE is not fulfilled.

Preconditions

- The AC for CREATE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.

Test

Present a CREATE FILE command with an ID of a not existing file and a wrong cryptogram.

Result

The expected status word is "98 04".

RC_CF_IV_03 subclause 9.4.6 c19_3, c9_1

Purpose

Check that CREATE FILE returns "98 10" if the DF is invalidated.

Preconditions

- The AC for CREATE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.
- The current DF is invalidated.

Test

Present a CREATE FILE command with an ID of a not existing file and a valid cryptogram.

Result

The expected status word is "98 10".

RC_CF_IV_04 subclause 9.4.6 c19_3

Purpose

Check that CREATE FILE returns "98 35" if no random has been asked for.

Preconditions

- The AC for CREATE is PRO.
- No random has been asked for.
- Enough memory for the file creation is available under the current DF.

Test

Present a CREATE FILE command with an ID of a not existing file and any cryptogram.

Result

The expected status word is "98 35".

RC_CF_IV_05 subclause 9.4.6 c19_3

Purpose

Check that CREATE FILE returns "92 0X" if the internal retry routine has been used.

Preconditions

- The AC for CREATE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.
- The internal memory can only be written after X retries.

Test

Present a CREATE FILE command with an ID of a not existing file and a valid cryptogram.

Result

The expected status word is "92 0X".

RC_CF_IV_06 subclause 9.4.6 c19_3

Purpose

Check that CREATE FILE returns "92 10" if the available memory is not sufficient.

Preconditions

- The AC for CREATE is PRO.
- A random has been asked for.
- There is not enough memory under the current DF available to create the file.

Test

Present a CREATE FILE command with an ID of a not existing file and a valid cryptogram.

Result

The expected status word is "92 10".

RC_CF_IV_07 subclause 9.4.6 c19_3

Purpose

Check that CREATE FILE returns "92 20" if the given file ID already exists.

Preconditions

- The AC for CREATE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.
- ID of an existing file is known.

Test

Present a CREATE FILE command with an ID of an existing file and a valid cryptogram.

Result

The expected status word is "92 20".

RC_CF_IV_08 subclause 9.4.6 c19_3

Purpose

Check that CREATE FILE returns "92 40" if the internal memory can not be written.

Preconditions

- The AC for CREATE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.
- The internal memory can not be written.

Test

Present a CREATE FILE command with an ID of a not existing file and a valid cryptogram.

Result

The expected status word is "92 40".

RC_CF_IV_09 subclause 9.4.6 c19_3

Purpose

Check that CREATE FILE returns "6B XX" if P2 > 3 or (P1 ≠ "00" and (P2 = "01" or P2 = "03")).

Preconditions

- The AC for CREATE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.

Test

Present a CREATE FILE command with an ID of a not existing file, a valid cryptogram and P1 ≠ "00" and P2 = "01".

Result

The expected status word is "6B XX".

RC_CF_IV_10 subclause 9.4.6 c19_3

Purpose

Check that CREATE FILE returns "6B XX" if P1 ≠ "00" and file ID = ."0001" (EF_{KEY_OP})

Preconditions

- The AC for CREATE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.
- EF_{KEY_OP} does not exist under the current DF.

Test

Present a CREATE FILE command with ID "0001", a valid cryptogram and P1 ≠ "00" and P2 = "00".

Result

The expected status word is "6B XX".

RC_CF_IV_11 subclause 9.4.6 c19_3

Purpose

Check that CREATE FILE returns "6B XX" if P1 ≠ "00" and file ID = ."0000" (EF_{CHV1})

Preconditions

- The AC for CREATE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.
- EF_{CHV1_OP} does not exist under the current DF.

Test

Present a CREATE FILE command with ID "0000", a valid cryptogram and P1 ≠ "00" and P2 = "00".

Result

The expected status word is "6B XX".

RC_CF_IV_12 subclause 9.4.6 c19_3

Purpose

Check that CREATE FILE returns "67 XX" if L_c < "10" or L_c > "21" + X.

Preconditions

- The AC for CREATE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.

Test

Present a CREATE FILE command with an ID of a not existing file, a valid cryptogram and L_c < "10" + X or L_c > "21" + X.

Result

The expected status word is "67 XX".

6.2.3.4 Delete File (DF)

6.2.3.4.1 Function

FU_DF_VA_01 subclause 8.4 c19_4, c23_4, c23_1

Purpose

Check that the DELETE FILE function can be performed successfully to delete an EF.

Preconditions

- EF exists within current DF;

Test

Perform a DELETE FILE command to delete the EF. Check by means of the SELECT command whether the EF has been deleted.

Result

The DELETE FILE command shall have a positive return code while the SELECT command shall fail.

FU_DF_VA_02 subclause 8.4 c19_4, c23_4, c23_1

Purpose

Check that the DELETE FILE function can be performed successfully to delete an empty DF.

Preconditions

- Empty DF exists within current DF;

Test

Perform a DELETE FILE command to delete the DF. Check by means of the SELECT command whether the DF has been deleted.

Result

The DELETE FILE command shall have a positive return code while the SELECT command shall fail.

FU_DF_VA_03 subclause 8.4 c19_4, c23_4, c23_3

Purpose

Check that the DELETE FILE function can be performed successfully to delete an empty DF and the deleted file can be newly created.

Preconditions

- Empty DF exists within current DF;

Test

Perform a DELETE FILE command to delete the DF.

Check by means of the CREATE FILE command whether the DF has been deleted.

Result

The DELETE FILE and the CREATE FILE command shall have a positive return code.

FU_DF_VA_04 subclause 8.4 c19_4, c23_4, c23_5

Purpose

Check that the DELETE FILE function can be performed successfully to delete an empty DF and the

deleted file is not available anymore for the EXTEND command.

Preconditions

- Empty DF exists within current DF;

Test

Perform a DELETE FILE command to delete the DF.

Check by means of the EXTEND command whether the DF has been deleted.

Result

The DELETE FILE command shall have a positive return code while the EXTENT command shall fail.

FU_DF_VA_05 subclause 8.4 c19_30, c23_3, c23_1

Purpose

Check that after file deletion and following CREATE FILE command execution data of original file is destroyed.

Preconditions

- Any transparent EF created

- Data pattern written into that EF

Test

Perform DELETE FILE command on EF

Perform CREATE FILE command on the deleted EF

Check that the EF is empty by using READ BINARY command

Result

All commands shall have a positive return code and data returned by the card shall be an empty string.

6.2.3.4.2 Command

The coding of the DELETE FILE command is the following:

Table 9: Return codes for the DELETE FILE command

CLA	Class byte
INS	"E4"
P1	"00"
P2	"00"
L_c field	Length of data field
Data field	File ID (+cryptogram)
L_e field	Empty

No tests are foreseen to test the DELETE FILE command other than those defined in the functions subclause.

6.2.3.4.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 10: Return codes for the DELETE FILE command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
94 04	- File ID not found
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" or P2 ≠ "00"
67 XX	- L_c ≠ "02" + X
90 00	- Normal ending (ACK) of the command

RC_DF_VA_01 subclause 9.4.6 c19_4

Purpose

Check that DELETE FILE returns "90 00" if used correctly.

Preconditions

- The AC for DELETE FILE is PRO.
- A random has been asked for.

Test

Present a DELETE FILE command with an ID of an existing EF and a valid cryptogram.

Result

The expected status word is "90 00".

RC_DF_IV_01 subclause 9.4.6 c19_4

Purpose

Check that DELETE FILE returns "98 02" if the key associated with the AC DELETE FILE does not exist.

Preconditions

- The AC for DELETE FILE is PRO.
- A random has been asked for.
- The key associated with the AC DELETE FILE does not exist.

Test

Present a DELETE FILE command with an ID of an existing EF and any cryptogram.

Result

The expected status word is "98 02".

RC_DF_IV_02 subclause 9.4.6 c19_4

Purpose

Check that DELETE FILE returns "98 04" if the AC for DELETE FILE is not fulfilled.

Preconditions

- The AC for DELETE FILE is PRO.
- A random has been asked for.

Test

Present a DELETE FILE command with an ID of an existing EF and a wrong cryptogram.

Result

The expected status word is "98 04".

RC_DF_IV_03 subclause 9.4.6 c19_4

Purpose

Check that DELETE FILE returns "98 10" if the parent DF is invalidated.

Preconditions

- The AC for DELETE FILE is PRO.
- A random has been asked for.
- The parent DF is invalidated.

Test

Present a DELETE FILE command with an ID of an existing EF and a valid cryptogram.

Result

The expected status word is "98 10".

RC_DF_IV_04 subclause 9.4.6 c19_4

Purpose

Check that DELETE FILE returns "98 35" if no random has been asked for.

Preconditions

- The AC for DELETE FILE is PRO.
- No random has been asked for.

Test

Present a DELETE FILE command with an ID of an existing EF and a valid cryptogram.

Result

The expected status word is "98 35".

RC_DF_IV_05 subclause 9.4.6 c19_4

Purpose

Check that DELETE FILE returns "92 0X" if the internal retry routine has been used.

Preconditions

- The AC for DELETE FILE is PRO.
- A random has been asked for.
- The internal memory can only be written after X retries.

Test

Present a DELETE FILE command with an ID of an existing EF and a valid cryptogram.

Result

The expected status word is "92 0X".

RC_DF_IV_06 subclause 9.4.6 c19_4

Purpose

Check that DELETE FILE returns "92 40" if the internal memory can not be written.

Preconditions

- The AC for DELETE FILE is PRO.
- A random has been asked for.
- The internal memory can not be written.

Test

Present a DELETE FILE command with an ID of an existing EF and a valid cryptogram.

Result

The expected status word is "92 40".

RC_DF_IV_07 subclause 9.4.6 c19_4

Purpose

Check that DELETE FILE returns "94 04" if the file ID could not be found.

Preconditions

- The AC for DELETE FILE is PRO.
- A random has been asked for.

Test

Present a DELETE FILE command with an ID of a not existing EF and a valid cryptogram.

Result

The expected status word is "94 04".

RC_DF_IV_08 subclause 9.4.6 c19_4

Purpose

Check that DELETE FILE returns "6B XX" if P1 ≠ "00" or P2 ≠ "00".

Preconditions

- The AC for DELETE FILE is PRO.
- A random has been asked for.

Test

Present a DELETE FILE command with an ID of an existing EF, a valid cryptogram and P1 ≠ "00" or P2 ≠ "00".

Result

The expected status word is "6B XX".

RC_DF_IV_09 subclause 9.4.6 c19_4

Purpose

Check that DELETE FILE returns "67 XX" if L_c ≠ "02" + X.

Preconditions

- The AC for DELETE FILE is PRO.
- A random has been asked for.

Test

Present a DELETE FILE command with an ID of an existing EF, a valid cryptogram and $L_c \neq 2 + X$.

Result

The expected status word is "67 XX".

6.2.3.5 EXTEND (ET)

6.2.3.5.1 Function

FU_ET_VA_01 subclause 8.5 c19_5, c23_5, c23_1

Purpose

Check that the EXTEND function can be performed successfully to extend an EF.

Preconditions

- Extendable EF exists in current DF;

Test

Perform an EXTEND command to extend the EF. Check by means of the SELECT command whether the extension was successful.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command was performed shall be in accordance with the data provided by the EXTEND command.

FU_ET_VA_02 subclause 8.5 c19_5, c23_5, c23_1

Purpose

Check that the EXTEND function can be performed successfully to extend a DF.

Preconditions

- Extendable DF exists in current DF;

Test

Perform an EXTEND command to extend the DF. Check by means of the SELECT command whether the extension was successful.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command was performed shall be in accordance with the data provided by the EXTEND command.

6.2.3.5.2 Command

The coding of the EXTEND command is the following:

Table 11: Return codes for the EXTEND command

CLA	Class byte
INS	"D4"
P1	Initialization value
P2	Type of extension
L_c field	Length of data field
Data field	File ID and number of bytes to extend (+cryptogram)
L_e field	Empty

CO_ET_VA_01 subclause 9.3 c23_5, c23_1, c6_2

Purpose
Check that the EXTEND command can be performed successfully to extend a linear fixed structure EF.

Preconditions
- Current EF has linear fixed structure and can be extended;

Test
Perform a EXTEND command to extend a linear fixed structure EF. Check by means of the SELECT command whether the EF has been extended.

Result
Both commands shall have a positive return code and the data returned by the card after the SELECT command was performed shall be in accordance with the data provided by the EXTEND command.

CO_ET_VA_02 subclause 9.3 c23_5, c23_1, c6_3

Purpose
Check that the EXTEND command can be performed successfully to extend a linear variable structure EF.

Preconditions
- Current EF has linear variable structure and can be extended;

Test
Perform a EXTEND command to extend a linear variable structure EF. Check by means of the SELECT command whether the EF has been extended.

Result
Both commands shall have a positive return code and the data returned by the card after the SELECT command was performed shall be in accordance with the data provided by the EXTEND command.

CO_ET_VA_03 subclause 9.3 c23_5, c23_1, c6_1, c9_1, c23_10

Purpose
Check that the EXTEND command can be performed successfully to extend a transparent EF and to fill the extension with an arbitrary value.

Preconditions
- Current EF is transparent and can be extended;

Test
Perform a EXTEND command to extend a transparent EF and to fill the extension with an arbitrary value. Check by means of the SELECT command whether the EF has been extended and by means of a READ BINARY whether the contents of the file matches the given value.

Result
All commands shall have a positive return code and the data returned by the card after the SELECT and READ BINARY commands are performed shall be in accordance with the data provided by the EXTEND command.

CO_ET_VA_04 subclause 9.3 c23_5, c23_1, c6_2, c23_12

Purpose
Check that the EXTEND command can be performed successfully to extend a linear fixed EF to be filled with records with an arbitrary value.

Preconditions
- Current EF has linear fixed structure and can be extended;

Test

Perform a EXTEND command to extend a linear fixed EF and to fill the extension with an arbitrary value. Check by means of the SELECT command whether the EF has been extended and by means of a READ RECORD command whether the number of records and contents of the file match.

Result

All commands shall have a positive return code and the data returned by the card after the SELECT and READ RECORD commands are performed shall be in accordance with the data provided by the EXTEND command.

CO_ET_VA_05 subclause 9.3 c23_5, c23_1, c6_1

Purpose

Check that the EXTEND command can be performed successfully to largely extend a transparent EF.

Preconditions

- Current EF is transparent can be extended;

Test

Perform a EXTEND command to largely extend a transparent EF. Check by means of the SELECT command whether the EF has been extended.

Result

Both commands shall have a positive return code and the data returned by the card after the SELECT command is performed shall be in accordance with the data provided by the EXTEND command.

6.2.3.5.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 12: Return codes for the EXTEND command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
92 0X	- Update successful but after using internal retry routine X times
92 10	- Insufficient memory space available
92 40	- Update impossible (memory problem)
94 08	- Current file is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" or P2 ≠ "00"
67 XX	- L_c ≠ "03" + X
90 00	- Normal ending (ACK) of the command

RC_ET_VA_01 subclause 9.4.6 c19_5

Purpose

Check that EXTEND returns "90 00" if used correctly.

Preconditions

- The AC for EXTEND FILE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.

Test

Present an EXTEND command with a valid cryptogram.

Result

The expected status word is "90 00".

RC_ET_IV_01 subclause 9.4.6 c19_5

Purpose

Check that EXTEND returns "98 02" if the key associated with the AC EXTEND FILE does not exist.

Preconditions

- The AC for EXTEND FILE is PRO.
- The key associated with the AC EXTEND FILE does not exist.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.

Test

Present an EXTEND command with any cryptogram.

Result

The expected status word is "98 02".

RC_ET_IV_02 subclause 9.4.6 c19_5

Purpose

Check that EXTEND returns "98 04" if the AC for EXTEND FILE is not fulfilled.

Preconditions

- The AC for EXTEND is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.

Test

Present an EXTEND command with a wrong cryptogram.

Result

The expected status word is "98 04".

RC_ET_IV_03 subclause 9.4.6 c19_5, c9_1

Purpose

Check that EXTEND returns "98 10" if the DF is invalidated.

Preconditions

- The AC for EXTEND FILE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.
- The current DF is invalidated.

Test

Present an EXTEND command with a valid cryptogram.

Result

The expected status word is "98 10".

RC_ET_IV_04 subclause 9.4.6 c19_5

Purpose

Check that EXTEND returns "98 35" if no random has been asked for.

Preconditions

- The AC for EXTEND FILE is PRO.
- No random has been asked for.
- Enough memory for the file creation is available under the current DF.

Test

Present an EXTEND command with any cryptogram.

Result

The expected status word is "98 35".

RC_ET_IV_05 subclause 9.4.6 c19_5

Purpose

Check that EXTEND returns "92 0X" if the internal retry routine has been used.

Preconditions

- The AC for EXTEND FILE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.
- The internal memory can only be written after X retries.

Test

Present an EXTEND command with a valid cryptogram.

Result

The expected status word is "92 0X".

RC_ET_IV_06 subclause 9.4.6 c19_5

Purpose

Check that EXTEND returns "92 10" if the available memory is not sufficient.

Preconditions

- The AC for EXTEND FILE is PRO.
- A random has been asked for.
- There is not enough memory under the current DF available to create the file.

Test

Present an EXTEND command with a valid cryptogram.

Result

The expected status word is "92 10".

RC_ET_IV_07 subclause 9.4.6 c19_5

Purpose

Check that EXTEND returns "92 40" if the internal memory can not be written.

Preconditions

- The AC for EXTEND FILE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.
- The internal memory can not be written.

Test

Present an EXTEND command with a valid cryptogram.

Result

The expected status word is "92 40".

RC_ET_IV_08 subclause 9.4.6 c19_5

Purpose

Check that EXTEND returns "94 08" if it is performed on a cyclic EF.

Preconditions

- Any cyclic EF within the current DF exists.

Test

Present an EXTEND command with file ID = cyclic EF file ID.

Result

The expected status word is "94 08".

RC_ET_IV_09 subclause 9.4.6 c19_5

Purpose

Check that EXTEND returns "6B XX" if P1 ≠ "00" or P2 ≠ "00".

Preconditions

- The AC for EXTEND FILE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.

Test

Present an EXTEND command with a valid cryptogram and P1 ≠ "00" or P2 ≠ "00".

Result

The expected status word is "6B XX".

RC_ET_IV_10 subclause 9.4.6 c19_5

Purpose
Check that EXTEND returns "67 XX" if L_c > "03" + X.

Preconditions
- The AC for EXTEND FILE is PRO.
- A random has been asked for.
- Enough memory for the file creation is available under the current DF.

Test
Present an EXTEND command with a valid cryptogram and $L_c \neq$ "03" + X.

Result
The expected status word is "67 XX".

RC_ET_IV_11 subclause 9.4.6 c19_5

Purpose
Check that EXTEND returns an error when it is used for a non existing file

Preconditions
- None

Test
Present an EXTEND command with a file ID that does not exist.

Result
The expected status word is any negative.

6.2.3.6 EXECUTE (EX)

6.2.3.6.1 Function

FU_EX_VA_01 subclause 8.6 c19_6, c23_6

Purpose
Check that the card is able to perform an EXECUTE function.

Preconditions
- An EF containing a program exists.

Test
Present an EXECUTE command.

Result
The expected status word is "90 00".

NOTE: It might be necessary to perform additional implementation specific tests.

Specification for this is under responsibility of the development team.

6.2.3.6.2 Command

The coding of the EXECUTE command is the following:

Table 13: Return codes for the EXECUTE command

CLA	Class byte
INS	"AE"
P1	"00" (other values are RFU)
P2	"00" (other values are RFU)
L_c field	Number of data bytes (+X)
Data field	Data sent to the card (+X)
L_e field	Empty

No tests are foreseen to test the EXECUTE command other than those defined in the functions subclause.

6.2.3.6.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 14: Return codes for the EXECUTE command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
94 00	- No EF selected as current
94 08	- Current file type is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ 0 or P2 ≠ 0
67 XX	- no test is foreseen for this status word
92 40	- no test is foreseen for this status word
90 00	- Normal ending (ACK) of the command
9F XX	- Length "XX" of the response data

RC_EX_VA_01 subclause 9.4.6 c19_6, c4_9

Purpose

Check that EXECUTE returns "90 00" if used correctly.

Preconditions

- An EF containing a program is selected.
- The AC for EXECUTE is fulfilled, no cryptogram is required.
- The data format needed is known.

Test
Present a valid EXECUTE command.

Result
The expected status word is "90 00".

RC_EX_VA_02 subclause 9.4.6 c19_6, c4_8

Purpose
Check that EXECUTE returns "9F XX" if used correctly.

Preconditions
- An EF containing a program is selected.
- The AC for EXECUTE is fulfilled, no cryptogram is required.
- The data format needed is known.

Test
Present a valid EXECUTE command.

Result
The expected status word is "9F XX".

RC_EX_IV_01 subclause 9.4.6 c19_6

Purpose
Check that EXECUTE returns "98 02" if the key associated with the file does not exist.

Preconditions
- An EF containing a program with a not existing key associated to EXECUTE is selected.
- The AC for EXECUTE is PRO.
- The data format needed is known.
- A random has been asked for.

Test
Present a valid EXECUTE command with any cryptogram appended and a matching L_c.

Result
The expected status word is "98 02".

RC_EX_IV_02 subclause 9.4.6 c19_6

Purpose
Check that EXECUTE returns "98 04" if the selected file has an unfulfilled access condition on EXECUTE.

Preconditions
- An EF containing a program is selected.
- The AC for EXECUTE is not fulfilled.
- The data format needed is known.

Test

Present a valid EXECUTE command.

Result

The expected status word is "98 04".

RC_EX_IV_03 subclause 9.4.6 c19_6

Purpose

Check that EXECUTE returns "98 10" if the selected file is invalidated.

Preconditions

- An invalidated EF containing a program is selected.
- The AC for EXECUTE is fulfilled, no cryptogram is required.
- The data format needed is known.

Test

Present a valid EXECUTE command.

Result

The expected status word is "98 10".

RC_EX_IV_04 subclause 9.4.6 c19_6

Purpose

Check that EXECUTE returns "98 35" if no random has been asked for.

Preconditions

- An EF containing a program is selected.
- The AC for EXECUTE is PRO.
- The data format needed is known.
- No random has been asked for.

Test

Present a valid EXECUTE command with any cryptogram appended and a matching L_c.

Result

The expected status word is "98 35".

RC_EX_IV_05 subclause 9.4.6 c19_6

Purpose

Check that EXECUTE returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.

Test

Present a valid EXECUTE command.

Result

The expected status word is "94 00".

RC_EX_IV_06 subclause 9.4.6 c19_6

Purpose

Check that EXECUTE returns "94 08" if a file, not containing a program is selected.

Preconditions

- EF_{ICC} is selected.

Test

Present a valid EXECUTE command.

Result

The expected status word is "94 08".

RC_EX_IV_07 subclause 9.4.6 c19_6

Purpose

Check that EXECUTE returns "6B XX" if P1 ≠ "00" or P2 ≠ "00".

Preconditions

- An EF containing a program is selected.
- The AC for EXECUTE is fulfilled, no cryptogram is required.
- The data format needed is known.

Test

Present an EXECUTE command with P1 ≠ "00" or P2 ≠ "00".

Result

The expected status word is "6B XX".

6.2.3.7 UPDATE BINARY (UB)

6.2.3.7.1 Function

FU_UB_VA_01 subclause 8.7 c19_7, c23_7, c23_1, c23_10

Purpose

Check that the UPDATE BINARY function can be performed.

Preconditions

- Writable transparent EF selected;

Test

Try to write a number of bytes to the EF. Then try to read them back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ BINARY command was performed shall be in accordance with the data written in that EF by the UPDATE BINARY command.

FU_UB_IV_01 subclause 8.7 c19_7, c23_7, c23_1, c23_10

Purpose

Check that UPDATE BINARY does not write into the EF if AC is not fulfilled.

Preconditions

- A transparent EF with known contents is selected.
- The AC for UPDATE is not fulfilled, no cryptogram is required.

Test

Present an UPDATE BINARY command with offset "0000", that is P1 = "00", P2 = "00" and L_c = "01".

Check by means of READ BINARY if file contents did not change.

Result

The expected status word for UPDATE BINARY is "98 04" while the READ BINARY returns a positive return code and the unchanged file contents.

6.2.3.7.2 Command

The coding of the UPDATE BINARY command is the following:

Table 15: Return codes for the UPDATE BINARY command

CLA	Class byte
INS	"D6"
P1	Offset
P2	Offset
L_c field	Length of data field
Data field	Data to be updated (+cryptogram)
L_e field	Empty

CO_UB_VA_01 subclause 9.7 c23_7, c23_1, c23_10

Purpose

Check that the UPDATE BINARY command can be performed using a small offset.

Preconditions

- Writable transparent non-empty (at least 48 bytes) EF (with known contents) selected;

Test

Try to write a number of bytes to the EF using offset "1A". Then try to read them back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ BINARY command was performed shall be in accordance with the data written in that EF by the UPDATE BINARY command.

CO_UB_VA_02 subclause 9.7 c23_7, c23_1, c23_10

Purpose

Check that the UPDATE BINARY command can be performed using a large offset.

Preconditions

- Writable transparent non-empty (at least 300 bytes) EF (with known contents) selected;

Test

Try to write a number of bytes to the EF using offset "0120". Then try to read them back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ BINARY command was performed shall be in accordance with the data written in that EF by the UPDATE BINARY command.

CO_UB_VA_03 subclause 9.7 c23_7, c23_1, c23_10

Purpose

Check that the UPDATE BINARY command can be performed using a large amount of data.

Preconditions

- Writable transparent non-empty (at least 256 bytes) EF (with known contents) selected;

Test

Try to write the maximum number of bytes allowed by the IUT to the EF in one UPDATE BINARY command. Then try to read them back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ BINARY command was performed shall be in accordance with the data written in that EF by the UPDATE BINARY command.

6.2.3.7.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 16: Return codes for the UPDATE BINARY command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
94 00	- No EF selected as current
94 02	- Out of range (invalid address)
94 08	- Current file type is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- (P1, P2) > file length
67 XX	- (P1, P2) + L_c > file length
90 00	- Normal ending (ACK) of the command

RC_UB_VA_01 subclause 9.4.6 c19_7, c4_9

Purpose

Check that UPDATE BINARY returns "90 00" if used correctly.

Preconditions

- A transparent EF is selected.
- The AC for UPDATE is fulfilled, no cryptogram is required.

Test

Present an UPDATE BINARY command with P1 = "00", P2 = "00" and L_c = "01".

Result

The expected status word is "90 00".

RC_UB_IV_01 subclause 9.4.6 c19_7

Purpose

Check that UPDATE BINARY returns "98 02" if the key associated with the file does not exist.

Preconditions

- A transparent EF with a not existing key associated to UPDATE is selected.
- The AC for UPDATE is PRO.
- A random has been asked for.

Test

Present a UPDATE BINARY command with offset "0000", that is P1 = "00", P2 = "00", any cryptogram and L_c = "01" + X.

Result

The expected status word is "98 02".

RC_UB_IV_02 subclause 9.4.6 c19_7

Purpose

Check that UPDATE BINARY returns "98 04" if the selected file has an unfulfilled access condition on UPDATE.

Preconditions

- A transparent EF is selected.
- The AC for UPDATE is not fulfilled, no cryptogram is required.

Test

Present an UPDATE BINARY command with offset "0000", that is P1 = "00", P2 = "00" and L_c = "01".

Result

The expected status word is "98 04".

RC_UB_IV_03 subclause 9.4.6 c19_7

Purpose

Check that UPDATE BINARY returns "98 10" if the selected file is invalidated.

Preconditions

- A transparent invalidated EF is selected.
- The AC for UPDATE is fulfilled, no cryptogram is required.

Test

Present a UPDATE BINARY command with offset "0000", that is P1 = "00", P2 = "00" and L_c = "01".

Result

The expected status word is "98 10".

RC_UB_IV_04 subclause 9.4.6 c19_7

Purpose

Check that UPDATE BINARY returns "98 35" if no random has been asked for.

Preconditions

- A transparent EF is selected.
- The AC for UPDATE is PRO.
- No random has been asked for.

Test

Present a UPDATE BINARY command with offset "0000", that is P1 = "00", P2 = "00", any cryptogram and L_c = "01" + X.

Result

The expected status word is "98 35".

RC_UB_IV_05 subclause 9.4.6 c19_7

Purpose

Check that UPDATE BINARY returns "92 0X" if the internal retry routine has been used.

Preconditions

- A transparent EF is selected.
- The AC for UPDATE is fulfilled, no cryptogram is required.
- The internal memory can only be written after X retries.

Test

Present an UPDATE BINARY command with P1 = "00", P2 = "00" and L_c = "01".

Result

The expected status word is "92 0X".

RC_UB_IV_06 subclause 9.4.6 c19_7

Purpose

Check that UPDATE BINARY returns "92 40" if the internal memory can not be written.

Preconditions

- A transparent EF is selected.
- The AC for UPDATE is fulfilled, no cryptogram is required.
- The internal memory can not be written.

Test

Present an UPDATE BINARY command with P1 = "00", P2 = "00" and L_c = "01".

Result

The expected status word is "92 40".

RC_UB_IV_07 subclause 9.4.6 c19_7

Purpose

Check that UPDATE BINARY returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.

Test

Present an UPDATE BINARY command with offset "0000", that is P1 = "00", P2 = "00" and L_c = "01".

Result

The expected status word is "94 00".

RC_UB_IV_08 subclause 9.4.6 c19_7

Purpose

Check that UPDATE BINARY returns "94 08" if a file, not valid for UPDATE BINARY is selected.

Preconditions

- Any linear fixed EF is selected.

Test

Present an UPDATE BINARY command with offset "0000", that is P1 = "00", P2 = "00" and L_c = "01".

Result

The expected status word is "94 08".

RC_UB_IV_09 subclause 9.4.6 c19_7

Purpose

Check that UPDATE BINARY returns "6B XX" or "94 02" if the offset is greater than the file size.

Preconditions

- A transparent EF is selected.
- The AC for UPDATE is fulfilled, no cryptogram is required.
- The length of the file is 20 byte.

Test

Present a UPDATE BINARY command with offset "0014", that is P1 = "00", P2 = "14" and L_c = "01".

Result

The expected status word is "6B XX" or "94 02".

RC_UB_IV_10 subclause 9.4.6 c19_7

Purpose

Check that UPDATE BINARY returns "67 XX" or "94 02" if the sum of the offset and the length is larger than the file size.

Preconditions

- A transparent EF is selected.
- The AC for UPDATE is fulfilled, no cryptogram is required.
- The length of the file is 20 byte.

Test

Present a UPDATE BINARY command with offset "0013", that is P1 = "00", P2 = "13" and L_c = "02".

Result

The expected status word is "67 XX" or "94 02".

6.2.3.8 UPDATE RECORD (UR)

6.2.3.8.1 Function

FU_UR_VA_01 subclause 8.8 c19_8, c23_8, c23_1, c23_12

Purpose

Check that the UPDATE RECORD function can be performed in FIRST mode.

Preconditions

- Writable linear fixed structure EF selected;

Test

Try to write a record in FIRST mode. Then try to read them back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the UPDATE RECORD command.

FU_UR_VA_02 subclause 8.8 c19_8, c23_8, c23_1, c23_12

Purpose

Check that the UPDATE RECORD function can be performed in LAST mode.

Preconditions

- Writable linear fixed structure EF selected;

Test

Try to write a record in LAST mode. Then try to read them back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the UPDATE RECORD command.

FU_UR_VA_03 subclause 8.8 c19_8, c23_8, c23_1, c23_12

Purpose

Check that the UPDATE RECORD function can be performed in NEXT mode.

Preconditions

- Writable linear fixed structure EF selected;

- Current record is known and not first nor last record;

Test

Try to write a record in NEXT mode. Then try to read it back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the UPDATE RECORD command.

FU_UR_VA_04 subclause 8.8 c19_8, c23_8, c23_1, c23_12

Purpose

Check that the UPDATE RECORD function can be performed in PREVIOUS mode.

Preconditions

- Writable linear fixed structure EF selected;
- Current record is known and not first nor last record;

Test

Try to write a record in PREVIOUS mode. Then try to read it back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the UPDATE RECORD command.

FU_UR_VA_05 subclause 8.8 c19_8, c23_8, c23_1, c23_12

Purpose

Check that the UPDATE RECORD function can be performed in ABSOLUTE mode.

Preconditions

- Writable linear fixed structure EF selected;

Test

Try to write a record in ABSOLUTE mode. Then try to read them back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the UPDATE RECORD command.

FU_UR_VA_06 subclause 8.8 c19_8, c23_8, c23_1, c23_12

Purpose

Check that the UPDATE RECORD function can be performed in CURRENT mode.

Preconditions

- Writable linear fixed structure EF selected;
- Current record is known and not first nor last record;

Test

Try to write a record in CURRENT mode. Finally try to read them back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the UPDATE RECORD command.

FU_UR_IV_01 subclause 8.8 c19_8, c23_8, c23_1, c23_12

Purpose

Check that UPDATE RECORD does not write into the EF if AC is not fulfilled.

Preconditions

- A linear fixed EF with known contents is selected.
- The AC for UPDATE is not fulfilled, no cryptogram is required.

Test

Present an UPDATE RECORD command with P1 = "00", P2 = "03" and L_c = record length.

Check by means of READ RECORD if file contents did not change.

Result

The expected status word for UPDATE RECORD is "98 04" while the READ RECORD returns a positive return code and the unchanged file contents.

6.2.3.8.2 Command

The coding of the UPDATE RECORD command is the following:

Table 17: Return codes for the UPDATE RECORD command

CLA	Class byte
INS	"DC"
P1	Record no.
P2	Mode
L_c field	Length of data field
Data field	Data to be updated (+cryptogram)
L_e field	Empty

No tests are foreseen to test the UPDATE RECORD command other than those defined in the functions subclause.

6.2.3.8.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 18: Return codes for the UPDATE RECORD command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
94 00	- No EF selected as current
94 02	- Out of range
94 04	- Record not found
94 08	- Current file type is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P2 > "04"
67 XX	- $L_c \neq$ record length (+X)
90 00	- Normal ending (ACK) of the command

RC_UR_VA_01 subclause 9.4.6 c19_8, c4_9

Purpose

Check that UPDATE RECORD returns "90 00" if used correctly.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for UPDATE is fulfilled, no cryptogram is required.

Test

Present an UPDATE RECORD command with P1 = "00", P2 = "00" and L_c = record length.

Result

The expected status word is "90 00".

RC_UR_IV_01 subclause 9.4.6 c19_8

Purpose

Check that UPDATE RECORD returns "98 02" if the key associated with the file does not exist.

Preconditions

- An EF with linear fixed structure with a not existing key associated to UPDATE is selected.
- The AC for UPDATE is PRO.
- A random has been asked for.

Test

Present an UPDATE RECORD command with P1 = "00", P2 = "00" and L_c = record length + X.

Result

The expected status word is "98 02".

RC_UR_IV_02 subclause 9.4.6 c19_8

Purpose

Check that UPDATE RECORD returns "98 04" if the selected file has an unfulfilled access condition on UPDATE.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for UPDATE is not fulfilled, no cryptogram is required.

Test

Present an UPDATE RECORD command with P1 = "00", P2 = "00" and L_c = record length.

Result

The expected status word is "98 04".

RC_UR_IV_03 subclause 9.4.6 c19_8, c9_1

Purpose

Check that UPDATE RECORD returns "98 10" if the selected file is invalidated.

Preconditions

- An invalidated EF with linear fixed structure is selected.
- The AC for UPDATE is fulfilled, no cryptogram is required.

Test

Present an UPDATE RECORD command with P1 = "00", P2 = "00" and L_c = record length.

Result

The expected status word is "98 10".

RC_UR_IV_04 subclause 9.4.6 c19_8

Purpose

Check that UPDATE RECORD returns "98 35" if no random has been asked for.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for UPDATE is PRO.
- No random has been asked for.

Test

Present an UPDATE RECORD command with P1 = "00", P2 = "00" and L_c = record length + X.

Result

The expected status word is "98 35".

RC_UR_IV_05 subclause 9.4.6 c19_8

Purpose

Check that UPDATE RECORD returns "92 0X" if the internal retry routine has been used.

Preconditions

- An EF with linear fixed structure is selected.

- The AC for UPDATE is fulfilled, no cryptogram is required.
- The internal memory can only be written after X retries.

Test

Present an UPDATE RECORD command with P1 = "00", P2 = "00" and L_c = record length.

Result

The expected status word is "92 0X".

RC_UR_IV_06 subclause 9.4.6 c19_8

Purpose

Check that UPDATE RECORD returns "92 40" if the internal memory can not be written.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for UPDATE is fulfilled, no cryptogram is required.
- The internal memory can not be written.

Test

Present an UPDATE RECORD command with P1 = "00", P2 = "00" and L_c = record length.

Result

The expected status word is "92 40".

RC_UR_IV_07 subclause 9.4.6 c19_8

Purpose

Check that UPDATE RECORD returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.

Test

Present an UPDATE RECORD command with P1 = "00", P2 = "00" and L_c = record length.

Result

The expected status word is "94 00".

RC_UR_IV_08 subclause 9.4.6 c19_8

Purpose

Check that UPDATE RECORD returns "94 02" or "94 04" if the addressed record is not found.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for UPDATE is fulfilled, no cryptogram is required.
- The number of records in that EF is known.

Test

Present an UPDATE RECORD command with P1 > number of existing records, P2 = "04" and L_c = record length.

Result

The expected status word is "94 02" or "94 04".

RC_UR_IV_09 subclause 9.4.6 c19_8

Purpose

Check that UPDATE RECORD returns "94 08" if a file, not valid for UPDATE RECORD is selected.

Preconditions

- EF_{KEY_MAN} is selected.

Test

Present an UPDATE RECORD command with P1 = "00", P2 = "00" and L_c = record length.

Result

The expected status word is "94 08".

RC_UR_IV_10 subclause 9.4.6 c19_8

Purpose

Check that UPDATE RECORD returns "6B XX" if P2 > "04".

Preconditions

- An EF with linear fixed structure is selected.
- The AC for UPDATE is fulfilled, no cryptogram is required.

Test

Present an UPDATE RECORD command with P1 = "00", P2 > "04" and L_c = record length.

Result

The expected status word is "6B XX".

RC_UR_IV_11 subclause 9.4.6 c19_8

Purpose

Check that UPDATE RECORD returns "67 XX" if the length of the datafield is not equal to the record length.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for UPDATE is fulfilled, no cryptogram is required.

Test

Present an UPDATE RECORD command with P1 = "00", P2 = "00" and L_c = record length.

Result

The expected status word is "67 XX".

6.2.3.9 CREATE RECORD (CR)

6.2.3.9.1 Function

FU_CR_VA_01 subclause 8.9 c19_9, c23_9, c23_1, c23_12

Purpose

Check that the CREATE RECORD function can be successfully performed on a empty linear fixed structure EF.

Preconditions

- Readable empty linear fixed structure EF selected;

Test

Perform a CREATE RECORD command and then a READ RECORD in CURRENT mode.

Result

Both commands shall have a positive return code and the data returned by the READ RECORD command shall be in accordance with the data provided by the CREATE RECORD command.

FU_CR_VA_02 subclause 8.9c19_9, c23_9, c23_1, c23_12

Purpose

Check that the CREATE RECORD function can be successfully performed on a non-empty linear variable structure EF.

Preconditions

- Readable non-empty (containing at least 2 non-empty records) linear variable structure EF (with known contents) selected;

- Last created record is also last written record

Test

Perform a CREATE RECORD command and then a READ RECORD in CURRENT mode.

Result

Both commands shall have a positive return code and the data returned by the READ RECORD command shall be in accordance with the data provided by the CREATE RECORD command.

FU_CR_VA_03 subclause 8.9 c19_9, c23_9, c23_1, c23_12

Purpose

Check that the CREATE RECORD function can be successfully performed on a non-empty cyclic EF.

Preconditions

- Readable non-empty (containing at least 2 non-empty records) cyclic EF (with known contents) selected;

- Last created record is also last written record

Test

Perform a CREATE RECORD command and then a READ RECORD in CURRENT mode.

Result

Both commands shall have a positive return code and the data returned by the READ RECORD command shall be in accordance with the data provided by the CREATE RECORD command.

FU_CR_IV_01 subclause 8.9 c19_9, c23_9, c23_1

Purpose

Check that the CREATE RECORD function cannot be successfully performed on a non-empty cyclic EF when the last created record is not the last written record.

Preconditions

- Readable non-empty (containing at least 2 non-empty records) cyclic EF (with known contents) selected;
- Last created record is not last written record

Test

Perform a CREATE RECORD command.

Result

The commands shall have a negative return code.

6.2.3.9.2 Command

The coding of the CREATE RECORD command is the following:

Table 19: Return codes for the CREATE RECORD command

CLA	Class byte
INS	"E2"
P1	"00"
P2	"00"
L_c field	Empty or Length of data field
Data field	Data of record to be created (+ cryptogram)
L_e field	Empty

6.2.3.9.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 20: Return codes for the CREATE RECORD command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
94 00	- No EF selected as current
94 02	- Out of range
94 08	- Current file type is inconsistent with the command
92 0X	- Update successful but after using internal retry routine X times
92 10	- Insufficient memory space available
92 40	- Update impossible (memory problem)
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" or P2 ≠ "00"
67 XX	- L_c ≠ record length +X
90 00	- Normal ending (ACK) of the command

RC_CR_VA_01 subclause 9.4.6 c19_9

Purpose
Check that CREATE RECORD returns "90 00" if used correctly.

Preconditions
- An EF with linear fixed structure is selected.
- The AC for CREATE RECORD is PRO.
- A random has been asked for.
- Enough memory for the record creation is available in the current file.

Test
Present an CREATE RECORD command with a valid cryptogram.

Result
The expected status word is "90 00".

RC_CR_IV_01 subclause 9.4.6 c19_9

Purpose
Check that CREATE RECORD returns "98 02" if the key associated with the AC CREATE RECORD does not exist.

Preconditions
- An EF with linear fixed structure is selected.
- The AC for CREATE RECORD is PRO.
- The key associated with the AC CREATE RECORD does not exist.
- A random has been asked for.
- Enough memory for the record creation is available in the current file.

Test

Present a CREATE RECORD command with any cryptogram.

Result

The expected status word is "98 02".

RC_CR_IV_02 subclause 9.4.6 c19_9

Purpose

Check that CREATE RECORD returns "98 04" if the AC for CREATE RECORD is not fulfilled.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for CREATE RECORD is PRO.
- A random has been asked for.
- Enough memory for the record creation is available in the current file.

Test

Present a CREATE RECORD command with a wrong cryptogram.

Result

The expected status word is "98 04".

RC_CR_IV_03 subclause 9.4.6 c19_9

Purpose

Check that CREATE RECORD returns "98 10" if the EF is invalidated.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for CREATE RECORD is PRO.
- A random has been asked for.
- Enough memory for the record creation is available in the current file.
- The current EF is invalidated.

Test

Present an CREATE RECORD command with a valid cryptogram.

Result

The expected status word is "98 10".

RC_CR_IV_04 subclause 9.4.6 c19_9

Purpose

Check that CREATE RECORD returns "98 35" if no random has been asked for.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for CREATE RECORD is PRO.
- No random has been asked for.
- Enough memory for the record creation is available in the current file.

Test

Present an CREATE RECORD command with any cryptogram.

Result

The expected status word is "98 35".

RC_CR_IV_05 subclause 9.4.6 c19_9

Purpose

Check that CREATE RECORD returns "92 0X" if the internal retry routine has been used.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for CREATE RECORD is PRO.
- A random has been asked for.
- Enough memory for the record creation is available in the current file.
- The internal memory can only be written after X retries.

Test

Present an CREATE RECORD command with a valid cryptogram.

Result

The expected status word is "92 0X".

RC_CR_IV_06 subclause 9.4.6 c19_9

Purpose

Check that CREATE RECORD returns "92 10" if the available memory is not sufficient.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for CREATE RECORD is PRO.
- A random has been asked for.
- There is not enough memory for the record creation available in the current file.

Test

Present an CREATE RECORD command with a valid cryptogram.

Result

The expected status word is "92 10".

RC_CR_IV_07 subclause 9.4.6 c19_9

Purpose

Check that CREATE RECORD returns "92 40" if the internal memory can not be written.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for CREATE RECORD is PRO.
- A random has been asked for.
- Enough memory for the record creation is available in the current file.
- The internal memory can not be written.

Test

Present an CREATE RECORD command with a valid cryptogram.

Result

The expected status word is "92 40".

RC_CR_IV_08 subclause 9.4.6 c19_9

Purpose

Check that CREATE RECORD returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.
- A random has been asked for.
- Enough memory for the record creation is available in the current file.

Test

Present an CREATE RECORD command with a valid cryptogram for any record length.

Result

The expected status word is "94 00".

RC_CR_IV_09 subclause 9.4.6 c19_9

Purpose

Check that CREATE RECORD returns "94 02" if the number of records would exceed 255.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for CREATE RECORD is PRO.
- A random has been asked for.
- Enough memory for the record creation is available in the current file.
- The number of records in that EF is 255.

Test

Present an CREATE RECORD command with a valid cryptogram.

Result

The expected status word is "94 02".

RC_CR_IV_10 subclause 9.4.6 c19_9

Purpose

Check that CREATE RECORD returns "94 08" if a file, not valid for CREATE RECORD is selected.

Preconditions

- EF_{ICC} is selected.
- A random has been asked for.
- Enough memory for the record creation is available in the current file.

Test

Present an CREATE RECORD command with any cryptogram.

Result

The expected status word is "94 08".

RC_CR_IV_11 subclause 9.4.6 c19_9

Purpose

Check that CREATE RECORD returns "6B XX" if P1 ≠ "00" or P2 ≠ "00".

Preconditions

- An EF with linear fixed structure is selected.
- The AC for CREATE RECORD is PRO.
- A random has been asked for.
- Enough memory for the record creation is available in the current file.

Test

Present an CREATE RECORD command with a valid cryptogram and P1 ≠ "00" or P2 ≠ "00".

Result

The expected status word is "6B XX".

RC_CR_IV_12 subclause 9.4.6 c19_9

Purpose

Check that CREATE RECORD returns "67 XX" if L_c > record length + X.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for CREATE RECORD is PRO.
- A random has been asked for.
- Enough memory for the record creation is available in the current file.

Test

Present an CREATE RECORD command with a valid cryptogram and L_c > record length + X.

Result

The expected status word is "67 XX".

6.2.3.10 READ BINARY (RB)

6.2.3.10.1 Function

FU_RB_VA_01 subclause 8.10 c19_10, c23_10, c23_1

Purpose

Check that the READ BINARY function can be performed.

Preconditions

- Readable transparent non-empty EF (with known contents) selected;

Test

Try to read a number of bytes from the EF.

Result

The READ BINARY command shall have a positive return code and the data returned by the command shall be in accordance with the actual contents of that EF.

FU_RB_VA_02 subclause 8.10 c19_10, c23_10, c23_1, c9_1

Purpose

Check that the READ BINARY function can be performed on invalidated and readable when invalidated files.

Preconditions

- Readable transparent non-empty EF (with known contents) selected;
- file is invalidated:
- file is readable when invalidated

Test

Try to read a number of bytes from the EF.

Result

The READ BINARY command shall have a positive return code and the data returned by the command shall be in accordance with the actual contents of that EF.

6.2.3.10.2 Command

The coding of the READ BINARY command is the following:

Table 21: Return codes for the READ BINARY command

CLA	Class byte
INS	"B0"
P1	Offset
P2	Offset
L_c field	Empty
Data field	Empty
L_e field	Number of bytes to be read

CO_RB_VA_01 subclause 9.10 c23_10, c23_1

Purpose

Check that the READ BINARY command can be performed using a small offset.

Preconditions

- Readable transparent non-empty (at least 48 bytes) EF (with known contents) selected;

Test

Try to read a number of bytes from the EF using offset "1A".

Result

The READ BINARY command shall have a positive return code and the data returned by the command shall be in accordance with the actual contents of that EF.

CO_RB_VA_02 subclause 9.10 c23_10, c23_1

Purpose

Check that the READ BINARY command can be performed using a large offset.

Preconditions

- Readable transparent non-empty (at least 300 bytes) EF (with known contents) selected;

Test

Try to read a number of bytes from the EF using offset "0120".

Result

The READ BINARY command shall have a positive return code and the data returned by the command shall be in accordance with the actual contents of that EF.

6.2.3.10.3 Return codes

Table 22: Return codes for the READ BINARY command

Return Code	Error description
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
92 40	- no test is foreseen for this status word
94 00	- No EF selected as current
94 02	- Out of range (invalid address) (ed. 2)
94 08	- Current file type is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- (P1, P2) > file length
67 XX	- no test is foreseen for this status word
90 00	- Normal ending (ACK) of the command

RC_RB_VA_01 subclause 9.4.6 c19_10, c4_9

Purpose

Check that READ BINARY returns "90 00" if used correctly.

Preconditions

- EF_{ICC} is selected.

Test

Present a READ BINARY command with P1 = "00", P2 = "00" and L_e = "0F".

Result

The expected status word is "90 00".

RC_RB_IV_01 subclause 9.4.6 c19_10

Purpose

Check that READ BINARY returns "98 04" if the selected file has an unfulfilled access condition on read.

Preconditions

- An EF with AC for READ is set to NEV or any other unfulfilled AC is selected, such as EFCHV or EFDIR.

Test

Present a READ BINARY command with offset "0000", that is P1 = "00" and P2 = "00" and L_e = "01".

Result

The expected status word is "98 04".

RC_RB_IV_02 subclause 9.4.6 c19_10

Purpose

Check that READ BINARY returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.

Test

Present a READ BINARY command with offset "0000".

Result

The expected status word is "94 00".

RC_RB_IV_03 subclause 9.4.6 c19_10, c9_1

Purpose

Check that READ BINARY returns "98 10" if the selected file is invalidated.

Preconditions

- A transparent invalidated EF is selected.
- That EF is not readable when invalidated.

Test

Present a READ BINARY command with offset "0000", that is P1 = "00" and P2 = "00" and L_e = "01".

Result

The expected status word is "98 10".

RC_RB_IV_04 subclause 9.4.6 c19_10

Purpose

Check that READ BINARY returns "94 08" if a file, not valid for READ BINARY is selected.

Preconditions

- EF_{KEY_MAN} is selected.

Test

Present a READ BINARY command with offset "0000".

Result

The expected status word is "94 08".

RC_RB_IV_05 subclause 9.4.6 c19_10

Purpose

Check that READ BINARY returns "6B XX" or "94 02" if the offset is greater than the file size.

Preconditions

- EF_{ICC} is selected.

Test

Present a READ BINARY command with offset "0014", that is P1 = "00" and P2 = "14" and L_e = "01".

Result

The expected status word is "6B XX".

6.2.3.11 READ BINARY STAMPED (RBS)

6.2.3.11.1 Function

FU_RBS_VA_01 subclause 8.11 c19_11, c23_11, c23_1, c23_24

Purpose

Check that the READ BINARY STAMPED function can be performed.

Preconditions

- Readable transparent non-empty EF (with known contents) selected;

- A random has been given.

Test

Try to read a number of bytes from the EF.

Result

The READ BINARY STAMPED command shall have a positive return code, the data returned by the command shall be in accordance with the actual contents of that EF and the returned cryptogram shall be correct.

6.2.3.11.2 Command

The coding of the READ BINARY STAMPED command is the following:

Table 23: Return codes for the READ BINARY STAMPED command

CLA	Class byte
INS	"B4"
P1	Offset
P2	Offset
L_c field	Empty
Data field	Empty
L_e field	Number of bytes to be read

CO_RBS_VA_01 subclause 9.2.11 c23_11, c23_1, c23_24

Purpose

Check that the READ BINARY STAMPED command can be performed using a small offset.

Preconditions

- Readable transparent non-empty (at least 48 bytes) EF (with known contents) selected;
- A random has been given.

Test

Try to read a number of bytes from the EF using offset "0A".

Result

The READ BINARY STAMPED command shall have a positive return code, the data returned by the command shall be in accordance with the actual contents of that EF and the cryptogram shall be correct.

CO_RBS_VA_02 subclause 9.2.11 c23_11, c23_1, c23_24

Purpose

Check that the READ BINARY STAMPED command can be performed using a large offset.

Preconditions

- Readable transparent non-empty (at least 300 bytes) EF (with known contents) selected;
- A random has been given.

Test

Try to read a number of bytes from the EF using offset "0120".

Result

The READ BINARY STAMPED command shall have a positive return code, the data returned by the command shall be in accordance with the actual contents of that EF and the cryptogram shall be correct.

6.2.3.11.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 24: Return codes for the READ BINARY STAMPED command

Return Code	Error description
98 02	– No key defined
98 04	– AC not fulfilled
98 10	– In contradiction with the invalidation status
98 35	– No ASK RANDOM / GIVE RANDOM before
92 40	– no test is foreseen for this status word
94 00	– No EF selected as current
94 02	– Out of range (invalid address) (note)
94 08	– Current file type is inconsistent with the command
6E XX	– Wrong instruction class given in the command
6D XX	– Unknown instruction code given in the command
6F XX	– Technical problem with no diagnostic given (command aborted)
6B XX	– (P1, P2) > file length
67 XX	– no test is foreseen for this status word
90 00	– Normal ending (ACK) of the command
NOTE: This error code shall not be used, but 6B XX instead. (CR)	

RC_RBS_VA_01 subclause 9.4.6 c19_11, c4_9

Purpose

Check that READ BINARY STAMPED returns "90 00" if used correctly.

Preconditions

- EF_{ICC} is selected.
- A random has been given.

Test

Present a READ BINARY STAMPED command with P1 = "00", P2 = "00" and L_e = "0F" + X.

Result

The expected status word is "90 00".

RC_RBS_IV_01 subclause 9.4.6 c19_11

Purpose

Check that READ BINARY STAMPED returns "98 02" if the key associated with the file does not exist.

Preconditions

- A transparent EF with a not existing key associated to READ is selected.
- A random has been given.

Test

Present a READ BINARY STAMPED command with offset "0000", that is P1 = "00" and P2 = "00" and

L_e = "01" + X.

Result

The expected status word is "98 02".

RC_RBS_IV_02 subclause 9.4.6 c19_11

Purpose

Check that READ BINARY STAMPED returns "98 04" if the selected file has an unfulfilled access condition on read.

Preconditions

- An EF with AC for READ is set to NEV or any other unfulfilled AC is selected, such as EFCHV or EFDIR.
- A random has been given.

Test

Present a READ BINARY STAMPED command with offset "0000", that is P1 = "00" and P2 = "00" and

L_e = "01" + X.

Result

The expected status word is "98 04".

RC_RBS_IV_03 subclause 9.4.6 c19_11

Purpose

Check that READ BINARY STAMPED returns "98 10" if the selected file is invalidated.

Preconditions

- A transparent invalidated EF is selected.
- That EF is not readable when invalidated.
- A random has been given.

Test

Present a READ BINARY STAMPED command with offset "0000", that is P1 = "00" and P2 = "00" and

L_e = "01" + X.

Result

The expected status word is "98 10".

RC_RBS_IV_04 subclause 9.4.6 c19_11

Purpose

Check that READ BINARY STAMPED returns "98 35" if no random has been given.

Preconditions

- EF_{ICC} is selected.
- No random has been given.

Test

Present a READ BINARY STAMPED command with offset "0000", that is P1 = "00" and P2 = "00" and

L_e = "01" + X.

Result

The expected status word is "98 35".

RC_RBS_IV_05 subclause 9.4.6 c19_11

Purpose

Check that READ BINARY STAMPED returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.
- A random has been given.

Test

Present a READ BINARY STAMPED command with offset "0000" and L_e = "01" + X.

Result

The expected status word is "94 00".

RC_RBS_IV_06 subclause 9.4.6 c19_11

Purpose

Check that READ BINARY STAMPED returns "94 08" if a file, not valid for READ BINARY STAMPED is selected.

Preconditions

- EF_{KEY_MAN} is selected.
- A random has been given.

Test

Present a READ BINARY STAMPED command with offset "0000" and L_e = "01" + X.

Result

The expected status word is "94 08".

RC_RBS_IV_07 subclause 9.4.6 c19_11

Purpose

Check that READ BINARY STAMPED returns "6B XX" or "94 02" if the offset is greater than the file size.

Preconditions

- EF_{ICC} is selected.
- A random has been given.

Test

Present a READ BINARY STAMPED command with offset "0014", that is P1 = "00", P2 = "14" and

L_e = "01" + X.

Result

The expected status word is "6B XX".

6.2.3.12 READ RECORD (RR)

6.2.3.12.1 Function

FU_RR_VA_01 subclause 8.12 c19_12, c23_10, c23_1

Purpose

Check that the READ RECORD function can be performed using the FIRST mode.

Preconditions

- Readable linear non-empty (containing at least 2 records) EF (with known contents) selected;

Test

Try to read the first record from the EF using the FIRST mode.

Result

The READ RECORD command shall have a positive return code and the data returned by the command shall be in accordance with the actual contents of that EF.

FU_RR_VA_02 subclause 8.12 c19_12, c23_10, c23_1, c23_1

Purpose

Check that the READ RECORD function can be performed using the LAST mode.

Preconditions

- Readable linear non-empty (containing at least 2 records) EF (with known contents) selected;

Test

Try to read the last record from the EF using the LAST mode.

Result

The READ RECORD command shall have a positive return code and the data returned by the command shall be in accordance with the actual contents of that EF.

FU_RR_VA_03 subclause 8.12 c19_12, c23_10, c23_1

Purpose

Check that the READ RECORD function can be performed using the NEXT mode.

Preconditions

- Readable linear non-empty (containing at least 2 records) EF (with known contents) selected;

- Current record pointer is defined but not at beginning or end;

Test

Try to read the next record using the NEXT mode.

Result

The READ RECORD command shall have a positive return code and the data returned by the command shall be in accordance with the actual contents of that EF.

FU_RR_VA_04 subclause 8.12 c19_12, c23_10, c23_1

Purpose

Check that the READ RECORD function can be performed using the PREVIOUS mode.

Preconditions

- Readable linear non-empty (containing at least 2 records) EF (with known contents) selected;
- Current record pointer is defined but not at beginning or end;

Test

Try to read the previous record using the PREVIOUS mode.

Result

The READ RECORD command shall have a positive return code and the data returned by the command shall be in accordance with the actual contents of that EF.

FU_RR_VA_05 subclause 8.12 c19_12, c23_10, c23_1

Purpose

Check that the READ RECORD function can be performed using the ABSOLUTE mode.

Preconditions

- Readable linear non-empty (containing at least 2 records) EF (with known contents) selected;

Test

Try to read a record from it using the ABSOLUTE mode.

Result

The READ RECORD command shall have a positive return code and the data returned by the command shall be in accordance with the actual contents of that EF.

FU_RR_VA_06 subclause 8.12 c19_12, c23_10, c23_1

Purpose

Check that the READ RECORD function can be performed using the CURRENT mode.

Preconditions

- Readable linear non-empty (containing at least 2 records) EF (with known contents) selected;
- Current record not at beginning or end;

Test

Try to read the current record using the CURRENT mode.

Result

The READ RECORD command shall have a positive return code and the data returned by the command shall be in accordance with the actual contents of that EF.

6.2.3.12.2 Command

The coding of the READ RECORD command is the following:

Table 25: Return codes for the READ RECORD command

CLA	Class byte
INS	"B2"
P1	Record no.
P2	Mode
L_c field	Empty
Data field	Empty
L_e field	Number of bytes to be read

CO_RR_VA_01 subclause 9.12 c23_12, c23_1, c28_1

Purpose
Check that the READ RECORD command can be performed while less bytes are requested then available in the record.

Preconditions
- Readable linear non-empty (containing at least 2 records, size larger than 3 bytes) EF (with known contents) selected;

Test
Try to read 3 bytes of the first record from the EF.

Result
The READ RECORD command shall have a positive return code and the data returned by the command shall be in accordance with the actual contents of that EF.

CO_RR_VA_02 subclause 9.10 c23_10, c23_1, c28_6

Purpose
Check that the READ RECORD command can be performed while requesting the complete contents from the current record to the end.

Preconditions
- Readable non-empty (containing at least 2 non-empty records) linear fixed structure EF (with known contents) selected;
- Current record not at beginning or end;

Test
Send an READ RECORD command (in CURRENT mode) to the IUT with field $L_e = 0$.

Result
The READ RECORD command shall have a positive return code and the data returned by the command shall be in accordance with the actual contents of that EF.

CO_RR_VA_03 subclause 9.10 c23_10, c23_1, c28_6

Purpose
Check that the READ RECORD command can be performed while requesting the complete contents from the current record to the logical end of a cyclic record file, wrapping the physical end of the file.

Preconditions
- Readable non-empty (containing at least 3 non-empty records) linear cyclic structure EF (with known contents) selected;
- Current record not at the physical end and not at the physical beginning of the file;

Test

Send a READ RECORD command (in CURRENT mode) to the IUT with field L_e = 0.

Result

The READ RECORD command shall have a positive return code, the data returned by the command shall be in accordance with the actual contents of that EF.

6.2.3.12.3 Return codes

Table 26: Return codes for the READ RECORD command

Return Code	Error description
98 04	- AC not fulfilled
98 10	- in contradiction with the invalidation status
92 40	- no test is foreseen for this status word
94 00	- No EF selected as current
94 02	- Out of range
94 04	- Record not found (ed. 2)
94 08	- Current file type is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P2 > "04"
67 XX	- no test is foreseen for this status word
90 00	- Normal ending (ACK) of the command

RC_RR_VA_01 subclause 9.4.6 c19_12, c4_9

Purpose

Check that READ RECORD returns "90 00" if used correctly.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is fulfilled.

Test

Present a READ RECORD command with P1 = "00", P2 = "00" and L_e = "01".

Result

The expected status word is "90 00".

RC_RR_IV_01 subclause 9.4.6 c19_12

Purpose

Check that READ RECORD returns "98 04" if the selected file has an unfulfilled access condition on read.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is not fulfilled.

Test

Present a READ RECORD command with P1 = "00", P2 = "00" and L_e = "01".

Result

The expected status word is "98 04".

RC_RR_IV_02 subclause 9.4.6 c19_12, c9_1

Purpose

Check that READ RECORD returns "98 10" if the selected file is invalidated.

Preconditions

- An invalidated EF with linear fixed structure is selected.
- That EF is not readable when invalidated.
- The AC for READ/SEEK is fulfilled.
- A random has been given.

Test

Present a READ RECORD command with P1 = "00", P2 = "00" and L_e = "01".

Result

The expected status word is "98 10".

RC_RR_IV_03 subclause 9.4.6 c19_12

Purpose

Check that READ RECORD returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.

Test

Present a READ RECORD command with P1 = "00", P2 = "00" and L_e = "01".

Result

The expected status word is "94 00".

RC_RR_IV_04 subclause 9.4.6 c19_12

Purpose

Check that READ RECORD returns "94 02" or "94 04" if the addressed record is not found.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is fulfilled.
- The number of records in that EF is known.

Test

Present a READ RECORD command with P1 greater than the number of existing records, P2 = "04" and L_e = "01".

Result

The expected status word is "94 02" or "94 04".

RC_RR_IV_05 subclause 9.4.6 c19_12

Purpose

Check that READ RECORD returns "94 08" if a file, not valid for READ RECORD is selected.

Preconditions

- EF_{ICC} is selected.

Test

Present a READ RECORD command with P1 = "00", P2 = "00" and L_e = "01".

Result

The expected status word is "94 08".

RC_RR_IV_06 subclause 9.4.6 c19_12

Purpose

Check that READ RECORD returns "6B XX" if P2 > "04".

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is fulfilled.

Test

Present a READ RECORD command with P1 = "00" and P2 > "04" and L_e = "01".

Result

The expected status word is "6B XX".

6.2.3.13 READ RECORD STAMPED (RRS)

6.2.3.13.1 Function

FU_RRS_VA_01 subclause 8.13 c19_13, c23_13, c23_1, c23_24, c29_1

Purpose

Check that the READ RECORD STAMPED function can be performed using the FIRST mode.

Preconditions

- Readable linear non-empty (containing at least 2 records) EF (with known contents) selected;
- A random has been given.

Test

Try to read the first record from the EF using the FIRST mode.

Result

The READ RECORD STAMPED command shall have a positive return code, the data returned by the command shall be in accordance with the actual contents of that EF and the returned cryptogram shall be correct.

FU_RRS_VA_02 subclause 8.13 c19_13, c23_13, c23_1, c23_24, c29_2

Purpose

Check that the READ RECORD STAMPED function can be performed using the LAST mode.

Preconditions

- Readable linear non-empty (containing at least 2 records) EF (with known contents) selected;
- A random has been given.

Test

Try to read the last record from the EF using the LAST mode.

Result

The READ RECORD STAMPED command shall have a positive return code, the data returned by the command shall be in accordance with the actual contents of that EF and the returned cryptogram shall be correct.

FU_RRS_VA_03 subclause 8.13 c19_13, c23_13, c23_1, c23_24, c29_3

Purpose

Check that the READ RECORD STAMPED function can be performed using the NEXT mode.

Preconditions

- Readable linear non-empty (containing at least 2 records) EF (with known contents) selected;
- Current record not at the end;
- A random has been given.

Test

Try to read the next record using the NEXT mode.

Result

The READ RECORD STAMPED command shall have a positive return code, the data returned by the command shall be in accordance with the actual contents of that EF and the returned cryptogram shall be correct.

FU_RRS_VA_04 subclause 8.13 c19_13, c23_13, c23_1, c23_24, c29_4

Purpose

Check that the READ RECORD STAMPED function can be performed using the PREVIOUS mode.

Preconditions

- Readable linear non-empty (containing at least 2 records) EF (with known contents) selected;
- Current record not at the beginning;
- A random has been given.

Test

Try to read the previous record using the PREVIOUS mode.

Result

The READ RECORD STAMPED command shall have a positive return code, the data returned by the command shall be in accordance with the actual contents of that EF and the returned cryptogram shall be correct.

FU_RRS_VA_05 subclause 8.13 c19_13, c23_13, c23_1, c23_24, c29_5

Purpose

Check that the READ RECORD STAMPED function can be performed using the ABSOLUTE mode.

Preconditions

- Readable linear non-empty (containing at least 2 records) EF (with known contents) selected;
- A random has been given.

Test

Try to read a record from it using the ABSOLUTE mode.

Result

The READ RECORD STAMPED command shall have a positive return code, the data returned by the command shall be in accordance with the actual contents of that EF and the returned cryptogram shall be correct.

FU_RRS_VA_06 subclause 8.13 c19_13, c23_13, c23_1, c23_24, c29_6

Purpose

Check that the READ RECORD STAMPED function can be performed using the CURRENT mode.

Preconditions

- Readable linear non-empty (containing at least 2 records) EF (with known contents) selected;
- Current record not at beginning or end;
- A random has been given.

Test

Try to read the current record using the CURRENT mode.

Result

The READ RECORD STAMPED command shall have a positive return code, the data returned by the command shall be in accordance with the actual contents of that EF and the returned cryptogram shall be correct.

6.2.3.13.2 Command

The coding of the READ RECORD STAMPED command is the following:

Table 27: Return codes for the READ RECORD STAMPED command

CLA	Class byte
INS	"B6"
P1	Record no.
P2	Mode
L_c field	Empty
Data field	Empty
L_e field	Number of bytes to be read

CO_RRS_VA_01 subclause 9.2.13 c23_13, c23_1, c23_24, c29_1

Purpose
Check that the READ RECORD STAMPED command can be performed while less bytes are requested then available in the record.

Preconditions
- Readable linear non-empty (containing at least 2 records, size larger than 3 bytes) EF (with known contents) - selected;
- A random has been given.

Test
Try to read 3 bytes of the first record from the EF.

Result
The READ RECORD STAMPED command shall have a positive return code, the data returned by the command shall be in accordance with the actual contents of that EF and the returned cryptogram shall be correct.

CO_RRS_VA_02 subclause 9.2.13 c23_13, c23_1, c23_24, c29_6

Purpose
Check that the READ RECORD STAMPED command can be performed while requesting the complete contents from the current record to the end.

Preconditions
- Readable non-empty (containing at least 2 non-empty records) linear fixed structure EF (with known contents) selected;
- Current record not at the end;
- A random has been given.

Test
Send a READ RECORD STAMPED command (in CURRENT mode) to the IUT with field $L_e = 0$.

Result
The READ RECORD STAMPED command shall have a positive return code, the data returned by the command shall be in accordance with the actual contents of that EF and the returned cryptogram shall be correct.

CO_RRS_VA_03 subclause 9.2.13 c23_13, c23_1, c23_24, c29_6

Purpose
Check that the READ RECORD STAMPED command can be performed while requesting the complete contents from the current record to the logical end of a cyclic record file wrapping the physical end of the file.

Preconditions
- Readable non-empty (containing at least 3 non-empty records) linear cyclic structure EF (with known contents) selected;
- Current record not at the physical end and not at the physical beginning of the file;
- A random has been given.

Test

Send a READ RECORD STAMPED command (in CURRENT mode) to the IUT with field L_e = 0.

Result

The READ RECORD STAMPED command shall have a positive return code, the data returned by the command shall be in accordance with the actual contents of that EF and the returned cryptogram shall be correct.

6.2.3.13.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 28: Return codes for the READ RECORD STAMPED command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
94 00	- No EF selected as current
94 02	- Out of range
94 04	- Record not found (note)
94 08	- Current file type is inconsistent with the command
92 40	- no test is foreseen for this status word
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P2 > "04"
67 XX	- L_e > record length
90 00	- Normal ending (ACK) of the command
NOTE: This error code shall not be used, but 94 02 instead. (CR)	

RC_RRS_VA_01 subclause 9.4.6 c19_13, c4_9

Purpose

Check that READ RECORD STAMPED returns "90 00" if used correctly.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is fulfilled.
- A random has been given.

Test

Present a READ RECORD STAMPED command with P1 = "00", P2 = "00" and L_e = "01" + X.

Result

The expected status word is "90 00".

RC_RRS_IV_01 subclause 9.4.6 c19_13

Purpose

Check that READ RECORD STAMPED returns "98 02" if the key associated with the file does not exist.

Preconditions

- An EF with linear fixed structure with a not existing key associated to READ is selected.
- The AC for READ/SEEK is fulfilled.
- A random has been given.

Test

Present a READ RECORD STAMPED command with P1 = "00", P2 = "00" and L_e = "01" + X.

Result

The expected status word is "98 02".

RC_RRS_IV_02 subclause 9.4.6 c19_13

Purpose

Check that READ RECORD STAMPED returns "98 04" if the selected file has an unfulfilled access condition on read.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is not fulfilled.
- A random has been given.

Test

Present a READ RECORD STAMPED command with P1 = "00", P2 = "00" and L_e = "01" + X.

Result

The expected status word is "98 04".

RC_RRS_IV_03 subclause 9.4.6 c19_13

Purpose

Check that READ RECORD STAMPED returns "98 10" if the selected file is invalidated.

Preconditions

- An invalidated EF with linear fixed structure is selected.
- That EF is not readable when invalidated.
- The AC for READ/SEEK is fulfilled.
- A random has been given.

Test

Present a READ RECORD STAMPED command with P1 = "00", P2 = "00" and L_e = "01" + X.

Result

The expected status word is "98 10".

RC_RRS_IV_04 subclause 9.4.6 c19_13

Purpose

Check that READ BINARY STAMPED returns "98 35" if no random has been given.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is fulfilled.
- No random has been given.
- A random has been given.

Test

Present a READ RECORD STAMPED command with P1 = "00", P2 = "00" and L_e = "01" + X.

Result

The expected status word is "98 35".

RC_RRS_IV_05 subclause 9.4.6 c19_13

Purpose

Check that READ RECORD STAMPED returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.
- A random has been given.

Test

Present a READ RECORD STAMPED command with P1 = "00", P2 = "00" and L_e = "01" + X.

Result

The expected status word is "94 00".

RC_RRS_IV_06 subclause 9.4.6 c19_13

Purpose

Check that READ RECORD STAMPED returns "94 02" or "94 04" if the addressed record is not found.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is fulfilled.
- The number of records in that EF is known.
- A random has been given.

Test

Present a READ RECORD STAMPED command with P1 greater than the number of existing records, P2 = "04" and L_e = "01" + X.

Result

The expected status word is "94 02" or "94 04".

RC_RRS_IV_07 subclause 9.4.6 c19_13

Purpose

Check that READ RECORD STAMPED returns "94 08" if a file, not valid for READ RECORD is selected.

Preconditions

- EF_{ICC} is selected.
- A random has been given.

Test

Present a READ RECORD STAMPED command with P1 = "00", P2 = "00" and L_e = "01" + X.

Result

The expected status word is "94 08".

RC_RRS_IV_08 subclause 9.4.6 c19_13

Purpose

Check that READ RECORD STAMPED returns "6B XX" if P2 > "04".

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is fulfilled.
- A random has been given.

Test

Present a READ RECORD STAMPED command with P1 = "00", P2 = "00" and L_e = "01" + X.

Result

The expected status word is "6B XX".

RC_RRS_IV_09 subclause 9.4.6 c19_13

Purpose

Check that READ RECORD STAMPED returns "67 XX" if L_e greater than the file size.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is fulfilled.
- The size of a record in that EF is known.
- A random has been given.

Test

Present a READ RECORD STAMPED command with P1 = "00", P2 = "00" and L_e is greater than the size of the record + X.

Result

The expected status word is "67 XX".

6.2.3.14 SEEK (SK)

6.2.3.14.1 Function

FU_SK_VA_01 subclause 8.14 c19_14, c23_14, c23_1

Purpose

Check that the SEEK function can be successfully performed on a linear fixed structure EF using a search from the beginning forward.

Preconditions

- Readable non-empty (containing at least 2 non-empty records) linear fixed structure EF (with known contents) selected;

Test

Try to seek for a record with a matching search string from the beginning forward.

Result

Command shall have a positive return code.

FU_SK_VA_02 subclause 8.14 c19_14, c23_14, c23_1

Purpose

Check that the SEEK function can be successfully performed on a linear fixed structure EF using a search from the end backward.

Preconditions

- Readable non-empty (containing at least 2 non-empty records) linear fixed structure EF (with known contents) selected;

Test

Try to seek for a record with a matching search string from the end backward.

Result

Command shall have a positive return code.

FU_SK_VA_03 subclause 8.14 c19_14, c23_14, c23_1

Purpose

Check that the SEEK function can be successfully performed on a linear fixed structure EF using a search from the next location forward.

Preconditions

- Readable non-empty (containing at least 2 non-empty records) linear fixed structure EF (with known contents) selected;

- Current record not at beginning or end;

Test

Try to seek for a record with a matching search string from the next location forward.

Result

Command shall have a positive return code.

FU_SK_VA_04 subclause 8.14 c19_14, c23_14, c23_1

Purpose

Check that the SEEK function can be successfully performed on a linear fixed structure EF using a search from the previous location backward.

Preconditions

- Readable non-empty (containing at least 2 non-empty records) linear fixed structure EF (with known contents) selected;

- Current record not at beginning or end;

Test

Try to seek for a record with a matching search string from the previous location backward.

Result

Command shall have a positive return code.

FU_SK_VA_05 subclause 8.14 c19_14, c23_14, c23_1

Purpose

Check that the SEEK function can be successfully performed on a linear variable structure EF using a search from the beginning forward.

Preconditions

- Readable non-empty (containing at least 2 non-empty records) linear variable structure EF (with known contents) selected;

Test

Try to seek for a record with a matching search string from the beginning forward.

Result

Command shall have a positive return code.

FU_SK_VA_06 subclause 8.14 c19_14, c23_14, c23_1

Purpose

Check that the SEEK function can be successfully performed on a cyclic EF using a search from the beginning forward.

Preconditions

- Readable non-empty (containing at least 2 non-empty records) cyclic EF (with known contents) selected;

Test

Try to seek for a record with a matching search string from the beginning forward.

Result

Command shall have a positive return code.

FU_SK_VA_07 subclause 8.14 c19_14, c23_14, c23_1

Purpose

Check that the SEEK function can be successfully performed on a cyclic EF using a search from the end backward.

Preconditions

- Readable non-empty (containing at least 2 non-empty records) cyclic EF (with known contents) selected;

Test

Try to seek for a record with a matching search string from the end backward.

Result

Command shall have a positive return code.

6.2.3.14.2 Command

The coding of the SEEK command is the following:

Table 29: Return codes for the SEEK command

CLA	Class byte
INS	"A2"
P1	Offset
P2	Type/Mode
L_c field	Length of data field
Data field	Data sent to the card
L_e field	Empty or 1 byte (for type = 2)

CO_SK_VA_01 subclause 9.14 c23_14, c23_1, c30_7

Purpose
Check that the SEEK command can be successfully performed on a linear fixed structure EF using a search from the beginning forward with offset 4.

Preconditions
- Readable non-empty (containing at least 2 non-empty records) linear fixed structure EF (with known contents) selected;

Test
Try to seek for a record with offset 4 and a matching search string from the beginning forward.

Result
Command shall have a positive return code.

CO_SK_VA_02 subclause 9.14 c23_14, c23_1, c30_7

Purpose
Check that the SEEK command can be successfully performed on a linear fixed structure EF using a search from the beginning forward with offset 7.

Preconditions
- Readable non-empty (containing at least 2 non-empty records) linear fixed structure EF (with known contents) selected;

Test
Try to seek for a record with offset 7 and a matching search string from the beginning forward.

Result
Command shall have a positive return code.

CO_SK_VA_03 subclause 9.14 c23_14, c23_1, c30_7

Purpose
Check that the SEEK command can be successfully performed on a linear fixed structure EF using a search from the beginning forward with a short search argument. No Response Data is requested.

Preconditions
- Readable non-empty (containing at least 2 non-empty records) linear fixed structure EF (with known contents) selected;

Test

Try to seek for a record with a one character matching search string from the beginning forward.

Set P2 = "00".

Result

Command shall have a positive return code.

There is no response data

CO_SK_VA_04 subclause 9.14 c23_14, c23_1, c30_7

Purpose

Check that the SEEK command can be successfully performed on a linear fixed structure EF using a search from the beginning forward with a short search argument. No Response Data is requested.

Preconditions

- Readable non-empty (containing at least 2 non-empty records) linear fixed structure EF (with known contents) selected;

Test

Try to seek for a record with a one character matching search string from the beginning forward.

Set P2 = "00".

Result

Command shall have a positive return code.

Record number is returned.

CO_SK_VA_05 subclause 9.14 c23_14, c23_1, c30_7

Purpose

Check that the SEEK command can be successfully performed on a linear fixed structure EF using a search from the beginning forward with a long search argument.

Preconditions

- Readable non-empty (containing at least 2 non-empty records of size larger than 20) linear fixed structure EF (with known contents) selected;

Test

Try to seek for a record with a 20 character matching search string from the beginning forward.

Result

Command shall have a positive return code.

CO_SK_VA_06 subclause 9.14 c23_14, c23_1, c30_7

Purpose

Check that the SEEK command can be successfully performed on a linear fixed structure EF using a search from the beginning forward with a search argument exactly matching a record.

Preconditions

- Readable non-empty (containing at least 2 non-empty records) linear fixed structure EF (with known contents) selected;

Test

Try to seek for a record with a 20 character matching search string from the beginning forward.

Result

Command shall have a positive return code.

6.2.3.14.3 Return codes

Table 30: Return codes for the SEEK command

Return Code	Error description
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status (note)
92 40	- no test is foreseen for this status word
94 00	- No EF selected as current
94 04	- Pattern not found
94 08	- Current file type is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P2 ≠ 000X00XX
67 XX	- L_e not empty for type 1 - L_e > 1 for type 2
90 00	- Normal ending (ACK) of the command
9F XX	- Length "XX" of the response data
NOTE: This status word is needed as the SEEK command depends on the invalidation status.	

RC_SK_VA_01 subclause 9.4.6 c19_14, c4_9

Purpose

Check that SEEK returns "90 00" if used correctly.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is fulfilled.
- The contents is known.

Test

Present a SEEK command with P1 = "00", P2 = "00", L_e empty and the datafield contains the contents of an existing record (with a matching L_c).

Result

The expected status word is "90 00".

RC_SK_VA_01 subclause 9.4.6 c19_14, c4_8

Purpose

Check that SEEK returns "90 00" if used correctly.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is fulfilled.
- The contents is known.

Test

Present a SEEK command with P1 = "00", P2 = "00", L_e empty and the datafield contains the contents of an existing record (with a matching L_c).

Result

The expected status word is "9F XX".

RC_SK_IV_01 subclause 9.4.6 c19_14

Purpose

Check that SEEK returns "98 04" if the selected file has an unfulfilled access condition on read.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is not fulfilled.
- The contents is known.

Test

Present a SEEK command with P1 = "00", P2 = "00", L_e empty and the datafield contains the contents of an existing record (with a matching L_c).

Result

The expected status word is "98 04".

RC_SK_IV_02 subclause 9.4.6 c19_14

Purpose

Check that SEEK returns "98 10" if the selected file is invalidated.

Preconditions

- An invalidated EF with linear fixed structure is selected.
- That EF is not readable when invalidated.
- The AC for READ/SEEK is fulfilled.
- The contents is known.

Test

Present a SEEK command with P1 = "00", P2 = "00", L_e empty and the datafield contains the contents of an existing record (with a matching L_c).

Result

The expected status word is "98 10".

RC_SK_IV_03 subclause 9.4.6 c19_14

Purpose

Check that SEEK returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.

Test

Present a SEEK command with P1 = "00", P2 = "00", L_e empty and the datafield contains the contents of any record (with a matching L_c).

Result

The expected status word is "94 00".

RC_SK_IV_04 subclause 9.4.6 c19_14

Purpose

Check that SEEK returns "94 04" if the pattern could not be found.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is fulfilled.
- The contents is known.

Test

Present a SEEK command with P1 = "00", P2 = "00", L_e empty and the datafield contains the contents of no existing record (with a matching L_c).

Result

The expected status word is "94 04".

RC_SK_IV_05 subclause 9.4.6 c19_14

Purpose

Check that the SEEK function returns "94 04" when performed on a linear fixed structure EF using a search from the next record onward while no further record matches the argument.

Preconditions

- An EF with linear fixed structure is selected.
- A record inside that EF is selected.
- The AC for READ/SEEK is fulfilled.
- The contents is known and contains at least one record different from the one currently selected and no record with the same contents.

Test

Present a SEEK command with P1 = "00", P2 = "02", L_e empty and the datafield contains the contents of the currently selected record (with a matching L_c).

Result

The expected status word is "94 04".

RC_SK_IV_06 subclause 9.4.6 c19_14

Purpose

Check that SEEK returns "94 08" if a file, not valid for SEEK is selected.

Preconditions

- EF_{ICC} is selected.

Test

Present a SEEK command with P1 = "00", P2 = "00", L_e empty and the datafield contains the first part of the contents of the file (with a matching L_c).

Result

The expected status word is "94 08".

RC_SK_IV_07 subclause 9.4.6 c19_14

Purpose

Check that SEEK returns "6B XX" if P2 ≠ 000X00XX.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is fulfilled.
- The contents is known.

Test

Present a SEEK command with P1 = "00", P2 ≠ 000X00XX, L_e empty and the datafield contains the contents of an existing record (with a matching L_c).

Result

The expected status word is "6B XX".

RC_SK_IV_08 subclause 9.4.6 c19_14

Purpose

Check that SEEK returns "67 XX" if L_e ≠ "01" for type 2.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for READ/SEEK is fulfilled.
- The size of a record in that EF is known.

Test

Present a SEEK command with P1 = "00", P2 = 000100XX, L_e ≠ "01" and the datafield contains the contents of an existing record (with a matching L_c).

Result

The expected status word is "67 XX".

6.2.3.15 VERIFY CHV (VC)

6.2.3.15.1 Function

FU_VC_VA_01 subclause 8.15 c19_15, c23_15, c23_1, c23_10, c12_5_1

Purpose

Check that the VERIFY CHV function can be performed successfully with CHV1.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.

- A transparent EF with AC READ = CHV1 exists.

Test

Reset the IUT.

Present a VERIFY CHV command.

Present a SELECT command on the EF with AC READ = CHV1.

Present a READ BINARY command to read that file.

Result

The selected EF shall be readable.

FU_VC_VA_02 subclause 8.15 c19_15, c23_15, c23_1, c23_10, c12_5_1

Purpose

Check that the VERIFY CHV function can be performed successfully with CHV2.

Preconditions

- EF_{CHV2} exists.
- CHV is to be presented in clear.
- A transparent EF with AC READ = CHV2 exists.

Test

Reset the IUT.

Present a VERIFY CHV command.

Present a SELECT command on the EF with AC READ = CHV2.

Present a READ BINARY command to read that file.

Result

The selected EF shall be readable.

FU_VC_VA_03 subclause 8.15 c19_15, c23_15, c12_5_1

Purpose

Check that the VERIFY CHV function can reset the "remaining CHV attempts counter".

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- The CHV has been presented unsuccessfully N-1 times.

Test

Present a VERIFY CHV command with the correct CHV.

Present a VERIFY CHV command with the wrong CHV.

Result

The expected SW for the second VERIFY CHV is "98 04".

FU_VC_VA_04 subclause 8.15 c19_15, c23_15, c12_5_1

Purpose

Check that the "remaining CHV attempts counter" remains blocked after N unsuccessful CHV representations.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- The CHV has been presented unsuccessfully N times.

Test

Present a VERIFY CHV command with the correct CHV.

Result

The expected SW for the VERIFY CHV is "98 40".

FU_VC_VA_05 subclause 8.15 c19_15, c23_15, c23_1, c23_10, c23_23, c12_5_2

Purpose

Check that the VERIFY CHV function can be used for an enciphered CHV.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented enciphered.
- A transparent EF with AC READ = CHV1 exists.
- A Random has been asked for.
- AC CHV1 is not yet fulfilled.

Test

Present a VERIFY CHV command with the CHV enciphered.

Present a SELECT command on the EF with AC READ = CHV1.

Present a READ BINARY command to read that file.

Result

The selected EF shall be readable.

FU_VC_VA_06 subclause 8.15 c19_15, c23_15, c23_1, c23_10, c12_1_2

Purpose

Check that the VERIFY CHV function can be performed successfully with CHV1 which stores a path to another CHV file.

Preconditions

- EF_{CHV1} exists containing path to existing CHV file.
- CHV is to be presented in clear.
- A transparent EF with AC READ = CHV1 exists.

Test

Reset the IUT.

Present a VERIFY CHV command.

Present a SELECT command on the EF with AC READ = CHV1.

Present a READ BINARY command to read that file.

Result

The selected EF shall be readable.

6.2.3.15.2 Command

The coding of the VERIFY CHV command is the following:

Table 31: Return codes for the VERIFY CHV command

CLA	Class byte
INS	"20"
P1	"00" (other values are RFU)
P2	"01" for CHV1 "02" for CHV2
L_c field	"08"
Data field	Data sent to the card
L_e field	Empty

No tests are foreseen to test the VERIFY CHV command other than those defined in the functions subclause.

6.2.3.15.3 Return codes

The following return codes are defined for VERIFY CHV:

Table 32: Return codes for the VERIFY CHV command

Return Code	Error description
98 02	- No CHV defined
98 04	- Unsuccessful CHV verification but VERIFY CHV mechanism still possible (number of false consecutive verification < N)
98 08	- In contradiction with CHV status
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
98 40	- Unsuccessful CHV verification, VERIFY CHV mechanism no longer possible (number of false consecutive verifications >= N)
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00", P2 ≠ "01" and P2 ≠ "02"
67 XX	- L_c ≠ "08"
90 00	- Normal ending (ACK) of the command

RC_VC_VA_01 subclause 9.4.6 c19_15

Purpose

Check that VERIFY CHV returns "90 00", if used correctly.

Preconditions

- EF_{CHV1} exists and is enabled.

- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a valid VERIFY CHV command with P2 = "01".

Result

The expected status word is "90 00".

RC_VC_IV_01 subclause 9.4.6 c19_15

Purpose

Check that VERIFY CHV returns "98 02", if no CHV is defined.

Preconditions

- EF_{CHV1} does not exist in the path to the current DF.

Test

Reset the UC and present a valid VERIFY CHV command with P2 = "01".

Result

The expected status word is "98 02".

RC_VC_IV_02 subclause 9.4.6 c19_15

Purpose

Check that VERIFY CHV returns "98 04", if the presented CHV is false.

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- At least two false attempts are allowed to present the CHV.

Test

Reset the UC and present a VERIFY CHV command with P2 = "01" and a wrong CHV.

Result

The expected status word is "98 04".

RC_VC_IV_03 subclause 9.4.6 c19_15

Purpose

Check that VERIFY CHV returns "98 04", if the presented CHV is false.

Preconditions

- EF_{CHV2} exists and is enabled.
- CHV is known.
- At least two false attempts are allowed to present the CHV.

Test

Reset the UC and present a VERIFY CHV command with P2 = "02" and a wrong CHV.

Result

The expected status word is "98 04".

RC_VC_IV_04 subclause 9.4.6 c19_15

Purpose

Check that VERIFY CHV returns "98 08", if the CHV is not activated.

Preconditions

- EF_{CHV1} exists.
- EF_{CHV1} is not activated (least significant bit in activation byte is set to 0).
- CHV is known.

Test

Reset the UC and present a valid VERIFY CHV command with P2 = "01".

Result

The expected status word is "98 08".

RC_VC_IV_05 subclause 9.4.6 c19_15

Purpose

Check that VERIFY CHV returns "98 08", if the CHV is present but disabled.

Preconditions

- EF_{CHV1} exists.
- EF_{CHV1} is disabled.
- CHV is known.

Test

Reset the UC and present a valid VERIFY CHV command with P2 = "01".

Result

The expected status word is "98 08".

RC_VC_IV_06 subclause 9.4.6 c19_15, c9_1

Purpose

Check that VERIFY CHV returns "98 10", if the CHV is present but invalidated.

Preconditions

- EF_{CHV1} exists.
- EF_{CHV1} is invalidated.
- CHV is known.

Test

Reset the UC and present a valid VERIFY CHV command with P2 = "01".

Result

The expected status word is "98 10".

RC_VC_IV_07 subclause 9.4.6 c19_15, c12_5_2

Purpose

Check that VERIFY CHV returns "98 35", if for an enciphered CHV no Random has been given.

Preconditions

- EF_{CHV1} exists and is enabled.
- EF_{CHV1} requires an enciphered CHV.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a VERIFY CHV command with P2 = "01" but present the CHV in clear.

Result

The expected status word is "98 35".

RC_VC_IV_08 subclause 9.4.6 c19_15

Purpose

Check that VERIFY CHV returns "98 40", after N unsuccessful tries.

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- N is known.
- CHV1 has been presented unsuccessfully N-1 times.

Test

Reset the UC and present a VERIFY CHV command with P2 = "01" and a wrong CHV.

Result

The expected status word is "98 40".

RC_VC_IV_09 subclause 9.4.6 c19_15

Purpose

Check that VERIFY CHV returns "92 0X" if the internal retry routine has been used.

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- The internal memory can only be written after X retries.
- Less than N false attempts have been made to present the CHV.

Test

Reset the UC and present a valid VERIFY CHV command with P2 = "01".

Result

The expected status word is "92 0X".

RC_VC_IV_10 subclause 9.4.6 c19_15

Purpose

Check that VERIFY CHV returns "92 40" if the internal memory can not be written.

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- The internal memory can not be written.
- Less than N false attempts have been made to present the CHV.

Test

Reset the UC and present a valid VERIFY CHV command with P2 = "01".

Result

The expected status word is "92 40".

RC_VC_IV_11 subclause 9.4.6 c19_15

Purpose

Check that VERIFY CHV returns "6B XX" if the parameter P1 ≠ "00".

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a VERIFY CHV command with P2 = "01" and P1 ≠ "00".

Result

The expected status word is "6B XX".

RC_VC_IV_12 subclause 9.4.6 c19_15

Purpose

Check that VERIFY CHV returns "6B XX" if the parameter P2 ≠ "01" and P2 ≠ "02".

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a VERIFY CHV command with P2 ≠ "01" and P2 ≠ "02".

Result

The expected status word is "6B XX".

RC_VC_IV_13 subclause 9.4.6 c19_15

Purpose

Check that VERIFY CHV returns "67 XX" if the parameter L_c ≠ "08".

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a VERIFY CHV command with L_c ≠ "08" and a matching datafield.

Result

The expected status word is "67 XX".

6.2.3.16 CHANGE CHV (CC)

6.2.3.16.1 Function

FU_CC_VA_01 subclause 8.16 c19_16, c23_16, c23_15, c23_1, c23_10, c12_5_1

Purpose

Check that the CHANGE CHV function can be performed successfully with CHV1.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- A transparent EF with AC READ = CHV1 exists.

Test

Reset the IUT.

Present a CHANGE CHV command.

Reset the IUT.

Present a VERIFY CHV command with the new CHV.

Present a SELECT command on the EF with AC READ = CHV1.

Present a READ BINARY command to read that file.

Result

The selected EF shall be readable.

FU_CC_VA_02 subclause 8.16 c19_16, c23_16, c23_15, c23_1, c23_10, c12_5_1

Purpose

Check that the CHANGE CHV function can be performed successfully with CHV2.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- A transparent EF with AC READ = CHV2 exists.

Test

Reset the IUT.

Present a CHANGE CHV command.

Reset the IUT.

Present a VERIFY CHV command with the new CHV.

Present a SELECT command on the EF with AC READ = CHV2.

Present a READ BINARY command to read that file.

Result

The selected EF shall be readable.

FU_CC_VA_03 subclause 8.16 c19_16, c23_16, c23_15, c12_5_1

Purpose

Check that the CHANGE CHV function can reset the "remaining CHV attempts counter".

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- The CHV has been presented unsuccessfully N-1 times.

Test

Present a CHANGE CHV command with the correct CHV.

Present a VERIFY CHV command with the wrong CHV.

Result

The expected SW for the VERIFY CHV is "98 04".

FU_CC_VA_04 subclause 8.15 c19_16, c23_16, c23_15, c12_5_1

Purpose

Check that the "remaining CHV attempts counter" remains blocked after N unsuccessful CHANGE CHV representations.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- The CHANGE CHV has been presented unsuccessfully N times.

Test

Present a CHANGE CHV command with the correct CHV.

Result

The expected SW for the CHANGE CHV is "98 40".

FU_CC_VA_05 subclause 8.16 c19_16, c23_16, c23_15, c23_1, c23_10, c23_23, c12_5_2

Purpose

Check that the CHANGE CHV function can be used for an enciphered CHV.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented enciphered.
- A transparent EF with AC READ = CHV1 exists.
- A Random has been asked for.
- AC CHV1 is not yet fulfilled.

Test

Present a CHANGE CHV command with the old and the new CHV enciphered.

Reset the IUT.

Present an ASK RANDOM command.

Present a VERIFY CHV command with the new CHV.

Present a SELECT command on the EF with AC READ = CHV1.

Present a READ BINARY command to read that file.

Result

The selected EF shall be readable.

FU_CC_VA_06 subclause 8.16 c19_16, c23_16, c23_15, c23_1, c23_10, c12_1_2

Purpose

Check that the CHANGE CHV function can be performed successfully with CHV1 which stores a path to another CHV file.

Preconditions

- EF_{CHV1} exists containing path to existing CHV file.
- CHV is to be presented in clear.
- A transparent EF with AC READ = CHV1 exists.

Test

Reset the IUT.

Present a CHANGE CHV command.

Reset the IUT.

Present a VERIFY CHV command with the new CHV.

Present a SELECT command on the EF with AC READ = CHV1.

Present a READ BINARY command to read that file.

Result

The selected EF shall be readable.

6.2.3.16.2 Command

The coding of the CHANGE CHV command is the following:

Table 33: Return codes for the CHANGE CHV command

CLA	Class byte
INS	"24"
P1	"00" (other values are RFU)
P2	"01" for CHV1 "02" for CHV2
L_c field	"10"
Data field	Data sent to the card
L_e field	Empty

No tests are foreseen to test the CHANGE CHV command other than those defined in the functions subclause.

6.2.3.16.3 Return codes

The following return codes are defined for CHANGE CHV:

Table 34: Return codes for the CHANGE CHV command

Return Code	Error description
98 02	- No CHV defined
98 04	- Unsuccessful CHV verification but VERIFY CHV mechanism still possible (number of false consecutive verification < N)
98 08	- In contradiction with CHV status
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
98 40	- Unsuccessful CHV verification, VERIFY CHV mechanism no longer possible (number of false consecutive verifications >= N)
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00", P2 ≠ "01" and P2 ≠ "02"
67 XX	- L_c ≠ "10"
90 00	- Normal ending (ACK) of the command

RC_CC_VA_01 subclause 9.4.6 c19_16

Purpose
Check that CHANGE CHV returns "90 00", if used correctly.

Preconditions
- EF_{CHV1} exists and is enabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test
Reset the UC and present a valid CHANGE CHV command with P2 = "01" and a new CHV different from the previous one.

Result
The expected status word is "90 00".

RC_CC_IV_01 subclause 9.4.6 c19_16

Purpose
Check that CHANGE CHV returns "98 02", if no CHV is defined.

Preconditions
- EF_{CHV1} does not exist.

Test

Reset the UC and present a valid CHANGE CHV command with P2 = "01" and a new CHV different from the previous one.

Result

The expected status word is "98 02".

RC_CC_IV_02 subclause 9.4.6 c19_16

Purpose

Check that CHANGE CHV returns "98 04", if the presented CHV1 is false.

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- At least two false attempts are allowed to present the CHV.

Test

Reset the UC and present a CHANGE CHV command with P2 = "01", a wrong CHV to verify and a new CHV different from the previous one.

Result

The expected status word is "98 04".

RC_CC_IV_03 subclause 9.4.6 c19_16

Purpose

Check that CHANGE CHV returns "98 04", if the presented CHV2 is false.

Preconditions

- EF_{CHV2} exists and is enabled.
- CHV is known.
- At least two false attempts are allowed to present the CHV.

Test

Reset the UC and present a CHANGE CHV command with P2 = "02", a wrong CHV to verify and a new CHV different from the previous one.

Result

The expected status word is "98 04".

RC_CC_IV_04 subclause 9.4.6 c19_16

Purpose

Check that CHANGE CHV returns "98 08", if the CHV is present but disabled.

Preconditions

- EF_{CHV1} exists.
- EF_{CHV1} is disabled.
- CHV is known.

Test

Reset the UC and present a valid CHANGE CHV command with P2 = "01" and a new CHV different from the previous one.

Result

The expected status word is "98 08".

RC_CC_IV_05 subclause 9.4.6 c19_16

Purpose

Check that CHANGE CHV returns "98 08", if the CHV is not activated.

Preconditions

- EF_{CHV1} exists.
- EF_{CHV1} is not activated (least significant bit in activation byte is set to 0).
- CHV is known.

Test

Reset the UC and present a valid CHANGE CHV command with P2 = "01" and a new CHV different from the previous one.

Result

The expected status word is "98 08".

RC_CC_IV_06 subclause 9.4.6 c19_16, c9_1

Purpose

Check that CHANGE CHV returns "98 10", if the CHV is present but invalidated.

Preconditions

- EF_{CHV1} exists.
- EF_{CHV1} is invalidated.
- CHV is known.

Test

Reset the UC and present a valid CHANGE CHV command with P2 = "01" and a new CHV different from the previous one.

Result

The expected status word is "98 10".

RC_CC_IV_07 subclause 9.4.6 c19_16, c12_5_2

Purpose

Check that CHANGE CHV returns "98 35", if for an enciphered CHV no Random has been given.

Preconditions

- EF_{CHV1} exists and is enabled.
- EF_{CHV1} requires an enciphered CHV.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a CHANGE CHV command with P2 = "01" and a new CHV different from the previous one but present the CHVs in clear.

Result

The expected status word is "98 35".

RC_CC_IV_08 subclause 9.4.6 c19_16

Purpose

Check that CHANGE CHV returns "98 40", after N unsuccessful tries.

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- N is known.
- CHV1 has been presented unsuccessfully N-1 times.

Test

Reset the UC and present a CHANGE CHV command with P2 = "01", a wrong CHV to verify and a new CHV different from the previous one.

Result

The expected status word is "98 40".

RC_CC_IV_09 subclause 9.4.6 c19_16

Purpose

Check that CHANGE CHV returns "92 0X" if the internal retry routine has been used.

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- The internal memory can only be written after X retries.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a CHANGE CHV command with P2 = "01" and a new CHV different from the previous one.

Result

The expected status word is "92 0X".

RC_CC_IV_10 subclause 9.4.6 c19_16

Purpose

Check that CHANGE CHV returns "92 40" if the internal memory can not be written.

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- The internal memory can not be written.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a CHANGE CHV command with P2 = "01" and a new CHV different from the previous one.

Result

The expected status word is "92 40".

RC_CC_IV_11 subclause 9.4.6 c19_16

Purpose

Check that CHANGE CHV returns "6B XX" if the parameter P1 ≠ 00.

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a CHANGE CHV command with P2 = "01" and P1 ≠ 00 and a new CHV different from the previous one.

Result

The expected status word is "6B XX".

RC_CC_IV_12 subclause 9.4.6 c19_16

Purpose

Check that CHANGE CHV returns "6B XX" if the parameter P2 ≠ "01" and P2 ≠ "02".

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a CHANGE CHV command with P2 ≠ "01" and P2 ≠ "02" and a new CHV different from the previous one.

Result

The expected status word is "6B XX".

RC_CC_IV_13 subclause 9.4.6 c19_16

Purpose

Check that CHANGE CHV returns "67 XX" if the parameter L_c ≠ "10".

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a CHANGE CHV command with $L_c \neq$ "10" and a new CHV different from the previous one in a matching datafield.

Result

The expected status word is "67 XX".

6.2.3.17 DISABLE CHV (DC)

6.2.3.17.1 Function

FU_DC_VA_01 subclause 8.17 c19_17, c23_17, c23_1, c23_10, c12_5_1

Purpose

Check that the DISABLE CHV function can be performed successfully with CHV1.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- A transparent EF with AC READ = CHV1 exists.
- The CHV is not disabled.

Test

Reset the IUT.

Present a DISABLE CHV command.

Reset the IUT.

Present a SELECT command on the EF with AC READ = CHV1.

Present a READ BINARY command to read that file.

Result

The selected EF shall be readable.

FU_DC_VA_02 subclause 8.17 c19_17, c23_17, c23_1, c23_10, c12_5_1

Purpose

Check that the DISABLE CHV function can be performed successfully with CHV2.

Preconditions

- EF_{CHV2} exists.
- CHV is to be presented in clear.
- A transparent EF with AC READ = CHV2 exists.
- The CHV is not disabled.

Test

Reset the IUT.

Present a DISABLE CHV command.

Reset the IUT.

Present a SELECT command on the EF with AC READ = CHV2.

Present a READ BINARY command to read that file.

Result

The selected EF shall be readable.

FU_DC_VA_03 subclause 8.17 c19_17, c23_17, c23_15, c12_5_1

Purpose

Check that the DISABLE CHV function can reset the "remaining CHV attempts counter".

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- The CHV has been presented unsuccessfully N-1 times.
- The CHV is not disabled.

Test

Present a DISABLE CHV command with the correct CHV.

Present a VERIFY CHV command with the wrong CHV.

Result

The expected SW for the VERIFY CHV is "98 04".

FU_DC_VA_04 subclause 8.15 c19_17, c23_15, c12_5_1

Purpose

Check that the "remaining CHV attempts counter" remains blocked after N unsuccessful DISABLE CHV representations.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- The DISABLE CHV has been presented unsuccessfully N times.

Test

Present a DISABLE CHV command with the correct CHV.

Result

The expected SW for the DISABLE CHV is "98 40".

FU_DC_VA_05 subclause 8.17 c19_17, c23_17, c23_1, c23_10, c23_23, c12_5_2

Purpose

Check that the DISABLE CHV function can be used for an enciphered CHV.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented enciphered.

- A transparent EF with AC READ = CHV1 exists.
- A Random has been asked for.
- AC CHV1 is not yet fulfilled.
- The CHV is not disabled.

Test

Present a DISABLE CHV command with the CHV enciphered.

Present a SELECT command on the EF with AC READ = CHV1.

Present a READ BINARY command to read that file.

Result

The selected EF shall be readable.

FU_DC_VA_06 subclause 8.17 c19_17, c23_17, c23_1, c23_10, c12_1_2

Purpose

Check that the DISABLE CHV function can be performed successfully with CHV1 which stores a path to another CHV file.

Preconditions

- EF_{CHV1} exists containing path to existing CHV file.
- CHV is to be presented in clear.
- A transparent EF with AC READ = CHV1 exists.
- The CHV is not disabled.

Test

Reset the IUT.

Present a DISABLE CHV command.

Reset the IUT.

Present a SELECT command on the EF with AC READ = CHV1.

Present a READ BINARY command to read that file.

Result

The selected EF shall be readable.

6.2.3.17.2 Command

The coding of the DISABLE CHV command is the following:

Table 35: Return codes for the DISABLE CHV command

CLA	Class byte
INS	"26"
P1	"00" (other values are RFU)
P2	"01" for CHV1 "02" for CHV2
L_c field	"08"
Data field	Data sent to the card
L_e field	Empty

No tests are foreseen to test the DISABLE CHV command other than those defined in the functions subclause.

6.2.3.17.3 Return codes

The following return codes are defined for DISABLE CHV:

Table 36: Return codes for the DISABLE CHV command

Return Code	Error description
98 02	- No CHV defined
98 04	- Unsuccessful CHV verification but VERIFY CHV mechanism still possible (number of false consecutive verification < N)
98 08	- In contradiction with CHV status
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
98 40	- Unsuccessful CHV verification, VERIFY CHV mechanism no longer possible (number of false consecutive verifications >= N)
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00", P2 ≠ "01" and P2 ≠ "02"
67 XX	- L_c ≠ "08"
90 00	- Normal ending (ACK) of the command

RC_DC_VA_01 subclause 9.4.6 c19_17

Purpose
Check that DISABLE CHV returns "90 00", if used correctly.

Preconditions
- EF_{CHV1} exists and is enabled.
- CHV is known.
- CHV status allows DISABLE CHV.
- At least one attempt is allowed to present the CHV.

Test
Reset the UC and present a valid DISABLE CHV command with P2 = "01".

Result
The expected status word is "90 00".

RC_DC_IV_01 subclause 9.4.6 c19_17

Purpose
Check that DISABLE CHV returns "98 02", if no CHV is defined.

Preconditions
- EF_{CHV1} does not exist

Test

Reset the UC and present a valid DISABLE CHV command with P2 = "01".

Result

The expected status word is "98 02".

RC_DC_IV_02 subclause 9.4.6 c19_17

Purpose

Check that DISABLE CHV returns "98 04", if the presented CHV is false.

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- At least two false attempts are allowed to present the CHV.

Test

Reset the UC and present a DISABLE CHV command with P2 = "01" and a wrong CHV.

Result

The expected status word is "98 04".

RC_DC_IV_03 subclause 9.4.6 c19_17

Purpose

Check that DISABLE CHV returns "98 08", if the CHV is present but disabled.

Preconditions

- EF_{CHV1} exists.
- EF_{CHV1} is disabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a valid DISABLE CHV command with P2 = "01".

Result

The expected status word is "98 08".

RC_DC_IV_04 subclause 9.4.6 c19_17

Purpose

Check that DISABLE CHV returns "98 08", if the CHV is not activated.

Preconditions

- EF_{CHV1} exists.
- EF_{CHV1} is not activated (least significant bit in activation byte is set to 0).
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a valid DISABLE CHV command with P2 = "01".

Result

The expected status word is "98 08".

RC_DC_IV_05 subclause 9.4.6 c19_17

Purpose

Check that DISABLE CHV returns "98 10", if the CHV is not allowed to be disabled.

Preconditions

- EF_{CHV1} exists and is enabled.
- EF_{CHV1} is not allowed to be disabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a valid DISABLE CHV command with P2 = "01".

Result

The expected status word is "98 10".

RC_DC_IV_06 subclause 9.4.6 c19_17, c12_5_2

Purpose

Check that DISABLE CHV returns "98 35", if for an enciphered CHV no Random has been given.

Preconditions

- EF_{CHV1} exists and is enabled.
- EF_{CHV1} requires an enciphered CHV.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a DISABLE CHV command with P2 = "01" but present the CHVs in clear.

Result

The expected status word is "98 35".

RC_DC_IV_07 subclause 9.4.6 c19_17

Purpose

Check that DISABLE CHV returns "98 40", after N unsuccessful tries.

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- N is known.
- CHV1 has been presented unsuccessfully N-1 times.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a DISABLE CHV command with P2 = "01" and a wrong CHV.

Result

The expected status word is "98 40".

RC_DC_IV_08 subclause 9.4.6 c19_17

Purpose

Check that DISABLE CHV returns "92 0X" if the internal retry routine has been used.

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- The internal memory can only be written after X retries.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a DISABLE CHV command with P2 = "01".

Result

The expected status word is "92 0X".

RC_DC_IV_09 subclause 9.4.6 c19_17

Purpose

Check that DISABLE CHV returns "92 40" if the internal memory can not be written.

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- The internal memory can not be written.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a DISABLE CHV command with P2 = "01".

Result

The expected status word is "92 40".

RC_DC_IV_10 subclause 9.4.6 c19_17

Purpose

Check that DISABLE CHV returns "6B XX" if the parameter P1 ≠ "00".

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a DISABLE CHV command with P2 = "01" and P1 ≠ "00".

Result

The expected status word is "6B XX".

RC_DC_IV_11 subclause 9.4.6 c19_17

Purpose

Check that DISABLE CHV returns "6B XX" if the parameter P2 ≠ "01" and P2 ≠ "02".

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a DISABLE CHV command with P2 ≠ "01" and P2 ≠ "02".

Result

The expected status word is "6B XX".

RC_DC_IV_12 subclause 9.4.6 c19_17

Purpose

Check that DISABLE CHV returns "67 XX" if the parameter L_c ≠ "08".

Preconditions

- EF_{CHV1} exists and is enabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a DISABLE CHV command with L_c ≠ "08" and a matching datafield.

Result

The expected status word is "67 XX".

6.2.3.18 ENABLE CHV (EC)

6.2.3.18.1 Function

FU_EC_VA_01 subclause 8.18 c19_18, c23_18, c23_1, c23_10, c12_5_1

Purpose

Check that the ENABLE CHV function can be performed successfully with CHV1.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- A transparent EF with AC READ = CHV1 exists.
- The CHV is disabled.

Test

Reset the IUT.

Present a ENABLE CHV command.

Reset the IUT.

Present a SELECT command on the EF with AC READ = CHV1.

Present a READ BINARY command to read that file.

Result

The expected SW for READ BINARY is "98 04".

FU_EC_VA_02 subclause 8.18 c19_18, c23_18, c23_1, c23_10, c12_5_1

Purpose

Check that the ENABLE CHV function can be performed successfully with CHV2.

Preconditions

- EF_{CHV2} exists.
- CHV is to be presented in clear.
- A transparent EF with AC READ = CHV2 exists.
- The CHV is disabled.

Test

Reset the IUT.

Present a ENABLE CHV command.

Reset the IUT.

Present a SELECT command on the EF with AC READ = CHV2.

Present a READ BINARY command to read that file.

Result

The expected SW for READ BINARY is "98 04".

FU_EC_VA_03 subclause 8.18 c19_18, c23_18, c23_15, c12_5_1

Purpose

Check that the ENABLE CHV function can reset the "remaining CHV attempts counter".

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- The CHV has been presented unsuccessfully N-1 times.
- The CHV is disabled.

Test

Present a ENABLE CHV command with the correct CHV.

Present a VERIFY CHV command with the wrong CHV.

Result

The expected SW for the VERIFY CHV is "98 04".

FU_EC_VA_04 subclause 8.18 c19_18, c23_18, c23_1, c23_10, c23_23, c12_5_2

Purpose

Check that the DISABLE CHV function can be used for an enciphered CHV.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented enciphered.
- A transparent EF with AC READ = CHV1 exists.
- A Random has been asked for.
- The CHV is not disabled.

Test

Present an ENABLE CHV command.

Reset the IUT.

Present a SELECT command on the EF with AC READ = CHV1.

Present a READ BINARY command to read that file.

Result

The expected SW for READ BINARY is "98 04".

FU_EC_VA_05 subclause 8.15 c19_18, c23_18, c23_15, c12_5_1

Purpose

Check that the "remaining CHV attempts counter" remains blocked after N unsuccessful ENABLE CHV representations.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- The ENABLE CHV has been presented unsuccessfully N times.

Test

Present a ENABLE CHV command with the correct CHV.

Result

The expected SW for the ENABLE CHV is "98 40".

FU_EC_VA_06 subclause 8.18 c19_18, c23_18, c23_1, c23_10, c12_1_2

Purpose

Check that the ENABLE CHV function can be performed successfully with CHV1 which stores a path to another CHV file.

Preconditions

- EF_{CHV1} exists containing path to existing CHV file.

- CHV is to be presented in clear.
- A transparent EF with AC READ = CHV1 exists.
- The CHV is disabled.

Test

Reset the IUT.

Present a ENABLE CHV command.

Reset the IUT.

Present a SELECT command on the EF with AC READ = CHV1.

Present a READ BINARY command to read that file.

Result

The expected SW for READ BINARY is "98 04".

6.2.3.18.2 Command

The coding of the ENABLE CHV command is the following:

Table 37: Return codes for the ENABLE CHV command

CLA	Class byte
INS	"28"
P1	"00" (other values are RFU)
P2	"01" for CHV1 "02" for CHV2
L_c field	"08"
Data field	Data sent to the card
L_e field	Empty

No tests are foreseen to test the ENABLE CHV command other than those defined in the functions subclause.

6.2.3.18.3 Return codes

The following return codes are defined for ENABLE CHV:

Table 38: Return codes for the ENABLE CHV command

Return Code	Error description
98 02	– No CHV defined
98 04	– Unsuccessful CHV verification but VERIFY CHV mechanism still possible (number of false consecutive verification < N)
98 08	– In contradiction with CHV status
98 10	– In contradiction with the invalidation status
98 35	– No ASK RANDOM / GIVE RANDOM before
98 40	– Unsuccessful CHV verification, VERIFY CHV mechanism no longer possible (number of false consecutive verifications >= N)
92 0X	– Update successful but after using internal retry routine X times
92 40	– Update impossible (memory problem)
6E XX	– Wrong instruction class given in the command
6D XX	– Unknown instruction code given in the command
6F XX	– Technical problem with no diagnostic given (command aborted)
6B XX	– P1 ≠ "00", P2 ≠ "01" and P2 ≠ "02"
67 XX	– L_c ≠ "08"
90 00	– Normal ending (ACK) of the command

RC_EC_VA_01 subclause 9.4.6 c19_18

Purpose
Check that ENABLE CHV returns "90 00", if used correctly.

Preconditions
- EF_{CHV1} exists and is disabled.
- CHV is known.
- CHV status allows ENABLE CHV.
- At least one attempt is allowed to present the CHV.

Test
Reset the UC and present a valid ENABLE CHV command with P2 = "01".

Result
The expected status word is "90 00".

RC_EC_IV_01 subclause 9.4.6 c19_18

Purpose
Check that ENABLE CHV returns "98 02", if no CHV is defined.

Preconditions
- EF_{CHV1} does not exist

Test
Reset the UC and present a valid ENABLE CHV command with P2 = "01".

Result
The expected status word is "98 02".

RC_EC_IV_02 subclause 9.4.6 c19_18

Purpose
Check that ENABLE CHV returns "98 04", if the presented CHV is false.

Preconditions
- EF_{CHV1} exists and is disabled.
- CHV is known.
- At least two false attempts are allowed to present the CHV.

Test
Reset the UC and present a ENABLE CHV command with P2 = "01" and a wrong CHV.

Result
The expected status word is "98 04".

RC_EC_IV_03 subclause 9.4.6 c19_18

Purpose
Check that ENABLE CHV returns "98 08", if the CHV is present and enabled.

Preconditions
- EF_{CHV1} exists.
- EF_{CHV1} is enabled.
- CHV is known.

- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a valid ENABLE CHV command with P2 = "01".

Result

The expected status word is "98 08".

RC_EC_IV_04 subclause 9.4.6 c19_18

Purpose

Check that ENABLE CHV returns "98 08", if the CHV is not activated.

Preconditions

- EF_{CHV1} exists.
- EF_{CHV1} is not activated (least significant bit in activation byte is set to 0).
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a valid ENABLE CHV command with P2 = "01".

Result

The expected status word is "98 08".

RC_EC_IV_05 subclause 9.4.6 c19_18

Purpose

Check that ENABLE CHV returns "98 10", if the CHV is not allowed to be enabled.

Preconditions

- EF_{CHV1} exists and is disabled.
- EF_{CHV1} is not allowed to be enabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a valid ENABLE CHV command with P2 = "01".

Result

The expected status word is "98 10".

RC_EC_IV_06 subclause 9.4.6 c19_18, c12_5_1

Purpose

Check that ENABLE CHV returns "98 35", if for an enciphered CHV no Random has been given.

Preconditions

- EF_{CHV1} exists and is disabled.
- EF_{CHV1} requires an enciphered CHV.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present a ENABLE CHV command with P2 = "01" but present the CHVs in clear.

Result

The expected status word is "98 35".

RC_EC_IV_07 subclause 9.4.6 c19_18

Purpose

Check that ENABLE CHV returns "98 40", after N unsuccessful tries.

Preconditions

- EF_{CHV1} exists and is disabled.
- CHV is known.
- N is known.
- CHV1 has been presented unsuccessfully N-1 times.

Test

Reset the UC and present a ENABLE CHV command with P2 = "01" and a wrong CHV.

Result

The expected status word is "98 40".

RC_EC_IV_08 subclause 9.4.6 c19_18

Purpose

Check that ENABLE CHV returns "92 0X" if the internal retry routine has been used.

Preconditions

- EF_{CHV1} exists and is disabled.
- CHV is known.
- The internal memory can only be written after X retries.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present an ENABLE CHV command with P2 = "01".

Result

The expected status word is "92 0X".

RC_EC_IV_09 subclause 9.4.6 c19_18

Purpose

Check that ENABLE CHV returns "92 40" if the internal memory can not be written.

Preconditions

- EF_{CHV1} exists and is disabled.
- CHV is known.
- The internal memory can not be written.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present an ENABLE CHV command with P2 = "01".

Result

The expected status word is "92 40".

RC_EC_IV_10 subclause 9.4.6 c19_18

Purpose

Check that ENABLE CHV returns "6B XX" if the parameter P1 ≠ "00".

Preconditions

- EF_{CHV1} exists and is disabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present an ENABLE CHV command with P2 = "01" and P1 ≠ "00".

Result

The expected status word is "6B XX".

RC_EC_IV_11 subclause 9.4.6 c19_18

Purpose

Check that ENABLE CHV returns "6B XX" if the parameter P2 ≠ "01" and P2 ≠ "02".

Preconditions

- EF_{CHV1} exists and is disabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present an ENABLE CHV command with P2 ≠ "01" and P2 ≠ "02".

Result

The expected status word is "6B XX".

RC_EC_IV_12 subclause 9.4.6 c19_18

Purpose

Check that ENABLE CHV returns "67 XX" if the parameter L_c ≠ "08".

Preconditions

- EF_{CHV1} exists and is disabled.
- CHV is known.
- At least one attempt is allowed to present the CHV.

Test

Reset the UC and present an ENABLE CHV command with $L_c \neq$ "08" and a matching datafield.

Result

The expected status word is "67 XX".

6.2.3.19 UNBLOCK CHV (UC)

6.2.3.19.1 Function

FU_UC_VA_01 subclause 8.19 c19_19, c23_19, c23_15, c12_5_1

Purpose

Check that the UNBLOCK CHV function can be performed successfully with CHV1 if P2="00".

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- EF_{CHV1} is blocked.

Test

Present a UNBLOCK CHV command with P2="00".

Present a VERIFY CHV command with a wrong CHV.

Result

The expected SW for VERIFY CHV is "98 04".

FU_UC_VA_02 subclause 8.19 c19_19, c23_19, c23_15, c12_5_1

Purpose

Check that the UNBLOCK CHV function can be performed successfully with CHV1 if P2="01".

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- EF_{CHV1} is blocked.

Test

Present a UNBLOCK CHV command with P2="01".

Present a VERIFY CHV command with a wrong CHV.

Result

The expected SW for VERIFY CHV is "98 04".

FU_UC_VA_03 subclause 8.19 c19_19, c23_19, c12_5_1

Purpose

Check that the mechanism usage counter of UNBLOCK CHV is decremented after successful usage if it were not equal to "FF".

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- EF_{CHV1} is blocked.

- Mechanism counter known and not equal to "FF".

Test

Present an UNBLOCK CHV command.

Present a SELECT command for EF_{CHV1}.

Result

The UNBLOCK CHV shall have a successful result.

The SELECT RESPONSE shall indicate that the mechanism usage counter is decremented by 1.

FU_UC_VA_04 subclause 8.19 c19_19, c23_19, c12_5_1

Purpose

Check that the mechanism usage counter of UNBLOCK CHV is not decremented after successful usage if it was equal to "FF".

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- EF_{CHV1} is blocked.
- Mechanism counter known and equal to "FF".

Test

Present an UNBLOCK CHV command.

Present a SELECT command for EF_{CHV1}.

Result

The UNBLOCK CHV shall have a successful result.

The SELECT RESPONSE shall indicate that the mechanism usage counter is still "FF".

FU_UC_VA_05 subclause 8.19 c19_19, c23_19, c23_15, c12_5_1

Purpose

Check that the UNBLOCK CHV function can be performed successfully with CHV1 if CHV file is not blocked..

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- EF_{CHV1} is not blocked.

Test

Present an UNBLOCK CHV command.

Present a VERIFY CHV command with a wrong CHV.

Result

The UNBLOCK CHV shall have a successful result.

The expected SW for VERIFY CHV is "98 04".

FU_UC_VA_06 subclause 8.19 c19_19, c23_19, c23_15, c12_5_1

Purpose

Check that the UNBLOCK CHV function can be performed successfully with CHV1 and fulfils AC CHV1.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.
- EF_{CHV1} is blocked.
- Any transparent EF with known contents exists with AC CHV1 for read.

Test

Present an UNBLOCK CHV command.

Present a READ BINARY command on EF.

Result

The UNBLOCK CHV shall have a successful result.

The READ BINARY command should have a successful result and return expected data.

FU_UC_VA_07 subclause 8.19 c19_19, c23_19, c23_15, c12_5_1

Purpose

Check that the UNBLOCK CHV function can be performed successfully with CHV2.

Preconditions

- EF_{CHV2} exists.
- CHV is to be presented in clear.
- EF_{CHV2} is blocked.

Test

Present a UNBLOCK CHV command.

Present a VERIFY CHV command with a wrong CHV.

Result

The expected SW for VERIFY CHV is "98 04".

FU_UC_VA_08 subclause 8.19 c19_19, c23_19, c12_5_1

Purpose

Check that the UNBLOCK CHV function can reset the "remaining UNBLOCK CHV attempts counter".

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.

- The CHV has been presented unsuccessfully 9 times.

Test

Present an UNBLOCK CHV command with the correct UNBLOCK CHV.

Present an UNBLOCK CHV command with the wrong UNBLOCK CHV.

Result

The expected SW for the second UNBLOCK CHV is "98 04".

FU_UC_VA_09 subclause 8.19 c19_19, c23_19, c23_15, c12_5_2

Purpose

Check that the UNBLOCK CHV function can be used for an enciphered UNBLOCKCHV.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented enciphered.
- A Random has been asked for.
- EF_{CHV1} is blocked.

Test

Present an UNBLOCK CHV command.

Present a VERIFY CHV command with a wrong CHV.

Result

The expected SW for VERIFY CHV is "98 04".

FU_UC_VA_10 subclause 8.19 c19_19, c23_19, c23_15, c12_1_2

Purpose

Check that the UNBLOCK CHV function can be performed successfully with CHV1 which stores a path to another CHV file.

Preconditions

- EF_{CHV1} exists containing path to existing CHV file.
- CHV is to be presented in clear.
- EF_{CHV1} is blocked.

Test

Present a UNBLOCK CHV command with P2 = "00".

Present a VERIFY CHV command with a wrong CHV.

Result

The expected SW for VERIFY CHV is "98 04".

FU_UC_IV_01 subclause 8.19 c19_19, c23_19, c12_5_1

Purpose

Check that UNBLOCK CHV does not succeed if the mechanism usage counter of the CHV file is zero.

Preconditions

- EF_{CHV1} exists.
- CHV is to be presented in clear.

- EF_{CHV1} is blocked.
- Unblock mechanism counter equal to zero.
- Unblock CHV is known.

Test

Present an UNBLOCK CHV command with a correct UNBLOCK CHV.

Result

The UNBLOCK CHV shall have a negative result "9840".

6.2.3.19.2 Command

The coding of the UNBLOCK CHV command is the following:

Table 39: Return codes for the UNBLOCK CHV command

CLA	Class byte
INS	"2C"
P1	"00" (other values are RFU)
P2	"00","01" for CHV1 "02" for CHV2
L_c field	"10"
Data field	Data sent to the card
L_e field	Empty

No tests are foreseen to test the UNBLOCK CHV command other than those defined in the functions subclause.

6.2.3.19.3 Return codes

The following return codes are defined for UNBLOCK CHV:

Table 40: Return codes for the UNBLOCK CHV command

Return Code	Error description
98 02	- No CHV defined
98 04	- Unsuccessful UNBLOCK CHV verification but UNBLOCK CHV mechanism still possible (number of false consecutive verification < 10)
98 08	- In contradiction with CHV status
98 35	- No ASK RANDOM / GIVE RANDOM before
98 40	- Unsuccessful UNBLOCK CHV verification, UNBLOCK CHV mechanism no longer possible (number of false consecutive verifications >= 10)
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00", P2 ≠ "01" and P2 ≠ "02"
67 XX	- L_c ≠ "10"
90 00	- Normal ending (ACK) of the command

RC_UC_VA_01 subclause 9.4.6 c19_19

Purpose

Check that UNBLOCK CHV returns "90 00", if used correctly.

Preconditions

- EF_{CHV1} exists, is enabled and blocked.
- Unblock CHV is known.

- UNBLOCK CHV mechanism is still possible.

Test

Reset the UC and present a valid UNBLOCK CHV command with P2 = "01".

Result

The expected status word is "90 00".

RC_UC_IV_01 subclause 9.4.6 c19_19

Purpose

Check that UNBLOCK CHV returns "98 02", if no CHV is defined.

Preconditions

- EF_{CHV1} does not exist

Test

Reset the UC and present a valid UNBLOCK CHV command with P2 = "01".

Result

The expected status word is "98 02".

RC_UC_IV_02 subclause 9.4.6 c19_19

Purpose

Check that UNBLOCK CHV returns "98 04", if the presented unblock CHV is false.

Preconditions

- EF_{CHV1} exists, is enabled and blocked.

- Unblock CHV is known.

- At least two false attempts are allowed to present the unblock CHV.

Test

Reset the UC and present a UNBLOCK CHV command with P2 = "01" and a wrong unblock CHV.

Result

The expected status word is "98 04".

RC_UC_IV_03 subclause 9.4.6 c19_19

Purpose

Check that UNBLOCK CHV returns "98 08", if the CHV is present and disabled.

Preconditions

- EF_{CHV1} exists, is disabled and blocked.

- Unblock CHV is known.

Test

Reset the UC and present a valid UNBLOCK CHV command with P2 = "01".

Result

The expected status word is "98 08".

RC_UC_IV_04 subclause 9.4.6 c19_19

Purpose

Check that UNBLOCK CHV returns "98 08", if the CHV is not activated.

Preconditions

- EF_{CHV1} exists, is not activated (least significant bit in activation byte is set to 0) and blocked.

- Unblock CHV is known.

Test

Reset the UC and present a valid UNBLOCK CHV command with P2 = "01".

Result

The expected status word is "98 08".

RC_UC_IV_05 subclause 9.4.6 c19_19, c12_5_2

Purpose

Check that UNBLOCK CHV returns "98 35", if for an enciphered CHV no Random has been given.

Preconditions

- EF_{CHV1} exists, is enabled and blocked.
- EF_{CHV1} requires an enciphered CHV.
- Unblock CHV is known.
- UNBLOCK CHV mechanism is still possible.

Test

Reset the UC and present an UNBLOCK CHV command with P2 = "01" but present the unblock CHV and the new CHV in clear.

Result

The expected status word is "98 35".

RC_UC_IV_06 subclause 9.4.6 c19_19

Purpose

Check that UNBLOCK CHV returns "98 40", after 10 unsuccessful attempts.

Preconditions

- EF_{CHV1} exists, is enabled and blocked.
- Unblock CHV is known.
- The unblock CHV has been presented unsuccessfully 9 times.

Test

Reset the UC and present a UNBLOCK CHV command with P2 = "01" and a wrong unblock CHV.

Result

The expected status word is "98 40".

RC_UC_IV_07 subclause 9.4.6 c19_19

Purpose

Check that UNBLOCK CHV returns "92 0X" if the internal retry routine has been used.

Preconditions

- EF_{CHV1} exists, is enabled and blocked.
- Unblock CHV is known.
- The internal memory can only be written after X retries.
- UNBLOCK CHV mechanism is still possible.

Test

Reset the UC and present an UNBLOCK CHV command with P2 = "01".

Result

The expected status word is "92 0X".

RC_UC_IV_08 subclause 9.4.6 c19_19

Purpose

Check that UNBLOCK CHV returns "92 40" if the internal memory can not be written.

Preconditions

- EF_{CHV1} exists, is enabled and blocked.
- Unblock CHV is known.
- The internal memory can not be written.
- UNBLOCK CHV mechanism is still possible.

Test

Reset the UC and present an UNBLOCK CHV command with P2 = "01".

Result

The expected status word is "92 40".

RC_UC_IV_09 subclause 9.4.6 c19_19

Purpose

Check that UNBLOCK CHV returns "6B XX" if the parameter P1 ≠ "00".

Preconditions

- EF_{CHV1} exists, is enabled and blocked.
- Unblock CHV is known.
- UNBLOCK CHV mechanism is still possible.

Test

Reset the UC and present an UNBLOCK CHV command with P2 = "01" and P1 ≠ "00".

Result

The expected status word is "6B XX".

RC_UC_IV_10 subclause 9.4.6 c19_19

Purpose

Check that UNBLOCK CHV returns "6B XX" if the parameter P2 ≠ "00", P2 ≠ "01" and P2 ≠ "02".

Preconditions

- EF_{CHV1} exists, is enabled and blocked.
- Unblock CHV is known.
- UNBLOCK CHV mechanism is still possible.

Test

Reset the UC and present an UNBLOCK CHV command with P2 ≠ "01" and P2 ≠ "02".

Result

The expected status word is "6B XX".

RC_UC_IV_11 subclause 9.4.6 c19_19

Purpose

Check that UNBLOCK CHV returns "67 XX" if the parameter L_c ≠ "10".

Preconditions

- EF_{CHV1} exists, is enabled and blocked.
- Unblock CHV is known.
- UNBLOCK CHV mechanism is still possible.

Test

Reset the UC and present an UNBLOCK CHV command with L_c ≠ "10" and a matching datafield.

Result

The expected status word is "67 XX".

6.2.3.20 INVALIDATE (IV)

6.2.3.20.1 Function

FU_IV_VA_01 subclause 8.20 c19_20, c23_20, c23_1, c23_7

Purpose

Check that the INVALIDATE function can be applied successfully to an EF.

Preconditions

- Current File is transparent EF (not a keyfile) and writable;

Test

Perform an INVALIDATE command. Check by means of the UPDATE BINARY command whether the invalidation was successful.

Result

The INVALIDATE command shall have a positive return code while the UPDATE BINARY command shall fail.

FU_IV_VA_02 subclause 8.20 c19_20, c23_20, c23_1, c23_3

Purpose

Check that the INVALIDATE function can be applied successfully to a DF.

Preconditions

- Current File is DF;

Test

Perform an INVALIDATE command. Check by means of the CREATE FILE command whether the invalidation was successful.

Result

The INVALIDATE command shall have a positive return code while the CREATE FILE command shall fail.

FU_IV_VA_03 subclause 8.20 c19_20, c23_20, c23_1, c23_23, c23_25

Purpose
Check that the INVALIDATE function can be applied successfully to an EF_{KEY_OP}.

Preconditions
- Current File is an EF_{KEY_OP};

Test
Perform an INVALIDATE command. Check by means of the ASK RANDOM and EXTERNAL AUTHENTICATION commands whether the invalidation was successful.

Result
The INVALIDATE command shall have a positive return code while the EXTERNAL AUTHENTICATION command shall fail.

6.2.3.20.2 Command

The coding of the INVALIDATE command is the following:

Table 41: Return codes for the INVALIDATE command

CLA	Class byte
INS	"04"
P1	"00"
P2	"00"
L_c field	Empty or length of data field
Data field	Empty or cryptogram
L_e field	Empty

No tests are foreseen to test the INVALIDATE command other than those defined in the functions subclause.

6.2.3.20.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 42: Return codes for the INVALIDATE command

Return Code	Error description
98 02	– No key defined
98 04	– AC not fulfilled
98 10	– In contradiction with the invalidation status
98 35	– No ASK RANDOM / GIVE RANDOM before
92 0X	– Update successful but after using internal retry routine X times
92 40	– Update impossible (memory problem)
94 08	– Current file is inconsistent with the command
6E XX	– Wrong instruction class given in the command
6D XX	– Unknown instruction code given in the command
6F XX	– Technical problem with no diagnostic given (command aborted)
6B XX	– P1 ≠ "00" or P2 ≠ "00"
67 XX	– L_c ≠ "00" (+ X)
90 00	– Normal ending (ACK) of the command

RC_IV_VA_01 subclause 9.4.6 c19_20

Purpose
Check that INVALIDATE returns "90 00" if used correctly.

Preconditions
- A not invalidated EF is selected.

- The AC for INVALIDATE is fulfilled, no cryptogram is required.

Test

Present an INVALIDATE command.

Result

The expected status word is "90 00".

RC_IV_IV_01 subclause 9.4.6 c19_20

Purpose

Check that INVALIDATE returns "98 02" if the key associated to INVALIDATE does not exist.

Preconditions

- A not invalidated EF is selected.
- The key associated to INVALIDATE is not existing.
- The AC for INVALIDATE is PRO.
- A random has been asked for.

Test

Present an INVALIDATE command with any cryptogram appended.

Result

The expected status word is "98 02".

RC_IV_IV_02 subclause 9.4.6 c19_20

Purpose

Check that INVALIDATE returns "98 04" if the AC for INVALIDATE is not fulfilled.

Preconditions

- A not invalidated EF is selected.
- The AC for INVALIDATE is not fulfilled, no cryptogram is required.

Test

Present an INVALIDATE command.

Result

The expected status word is "98 04".

RC_IV_IV_03 subclause 9.4.6 c19_20

Purpose

Check that INVALIDATE returns "98 10" if the selected file is invalidated.

Preconditions

- An invalidated EF is selected.
- The AC for INVALIDATE is fulfilled, no cryptogram is required.

Test

Present an INVALIDATE command.

Result

The expected status word is "98 10".

RC_IV_IV_04 subclause 9.4.6 c19_20

Purpose

Check that INVALIDATE returns "98 35" if no random has been asked for.

Preconditions

- A not invalidated EF is selected.
- The AC for INVALIDATE is PRO.
- No random has been asked for.

Test

Present an INVALIDATE command with any cryptogram appended.

Result

The expected status word is "98 35".

RC_IV_IV_05 subclause 9.4.6 c19_20

Purpose

Check that INVALIDATE returns "92 0X" if the internal retry routine has been used.

Preconditions

- A not invalidated EF is selected.
- The AC for INVALIDATE is fulfilled, no cryptogram is required.
- The internal memory can only be written after X retries.

Test

Present an INVALIDATE command.

Result

The expected status word is "92 0X".

RC_IV_IV_06 subclause 9.4.6 c19_20

Purpose

Check that INVALIDATE returns "92 40" if the internal memory can not be written.

Preconditions

- A not invalidated EF is selected.
- The AC for INVALIDATE is fulfilled, no cryptogram is required.
- The internal memory can not be written.

Test

Present an INVALIDATE command.

Result

The expected status word is "92 40".

RC_IV_IV_07 subclause 9.4.6 c19_20

Purpose

Check that INVALIDATE returns "94 08" if file to be invalidated is EF_{KEY_MAN}.

Preconditions

- A not invalidated EF_{KEY_MAN} is selected.
- The AC for INVALIDATE is fulfilled, no cryptogram is required.

Test

Present an INVALIDATE command.

Result

The expected status word is "98 35".

RC_IV_IV_08 subclause 9.4.6 c19_20

Purpose

Check that INVALIDATE returns "6B XX" if P1 ≠ "00" or P2 ≠ "00".

Preconditions

- A not invalidated EF is selected.
- The AC for INVALIDATE is fulfilled, no cryptogram is required.

Test

Present an INVALIDATE command with P1 ≠ "00" or P2 ≠ "00".

Result

The expected status word is "6B XX".

RC_IV_IV_09 subclause 9.4.6 c19_20

Purpose

Check that INVALIDATE returns "67 XX" if L_c ≠ "00" + X.

Preconditions

- A not invalidated EF is selected.
- The AC for INVALIDATE is fulfilled, no cryptogram is required.

Test

Present an INVALIDATE command with $L_c \neq$ "00" and any data.

Result

The expected status word is "67 XX".

6.2.3.21 REHABILITATE (RH)

6.2.3.21.1 Function

FU_RH_VA_01 subclause 8.21 c19_21, c23_21, c23_1, c23_7

Purpose

Check that the REHABILITATE function can be applied successfully to an EF.

Preconditions

- Current File is transparent EF (not a keyfile), normally writable but invalidated;

Test

Perform an REHABILITATE command. Check by means of the UPDATE BINARY command whether the rehabilitation was successful.

Result

Both commands shall have a positive return code.

FU_RH_VA_02 subclause 8.21 c19_21, c23_21, c23_1, c23_3

Purpose

Check that the REHABILITATE function can be applied successfully to a DF.

Preconditions

- Current File is DF;

Test

Perform an REHABILITATE command. Check by means of the CREATE FILE command whether the rehabilitation was successful.

Result

Both commands shall have a positive return code.

FU_RH_VA_03 subclause 8.21 c19_21, c23_21, c23_1, c23_23, c23_25

Purpose

Check that the REHABILITATE function can be applied successfully to an EF_{KEY_OP}.

Preconditions

- Current File is an EF_{KEY_OP};

Test

Perform an REHABILITATE command. Check by means of the ASK RANDOM and EXTERNAL AUTHENTICATION commands whether the rehabilitation was successful.

Result

All three commands shall have a positive return code.

6.2.3.21.2 Command

The coding of the Rehabilitate command is the following:

Table 43: Return codes for the REHABILITATE command

CLA	Class byte
INS	"44"
P1	"00"
P2	"00"
L_c field	Empty or length of data field
Data field	Empty or cryptogram
L_e field	Empty

No tests are foreseen to test the REHABILITATE command other than those defined in the functions subclause.

6.2.3.21.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 44: Return codes for the REHABILITATE command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
94 08	- Current file is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" or P2 ≠ "00"
67 XX	- L_c ≠ "00" (+ X)
90 00	- Normal ending (ACK) of the command

RC_RH_VA_01 subclause 9.4.6 c19_21

Purpose
Check that REHABILITATE returns "90 00" if used correctly.

Preconditions
- An invalidated EF is selected.
- The AC for REHABILITATE is fulfilled, no cryptogram is required.

Test
Present an REHABILITATE command.

Result
The expected status word is "90 00".

RC_RH_IV_01 subclause 9.4.6 c19_21

Purpose
Check that REHABILITATE returns "98 02" if the key associated to REHABILITATE does not exist.

Preconditions
- An invalidated EF is selected.
- The key associated to REHABILITATE is not existing.

- The AC for REHABILITATE is PRO.
- A random has been asked for.

Test
Present an REHABILITATE command with any cryptogram appended.

Result
The expected status word is "98 02".

RC_RH_IV_02 subclause 9.4.6 c19_21

Purpose
Check that REHABILITATE returns "98 04" if the AC for REHABILITATE is not fulfilled.

Preconditions
- An invalidated EF is selected.
- The AC for REHABILITATE is not fulfilled, no cryptogram is required.

Test
Present an REHABILITATE command.

Result
The expected status word is "98 04".

RC_RH_IV_03 subclause 9.4.6 c19_21

Purpose
Check that REHABILITATE returns "98 10" if the selected file is not invalidated.

Preconditions
- A not invalidated EF is selected.
- The AC for REHABILITATE is fulfilled, no cryptogram is required.

Test
Present an REHABILITATE command.

Result
The expected status word is "98 10".

RC_RH_IV_04 subclause 9.4.6 c19_21

Purpose
Check that REHABILITATE returns "98 35" if no random has been asked for.

Preconditions
- An invalidated EF is selected.
- The AC for REHABILITATE is PRO.
- No random has been asked for.

Test

Present an REHABILITATE command with any cryptogram appended.

Result

The expected status word is "98 35".

RC_RH_IV_05 subclause 9.4.6 c19_21

Purpose

Check that REHABILITATE returns "92 0X" if the internal retry routine has been used.

Preconditions

- An invalidated EF is selected.
- The AC for REHABILITATE is fulfilled, no cryptogram is required.
- The internal memory can only be written after X retries.

Test

Present an REHABILITATE command.

Result

The expected status word is "92 0X".

RC_RH_IV_06 subclause 9.4.6 c19_21

Purpose

Check that REHABILITATE returns "92 40" if the internal memory can not be written.

Preconditions

- An invalidated EF is selected.
- The AC for REHABILITATE is fulfilled, no cryptogram is required.
- The internal memory can not be written.

Test

Present an REHABILITATE command.

Result

The expected status word is "92 40".

RC_RH_IV_07 subclause 9.4.6 c19_21

Purpose

Check that REHABILITATE returns "6B XX" if P1 ≠ "00" or P2 ≠ "00".

Preconditions

- An invalidated EF is selected.
- The AC for REHABILITATE is fulfilled, no cryptogram is required.

Test

Present an REHABILITATE command with P1 ≠ "00" or P2 ≠ "00".

Result

The expected status word is "6B XX".

RC_RH_IV_08 subclause 9.4.6 c19_21

Purpose

Check that REHABILITATE returns "67 XX" if L_c ≠ "00" + X.

Preconditions

- An invalidated EF is selected.
- The AC for REHABILITATE is fulfilled, no cryptogram is required.

Test

Present an REHABILITATE command with L_c ≠ "00" and any data.

Result

The expected status word is "67 XX".

6.2.3.22 INTERNAL AUTHENTICATION (IA)

6.2.3.22.1 Function

FU_IA_VA_01 subclause 8.22 c19_22, c23_22, c23_1

Purpose

Check that the INTERNAL AUTHENTICATION function performs correctly on a key from EF_{KEY_OP}.

Preconditions

- A key valid for INTERNAL AUTHENTICATION exists in EF_{KEY_OP}.
- An EF is selected.

Test

Present an INTERNAL AUTHENTICATION function.

Result

The expected status word is "90 00" and the returned cryptogram has to be correct.

FU_IA_VA_02 subclause 8.22 c19_22, c23_22, c23_1

Purpose

Check that the INTERNAL AUTHENTICATION function performs correctly on a key from EF_{KEY_MAN}.

Preconditions

- A key valid for INTERNAL AUTHENTICATION exists in EF_{KEY_MAN}.
- A MF/DF or keyfile is selected.

Test

Present an INTERNAL AUTHENTICATION function.

Result

The expected status word is "90 00" and the returned cryptogram has to be correct.

6.2.3.22.2 Command

The coding of the INTERNAL AUTHENTICATION command is the following:

Table 45: Return codes for the INTERNAL AUTHENTICATION command

CLA	Class byte
INS	"88"
P1	"00" (other values are RFU)
P2	Key Number "00" - "0F"
L_c field	Length of the challenge
Data field	Challenge
L_e field	Length of the cryptogram

No tests are foreseen to test the INTERNAL AUTHENTICATION command other than those defined in the functions subclause.

6.2.3.22.3 Return codes

Table 46: Return codes for the INTERNAL AUTHENTICATION command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled (note)
98 10	- In contradiction with the invalidation status
92 40	- no test is foreseen for this status word
94 08	- Current file type is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" or P2 > "0F"
67 XX	- no test is foreseen for this status word
90 00	- Normal ending (ACK) of the command
9F XX	- Length "XX" of the response data
NOTE: This error occurs if VERIFY CHV is required before INTERNAL AUTHENTICATION (byte 8) of DF at creation time (CR).	

RC_IA_VA_01 subclause 9.4.6 c19_22, c4_9

Purpose

Check that INTERNAL AUTHENTICATION returns "90 00" if used correctly.

Preconditions

- A key valid for internal authentication is available in EF_{KEY_OP}.
- A VERIFY CHV has been done if necessary for the selected DF.
- An EF is selected.

Test

Present an INTERNAL AUTHENTICATION command.

Result

The expected status word is "90 00".

RC_IA_VA_02 subclause 9.4.6 c19_22, c4_8

Purpose

Check that INTERNAL AUTHENTICATION returns "9F XX" if used correctly.

Preconditions

- A key valid for internal authentication is available in EF_{KEY_OP}.
- A VERIFY CHV has been done if necessary for the selected DF.
- An EF is selected.

Test

Present an INTERNAL AUTHENTICATION command.

Result

The expected status word is "9F XX".

RC_IA_IV_01 subclause 9.4.6 c19_22

Purpose

Check that INTERNAL AUTHENTICATION returns "98 02" if the indicated key does not exist.

Preconditions

- A VERIFY CHV has been done if necessary for the selected DF.
- An EF is selected.

Test

Present an INTERNAL AUTHENTICATION command indicating in P2 a Nonexisting key in EF_{KEY_OP}.

Result

The expected status word is "98 02".

RC_IA_IV_02 subclause 9.4.6 c19_22

Purpose

Check that INTERNAL AUTHENTICATION returns "98 04" if a CHV has not been presented and the DF indicates that it is necessary.

Preconditions

- A key valid for internal authentication is available in EF_{KEY_OP}.
- A DF requiring a VERIFY CHV before INTERNAL AUTHENTICATION is selected.
- A VERIFY CHV has not been done.
- An EF is selected.

Test

Present an INTERNAL AUTHENTICATION command.

Result

The expected status word is "98 04".

RC_IA_IV_03 subclause 9.4.6 c19_22, c9_1

Purpose

Check that INTERNAL AUTHENTICATION returns "98 10" if EF_{KEY_OP} is invalidated.

Preconditions

- A key valid for internal authentication is available in EF_{KEY_OP}.
- EF_{KEY_OP} is invalidated.
- A VERIFY CHV has been done if necessary for the selected DF.
- An EF is selected.

Test

Present an INTERNAL AUTHENTICATION command.

Result

The expected status word is "98 10".

RC_IA_IV_04 subclause 9.4.6 c19_22

Purpose

Check that INTERNAL AUTHENTICATION returns "94 08" if the selected file is the MF.

Preconditions

- A key valid for internal authentication is available in EF_{KEY_OP}.
- A VERIFY CHV has been done if necessary for the selected DF.
- The MF is selected.

Test

Present an INTERNAL AUTHENTICATION command.

Result

The expected status word is "94 08".

RC_IA_IV_05 subclause 9.4.6 c19_22

Purpose

Check that INTERNAL AUTHENTICATION returns "6B XX" if P1 ≠ "00".

Preconditions

- A key valid for internal authentication is available in EF_{KEY_OP}.
- A VERIFY CHV has been done if necessary for the selected DF.

Test

Present an INTERNAL AUTHENTICATION command with P1 ≠ "00".

Result

The expected status word is "6B XX".

6.2.3.23 ASK RANDOM (AR)

6.2.3.23.1 Function

FU_AR_VA_01 subclause 8.23 c19_23, c23_23, c23_25

Purpose
Check that the ASK RANDOM function response is used in the next function.

Preconditions
- None.

Test
Present an ASK RANDOM command.

Present an EXTERNAL AUTHENTICATION command with a cryptogram using the random and a valid key.

Result
The expected status word is "90 00" for both functions.

FU_AR_VA_02 subclause 8.23 c19_23, c23_23, c23_25

Purpose
Check that the random of the ASK RANDOM function is valid only once.

Preconditions
- ASK RANDOM has been given.
- EXTERNAL AUTHENTICATION has been performed successfully once.

Test
Present an EXTERNAL AUTHENTICATION command with a cryptogram using the random and a valid key.

Result
The expected status word is "98 35".

6.2.3.23.2 Command

The coding of the ASK RANDOM command is the following:

Table 47: Return codes for the ASK RANDOM command

CLA	Class byte
INS	"84"
P1	"00" (other values are RFU)
P2	"00" (other values are RFU)
L_c field	Empty
Data field	Empty
L_e field	Maximum length of data expected in response

CO_AR_VA_01 subclause 9.2.23 c19_23, c23_23, c23_25

Purpose
Check that the ASK RANDOM returns random values with different length.

Preconditions
- None.

Test

Present an ASK RANDOM command with L_e = "08".

Present an ASK RANDOM command with L_e = "10".

Result

The first 8 bytes of both random values shall be different.

The second random shall have a length of 16 byte.

The expected status word for both commands is "90 00".

6.2.3.23.3 Return codes

Table 48: Return codes for the ASK RANDOM command

Return Code	Error description
92 40	- no test is foreseen for this status word
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" or P2 ≠ "00"
67 XX	- no test is foreseen for this status word
90 00	- Normal ending (ACK) of the command

RC_AR_VA_01 subclause 9.4.6 c19_23

Purpose

Check that ASK RANDOM returns "90 00", if used correctly.

Preconditions

- None.

Test

Present a valid ASK RANDOM command.

Result

The expected status word is "90 00".

RC_AR_IV_01 subclause 9.4.6 c19_23

Purpose

Check that ASK RANDOM returns "6B XX" if the parameter P1 ≠ "00" or P2 ≠ "00".

Preconditions

- None.

Test

Present a ASK RANDOM command with P1 ≠ "00" or P2 ≠ "00".

Result

The expected status word is "6B XX".

6.2.3.24 GIVE RANDOM (GR)

6.2.3.24.1 Function

FU_GR_VA_01 subclause 8.24 c19_24, c23_24, c23_1, c23_22

Purpose

Check that the card uses the random submitted by the GIVE RANDOM function.

Preconditions

- None

Test

Present a GIVE RANDOM command.

Present an INTERNAL AUTHENTICATION command.

Result

The expected status word for both commands is "90 00".

The cryptogram returned by INTERNAL AUTHENTICATION shall be correct.

6.2.3.24.2 Command

The coding of the GIVE RANDOM command is the following:

Table 49: Return codes for the GIVE RANDOM command

CLA	Class byte
INS	"86"
P1	"00" (other values are RFU)
P2	"00" (other values are RFU)
L_c field	Number of data bytes
Data field	Data sent to the card
L_e field	Empty

No tests are foreseen to test the GIVE RANDOM command other than those defined in the functions subclause.

CO_GR_VA_01 subclause 9.2.24 c19_24, c23_24

Purpose

Check that the card handles extreme random values correctly.

Preconditions

- Readable EF is present and selected.

Test

Present a GIVE RANDOM command with random value "00 00....00".

Present a READ BINARY STAMPED command

Result

Both commands shall have a positive return code and the stamp shall be calculated correctly

CO_GR_VA_02 subclause 9.2.24 c19_24, c23_24

Purpose

Check that the Card handles extreme random values correctly.

Preconditions

- Readable EF is present and selected.

Test

Present a GIVE RANDOM command with random value "FF FF....FF".

Present a READ BINARY STAMPED command

Result

Both commands shall have a positive return code and the stamp shall be calculated correctly

6.2.3.24.3 Return codes

Table 50: Return codes for the GIVE RANDOM command

Return Code	Error description
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" or P2 ≠ "00"
67 XX	- no test is foreseen for this status word
92 40	- no test is foreseen for this status word
90 00	- Normal ending (ACK) of the command

RC_GR_VA_01 subclause 9.4.6 c19_24

Purpose

Check that GIVE RANDOM returns "90 00", if used correctly.

Preconditions

- None.

Test

Present a valid GIVE RANDOM command.

Result

The expected status word is "90 00".

RC_GR_IV_01 subclause 9.4.6 c19_24

Purpose

Check that GIVE RANDOM returns "6B XX" if the parameter P1 ≠ "00" or P2 ≠ "00".

Preconditions

- None.

Test

Present a GIVE RANDOM command with P1 ≠ "00" or P2 ≠ "00".

Result

The expected status word is "6B XX".

6.2.3.25 EXTERNAL AUTHENTICATION (EA)

6.2.3.25.1 Function

FU_EA_VA_01 subclause 8.25 c19_25, c23_25, c23_1, c23_10, c23_23

Purpose

Check that the EXTERNAL AUTHENTICATION function performs correctly on a key from EF_{KEY_OP}.

Preconditions

- An EF is selected.
- A transparent EF with AC AUT on READ exists.
- A random has been asked for.

Test

Present an EXTERNAL AUTHENTICATION function using the key for AC READ.

Present a READ BINARY function on the transparent file.

Result

The expected status word is "90 00" for both functions and the transparent EF has been read successfully.

FU_EA_VA_02 subclause 8.25 c19_25, c23_25, c23_1, c23_4, c23_23

Purpose

Check that the EXTERNAL AUTHENTICATION function performs correctly on a key from EF_{KEY_MAN}.

Preconditions

- A DF is selected.
- The AC for DELETE FILE is AUT.
- A file which can be deleted is available.
- A random has been asked for.

Test

Present an EXTERNAL AUTHENTICATION function using the key for the AC on DELETE FILE.

Present a DELETE FILE function.

Present a SELECT function on that deleted file.

Result

The expected status word is "90 00" for the first two functions and "9404" for the SELECT function.

6.2.3.25.2 Command

The coding of the INTERNAL AUTHENTICATION command is the following:

Table 51: Return codes for the EXTERNAL AUTHENTICATION command

CLA	Class byte
INS	"82"
P1	"00" (other values are RFU)
P2	"00" (other values are RFU)
L_c field	Length of the data
Data field	Data to be sent to the card
L_e field	Empty

No tests are foreseen to test the EXTERNAL AUTHENTICATION command other than those defined in the functions subclause.

6.2.3.25.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 52: Return codes for the EXTERNAL AUTHENTICATION command

Return Code	Error description
98 02	- No key defined / key not valid for function
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" or P2 ≠ "00"
67 XX	- L_c > "01" + X
90 00	- Normal ending (ACK) of the command

RC_EA_VA_01 subclause 9.4.6 c19_25, c4_9

Purpose

Check that EXTERNAL AUTHENTICATION returns "90 00" if used correctly.

Preconditions

- The given key exists in EF_{KEY_OP}.
- A random has been asked for.
- An EF is selected.

Test

Present an EXTERNAL AUTHENTICATION command.

Result

The expected status word is "90 00".

RC_EA_IV_01 subclause 9.4.6 c19_25

Purpose

Check that EXTERNAL AUTHENTICATION returns "98 02" if the indicated key does not exist.

Preconditions

- A random has been asked for.
- An EF is selected.

Test

Present an EXTERNAL AUTHENTICATION command with a datafield indicating a non existing key.

Result

The expected status word is "98 02".

RC_EA_IV_02 subclause 9.4.6 c19_25

Purpose

Check that EXTERNAL AUTHENTICATION returns "98 04" if the given cryptogram is not correct.

Preconditions

- The given key exists in EF_{KEY_OP}.
- A random has been asked for.
- An EF is selected.

Test

Present an EXTERNAL AUTHENTICATION command, with a wrong cryptogram.

Result

The expected status word is "98 04".

RC_EA_IV_03 subclause 9.4.6 c19_25, c9_1

Purpose

Check that EXTERNAL AUTHENTICATION returns "98 10" if EF_{KEY_OP} is invalidated.

Preconditions

- The given key exists in EF_{KEY_OP}.
- A random has been asked for.
- An EF is selected.
- EF_{KEY_OP} is invalidated.

Test
Present an EXTERNAL AUTHENTICATION command.

Result
The expected status word is "98 10".

RC_EA_IV_04 subclause 9.4.6 c19_25

Purpose
Check that EXTERNAL AUTHENTICATION returns "98 35" if no random has been asked for.

Preconditions
- The given key exists in EF_{KEY_OP}.
- A random has not been asked for.
- An EF is selected.

Test
Present an EXTERNAL AUTHENTICATION command.

Result
The expected status word is "98 35".

RC_EA_IV_05 subclause 9.4.6 c19_25

Purpose
Check that EXTERNAL AUTHENTICATION returns "92 0X" if the internal retry routine has been used to write the fulfilled AC.

Preconditions
- The given key exists in EF_{KEY_OP}.
- A random has been asked for.
- An EF is selected.
- The internal memory can only be written after X retries.

Test
Present an EXTERNAL AUTHENTICATION command.

Result
The expected status word is "92 0X".

RC_EA_IV_06 subclause 9.4.6 c19_25

Purpose
Check that EXTERNAL AUTHENTICATION returns "92 40" if the memory can not be written with the fulfilled AC.

Preconditions
- The given key exists in EF_{KEY_OP}.
- A random has been asked for.
- An EF is selected.
- The internal memory can not be written.

Test

Present an EXTERNAL AUTHENTICATION command.

Result

The expected status word is "92 40".

RC_EA_IV_07 subclause 9.4.6 c19_25

Purpose

Check that EXTERNAL AUTHENTICATION returns "6B XX" if P1 ≠ "00" or P2 ≠ "00".

Preconditions

- The given key exists in EF_{KEY_OP}.
- A random has been asked for.
- An EF is selected.

Test

Present an EXTERNAL AUTHENTICATION command with P1 ≠ "00" or P2 ≠ "00".

Result

The expected status word is "6B XX".

RC_EA_IV_08 subclause 9.4.6 c19_25

Purpose

Check that EXTERNAL AUTHENTICATION returns "67 XX" if L_c > "01" + X.

Preconditions

- The given key exists in EF_{KEY_OP}.
- A random has been asked for.
- An EF is selected.

Test

Present an EXTERNAL AUTHENTICATION command with a data field which contain any additional data.

Result

The expected status word is "67 XX".

6.2.3.26 CLOSE APPLICATION (CA)

6.2.3.26.1 Function

FU_CA_VA_01 subclause 8.26 c19_26, c23_26, c23_10, c23_1

Purpose

Check that the card is can perform a CLOSE APPLICATION function and a fulfilled AUT AC is reset.

Preconditions

- The AC AUT has been fulfilled in a DF.
- A transparent file exists, which AC for READ is AUT with the same key as the fulfilled AC.

Test

Present a CLOSE APPLICATION function.

Present a SELECT function on the transparent EF

Present a READ BINARY function.

Result

The expected status word is "90 00" for the first 2 commands and "98 04" for the READ command.

FU_CA_VA_02 subclause 8.26 c19_26, c23_26, c23_10, c23_1, c10_2

Purpose

Check that the card is can perform a CLOSE APPLICATION function and a fulfilled CHV AC is reset.

Preconditions

- The AC CHV1 has been fulfilled in a DF.
- A transparent file exists, which AC for READ is CHV1.

Test

Present a CLOSE APPLICATION function.

Present a SELECT function on the transparent EF

Present a READ BINARY function.

Result

The expected status word is "90 00" for the first 2 commands and "98 04" for the READ command.

6.2.3.26.2 Command

The coding of the CLOSE APPLICATION command is the following:

Table 53: Return codes for the CLOSE APPLICATION command

CLA	Class byte
INS	"AC"
P1	File-ID
P2	File-ID
L_c field	Empty
Data field	Empty
L_e field	Empty

No tests are foreseen to test the CLOSE APPLICATION command other than those defined in the functions subclause.

6.2.3.26.3 Return codes

Table 54: Return codes for the CLOSE APPLICATION command

Return Code	Error description
92 40	- no test is foreseen for this status word
94 04	- File ID not found
94 08	- Current file type is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- no test is foreseen for this status word
67 XX	- no test is foreseen for this status word
90 00	- Normal ending (ACK) of the command

RC_CA_VA_01 subclause 9.4.6 c19_26

Purpose
Check that CLOSE APPLICATION returns "90 00", if used correctly.

Preconditions
- A DF exists.

Test
Present a CLOSE APPLICATION command with P1 and P2 giving the DF-ID.

Result
The expected status word is "90 00".

RC_CA_IV_01 subclause 9.4.6 c19_26

Purpose
Check that CLOSE APPLICATION returns "94 04" if the given DF is not existing.

Preconditions
- None.

Test
Present a CLOSE APPLICATION command with P1 and P2 giving a DF - ID of a not existing DF.

Result
The expected status word is "94 04".

RC_CA_IV_02 subclause 9.4.6 c19_26

Purpose
Check that CLOSE APPLICATION returns "94 08" if the given ID is not a DF - ID.

Preconditions
- None.

Test
Present a CLOSE APPLICATION command with P1 = "00" and P2 = "02", that is giving the ID of EF_{ICC}.

Result
The expected status word is "94 08".

6.2.3.27 WRITE BINARY (WB)

6.2.3.27.1 Function

FU_WB_VA_01 subclause 8.27 c19_27, c23_27, c23_1, c23_10

Purpose
Check that the WRITE BINARY function can be performed.

Preconditions
- Writable transparent EF selected;

Test

Try to write a number of bytes to the EF. Then try to read them back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ BINARY command was performed shall be in accordance with the data written in that EF by the WRITE BINARY command and the original data in the EF.

FU_WB_IV_01 subclause 8.27 c19_27, c23_27, c23_1, c23_10

Purpose

Check that WRITE BINARY does not write into the EF if AC is not fulfilled.

Preconditions

- A transparent EF with known contents is selected.
- The AC for WRITE is not fulfilled, no cryptogram is required.

Test

Present a WRITE BINARY command with offset "0000", that is P1 = "00", P2 = "00" and L_c = "01".

Check by means of READ BINARY if file contents did not change.

Result

The expected status word for WRITE BINARY is "98 04" while the READ BINARY returns a positive return code and the unchanged file contents.

6.2.3.27.2 Command

The coding of the WRITE BINARY command is the following:

Table 55: Return codes for the WRITE BINARY command

CLA	Class byte
INS	"D0"
P1	Offset
P2	Offset
L_c field	Length of data field
Data field	Data to be updated (+cryptogram)
L_e field	Empty

CO_WB_VA_01 subclause 9.27 c23_27, c23_1, c23_10

Purpose

Check that the WRITE BINARY command can be performed using a large amount of data.

Preconditions

- Writable transparent non-empty (at least 256 bytes) EF (with known contents) selected;

Test

Try to write the maximum number of bytes allowed by the IUT to the EF in one WRITE BINARY command. Then try to read them back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ BINARY command was performed shall be in accordance with the data written in that EF by the WRITE BINARY command and the original data in the EF.

6.2.3.27.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 56: Return codes for the WRITE BINARY command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
92 0X	- WRITE successful but after using internal retry routine X times
92 40	- WRITE impossible (memory problem)
94 00	- No EF selected as current
94 02	- Out of range (invalid address)
94 08	- Current file type is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- (P1, P2) > file length
67 XX	- (P1, P2) + L_c > file length
90 00	- Normal ending (ACK) of the command

RC_WB_VA_01 subclause 9.4.6 c19_27, c4_9

Purpose

Check that WRITE BINARY returns "90 00" if used correctly.

Preconditions

- A transparent EF is selected.
- The AC for WRITE is fulfilled, no cryptogram is required.

Test

Present an WRITE BINARY command with P1 = "00", P2 = "00" and L_c = "01".

Result

The expected status word is "90 00".

RC_WB_IV_01 subclause 9.4.6 c19_27

Purpose

Check that WRITE BINARY returns "98 02" if the key associated with the file does not exist.

Preconditions

- A transparent EF with a not existing key associated to WRITE is selected.
- The AC for WRITE is PRO.
- A random has been asked for.

Test

Present a WRITE BINARY command with offset "0000", that is P1 = "00", P2 = "00", any cryptogram and L_c = "01" + X.

Result

The expected status word is "98 02".

RC_WB_IV_02 subclause 9.4.6 c19_27

Purpose

Check that WRITE BINARY returns "98 04" if the selected file has an unfulfilled access condition on WRITE.

Preconditions

- A transparent EF is selected.
- The AC for WRITE is not fulfilled, no cryptogram is required.

Test

Present an WRITE BINARY command with offset "0000", that is P1 = "00", P2 = "00" and L_c = "01".

Result

The expected status word is "98 04".

RC_WB_IV_03 subclause 9.4.6 c19_27

Purpose

Check that WRITE BINARY returns "98 10" if the selected file is invalidated.

Preconditions

- A transparent invalidated EF is selected.
- The AC for WRITE is fulfilled, no cryptogram is required.

Test

Present a WRITE BINARY command with offset "0000", that is P1 = "00", P2 = "00" and L_c = "01".

Result

The expected status word is "98 10".

RC_WB_IV_04 subclause 9.4.6 c19_27

Purpose

Check that WRITE BINARY returns "98 35" if no random has been asked for.

Preconditions

- A transparent EF is selected.
- The AC for WRITE is PRO.
- No random has been asked for.

Test

Present a WRITE BINARY command with offset "0000", that is P1 = "00", P2 = "00", any cryptogram and L_c = "01" + X.

Result

The expected status word is "98 35".

RC_WB_IV_05 subclause 9.4.6 c19_27

Purpose

Check that WRITE BINARY returns "92 0X" if the internal retry routine has been used.

Preconditions

- A transparent EF is selected.
- The AC for WRITE is fulfilled, no cryptogram is required.
- The internal memory can only be written after X retries.

Test

Present an WRITE BINARY command with P1 = "00", P2 = "00" and L_c = "01".

Result

The expected status word is "92 0X".

RC_WB_IV_06 subclause 9.4.6 c19_27

Purpose

Check that WRITE BINARY returns "92 40" if the internal memory can not be written.

Preconditions

- A transparent EF is selected.
- The AC for WRITE is fulfilled, no cryptogram is required.
- The internal memory can not be written.

Test

Present an WRITE BINARY command with P1 = "00", P2 = "00" and L_c = "01".

Result

The expected status word is "92 40".

RC_WB_IV_07 subclause 9.4.6 c19_27

Purpose

Check that WRITE BINARY returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.

Test

Present an WRITE BINARY command with offset "0000", that is P1 = "00", P2 = "00" and L_c = "01".

Result

The expected status word is "94 00".

RC_WB_IV_08 subclause 9.4.6 c19_27

Purpose

Check that WRITE BINARY returns "94 08" if a file, not valid for WRITE BINARY is selected.

Preconditions

- EF_{KEY_MAN} is selected.

Test

Present an WRITE BINARY command with offset "0000", that is P1 = "00", P2 = "00" and L_c = "01".

Result

The expected status word is "94 08".

RC_WB_IV_09 subclause 9.4.6 c19_27

Purpose

Check that WRITE BINARY returns "6B XX" or "94 02" if the offset is greater than the file size.

Preconditions

- A transparent EF is selected.
- The AC for WRITE is fulfilled, no cryptogram is required.
- The length of the file is 20 byte.

Test

Present a WRITE BINARY command with offset "0014", that is P1 = "00", P2 = "14" and L_c = "01".

Result

The expected status word is "6B XX" or "94 02".

6.2.3.28 WRITE RECORD (WR)

6.2.3.28.1 Function

FU_WR_VA_01 subclause 8.28 c19_28, c23_28, c23_1, c23_12

Purpose

Check that the WRITE RECORD function can be performed in FIRST mode.

Preconditions

- Writable linear fixed structure EF selected;

Test

Try to write a record in FIRST mode. Then try to read it back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the WRITE RECORD command and the original data in the EF.

FU_WR_VA_02 subclause 8.28 c19_28, c23_28, c23_1, c23_12

Purpose

Check that the WRITE RECORD function can be performed in LAST mode.

Preconditions

- Writable linear fixed structure EF selected;

Test

Try to write a record in LAST mode. Then try to read it back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the WRITE RECORD command and the original data in the EF.

FU_WR_VA_03 subclause 8.28 c19_28, c23_28, c23_1, c23_12

Purpose

Check that the WRITE RECORD function can be performed in NEXT mode.

Preconditions

- Writable linear fixed structure EF selected;
- Current record is known and not first nor last record

Test

Try to write a record in NEXT mode. Then try to read it back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the WRITE RECORD command and the original data in the EF.

FU_WR_VA_04 subclause 8.28 c19_28, c23_28, c23_1, c23_12

Purpose

Check that the WRITE RECORD function can be performed in PREVIOUS mode.

Preconditions

- Writable linear fixed structure EF selected;
- Current record is known and not first nor last record

Test

Try to write a record in PREVIOUS mode. Then try to read it back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the WRITE RECORD command and the original data in the EF.

FU_WR_VA_05 subclause 8.28 c19_28, c23_28, c23_1, c23_12

Purpose

Check that the WRITE RECORD function can be performed in ABSOLUTE mode.

Preconditions

- Writable linear fixed structure EF selected;

Test

Try to write a record in ABSOLUTE mode. Then try to read it back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the WRITE RECORD command and the original data in the EF.

FU_WR_VA_06 subclause 8.28 c19_28, c23_28, c23_1, c23_12

Purpose

Check that the WRITE RECORD function can be performed in CURRENT mode.

Preconditions

- Writable linear fixed structure EF selected;
- Current record is known and not first nor last record

Test

Try to write a record in CURRENT mode. Then try to read it back.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the WRITE RECORD command and the original data in the EF.

FU_WR_IV_01 subclause 8.28 c19_28, c23_28, c23_1, c23_12

Purpose

Check that WRITE RECORD does not write into the EF if AC is not fulfilled.

Preconditions

- A linear fixed EF with known contents is selected.
- The AC for WRITE is not fulfilled, no cryptogram is required.

Test

Present a WRITE RECORD command with P1 = "00", P2 = "03" and L_c = record length.

Check by means of READ RECORD if file contents did not change.

Result

The expected status word for WRITE RECORD is "98 04" while the READ RECORD returns a positive return code and the unchanged file contents.

6.2.3.28.2 Command

The coding of the WRITE RECORD command is the following:

Table 57: Return codes for the WRITE RECORD command

CLA	Class byte
INS	"D2"
P1	Record no.
P2	Mode
L_c field	Length of data field
Data field	Data to be updated (+cryptogram)
L_e field	Empty

No tests are foreseen to test the WRITE RECORD command other than those defined in the functions subclause.

6.2.3.28.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 58: Return codes for the WRITE RECORD command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
92 0X	- WRITE successful but after using internal retry routine X times
92 40	- WRITE impossible (memory problem)
94 00	- No EF selected as current
94 02	- Out of range
94 04	- Record not found
94 08	- Current file type is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P2 > "04"
67 XX	- $L_c \neq$ record length (+ X)
90 00	- Normal ending (ACK) of the command

RC_WR_VA_01 subclause 9.4.6 c19_28, c4_9

Purpose

Check that WRITE RECORD returns "90 00" if used correctly.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for WRITE is fulfilled, no cryptogram is required.

Test

Present an WRITE RECORD command with P1 = "00", P2 = "03" and L_c = record length.

Result

The expected status word is "90 00".

RC_WR_IV_01 subclause 9.4.6 c19_28

Purpose

Check that WRITE RECORD returns "98 02" if the key associated with the file does not exist.

Preconditions

- An EF with linear fixed structure with a not existing key associated to WRITE is selected.
- The AC for WRITE is PRO.
- A random has been asked for.

Test

Present an WRITE RECORD command with P1 = "00", P2 = "03" and L_c = record length + X.

Result

The expected status word is "98 02".

RC_WR_IV_02 subclause 9.4.6 c19_28

Purpose

Check that WRITE RECORD returns "98 04" if the selected file has an unfulfilled access condition on WRITE.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for WRITE is not fulfilled, no cryptogram is required.

Test

Present an WRITE RECORD command with P1 = "00", P2 = "03" and L_c = record length.

Result

The expected status word is "98 04".

RC_WR_IV_03 subclause 9.4.6 c19_28

Purpose

Check that WRITE RECORD returns "98 10" if the selected file is invalidated.

Preconditions

- An invalidated EF with linear fixed structure is selected.
- The AC for WRITE is fulfilled, no cryptogram is required.

Test

Present an WRITE RECORD command with P1 = "00", P2 = "03" and L_c = record length.

Result

The expected status word is "98 10".

RC_WR_IV_04 subclause 9.4.6 c19_28

Purpose

Check that WRITE RECORD returns "98 35" if no random has been asked for.

Preconditions

- An EF with linear fixed structure is selected.

- The AC for WRITE is PRO.
- No random has been asked for.

Test

Present an WRITE RECORD command with P1 = "00", P2 = "03" and L_c = record length + X.

Result

The expected status word is "98 35".

RC_WR_IV_05 subclause 9.4.6 c19_28

Purpose

Check that WRITE RECORD returns "92 0X" if the internal retry routine has been used.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for WRITE is fulfilled, no cryptogram is required.
- The internal memory can only be written after X retries.

Test

Present an WRITE RECORD command with P1 = "00", P2 = "03" and L_c = record length.

Result

The expected status word is "92 0X".

RC_WR_IV_06 subclause 9.4.6 c19_28

Purpose

Check that WRITE RECORD returns "92 40" if the internal memory can not be written.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for WRITE is fulfilled, no cryptogram is required.
- The internal memory can not be written.

Test

Present an WRITE RECORD command with P1 = "00", P2 = "03" and L_c = record length.

Result

The expected status word is "92 40".

RC_WR_IV_07 subclause 9.4.6 c19_28

Purpose

Check that WRITE RECORD returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.

Test

Present an WRITE RECORD command with P1 = "00", P2 = "03" and L_c = record length.

Result

The expected status word is "94 00".

RC_WR_IV_08 subclause 9.4.6 c19_28

Purpose

Check that WRITE RECORD returns "94 02" or "94 04" if the addressed record is not found.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for WRITE is fulfilled, no cryptogram is required.
- The number of records in that EF is known.

Test

Present an WRITE RECORD command with P1 > number of existing records, P2 = "04" and L_c = record length.

Result

The expected status word is "94 02" or "94 04".

RC_WR_IV_09 subclause 9.4.6 c19_28

Purpose

Check that WRITE RECORD returns "94 08" if a file, not valid for WRITE RECORD is selected.

Preconditions

- EF_{KEY_MAN} is selected.

Test

Present an WRITE RECORD command with P1 = "00", P2 = "03" and L_c = record length.

Result

The expected status word is "94 08".

RC_WR_IV_10 subclause 9.4.6 c19_28

Purpose

Check that WRITE RECORD returns "6B XX" if P2 > "04".

Preconditions

- An EF with linear fixed structure is selected.
- The AC for WRITE is fulfilled, no cryptogram is required.

Test

Present an WRITE RECORD command with P1 = "00", P2 > "04" and L_c = record length.

Result

The expected status word is "6B XX".

RC_WR_IV_11 subclause 9.4.6 c19_28

Purpose

Check that WRITE RECORD returns "67 XX" if the length of the datafield is greater than the record length.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for WRITE is fulfilled, no cryptogram is required.

Test

Present an WRITE RECORD command with P1 = "00", P2 = "03" and L_c > record length.

Result

The expected status word is "67 XX".

RC_WR_IV_12 subclause 9.4.6 c19_28

Purpose

Check that WRITE RECORD returns "67 XX" if the length of the datafield is less than the record length.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for WRITE is fulfilled, no cryptogram is required.

Test

Present an WRITE RECORD command with P1 = "00", P2 = "03" and L_c < record length.

Result

The expected status word is "67 XX".

6.2.3.29 LOCK (LO)

6.2.3.29.1 Function

FU_LO_VA_01 subclause 8.29 c19_29, c23_29, c23_1, c23_7

Purpose

Check that the LOCK function can be applied successfully to an EF.

Preconditions

- Current File is transparent EF (not a keyfile);

Test

Perform a LOCK command for group 2.

Check by means of the SELECT command whether the locking was successful.

Perform an UPDATE Command.

Result

Both commands shall have a positive return code while the SELECT response will show the status of the locked function groups. Update shall fail returning error code "Access Condition not fulfilled".

FU_LO_VA_02 subclause 8.29 c19_29, c23_29, c23_1

Purpose

Check that the LOCK function can be applied successfully to a DF.

Preconditions

- Current File is DF;

Test

Perform a LOCK command for group 3.

Check by means of the SELECT command whether the locking was successful.

Perform a DELETE FILE command.

Result

Both commands shall have a positive return code while the SELECT response will show the status of the locked function groups. DELETE FILE shall fail returning error code "Access Condition not fulfilled".

FU_LO_VA_03 subclause 8.29 c19_29, c23_29, c23_1

Purpose

Check that the LOCK function can be applied successfully to an EF_{KEY_OP}.

Preconditions

- Current File is an EF_{KEY_OP};

Test

Perform a LOCK command for group 1. Check by means of the SELECT command whether the locking was successful.

Result

Both commands shall have a positive return code while the SELECT response will show the status of the locked function groups.

FU_LO_VA_04 subclause 8.29 c19_29, c23_29, c23_1

Purpose

Check that the LOCK function to a non keyfile is rejected.

Preconditions

- Current File is an EF different from an EF_KEY file;

Test

Perform a LOCK command for group 1. Check by means of the SELECT command whether the locking has any effect on AC.

Result

LOCK shall fail.

SELECT shall return an unchanged AC for group 1.

6.2.3.29.2 Command

The coding of the LOCK command is the following:

Table 59: Return codes for the LOCK command

CLA	Class byte
INS	"76"
P1	Group
P2	"00"
L_c field	Length of data field
Data field	File ID
L_e field	Empty

CO_LO_VA_01 subclause 9.29 c23_29, c23_1, c23_7

Purpose
Check that the LOCK command can be applied successfully to an EF for locking function group 2.

Preconditions
- Current File is transparent EF (not a keyfile);

Test
Perform a LOCK command for group 2. Check by means of the SELECT command whether the locking was successful.

Result
Both commands shall have a positive return code while the SELECT response will show the status of the locked function groups.

CO_LO_VA_02 subclause 9.29 c23_29, c23_1, c23_7

Purpose
Check that the LOCK command can be applied successfully to an EF for locking function group 3.

Preconditions
- Current File is transparent EF (not a keyfile);

Test
Perform a LOCK command for group 3. Check by means of the SELECT command whether the locking was successful.

Result
Both commands shall have a positive return code while the SELECT response will show the status of the locked function groups.

CO_LO_VA_03 subclause 9.29 c23_29, c23_1, c23_7

Purpose
Check that the LOCK command can be applied successfully to an EF for locking function group 4.

Preconditions
- Current File is transparent EF (not a keyfile);

Test
Perform a LOCK command for group 4. Check by means of the SELECT command whether the locking was successful.

Result
Both commands shall have a positive return code while the SELECT response will show the status of the locked function groups.

CO_LO_VA_04 subclause 9.29 c23_29, c23_1, c23_7

Purpose
Check that the LOCK command can be applied successfully to an EF for locking function group 5.

Preconditions
- Current File is transparent EF (not a keyfile);

Test

Perform a LOCK command for group 5. Check by means of the SELECT command whether the locking was successful.

Result

Both commands shall have a positive return code while the SELECT response will show the status of the locked function groups.

CO_LO_VA_05 subclause 9.29 c23_29, c23_1, c23_7

Purpose

Check that the LOCK command can be applied successfully to an EF for locking function group 6.

Preconditions

- Current File is transparent EF (not a keyfile);

Test

Perform a LOCK command for group 6. Check by means of the SELECT command whether the locking was successful.

Result

Both commands shall have a positive return code while the SELECT response will show the status of the locked function groups.

CO_LO_VA_06 subclause 9.29 c23_29, c23_1, c23_7

Purpose

Check that the LOCK command can be applied successfully to an EF for locking all function groups.

Preconditions

- Current File is an EF (not a keyfile);

Test

Perform a LOCK command for all function groups except group 1. Check by means of the SELECT command whether the locking was successful.

Result

Both commands shall have a positive return code while the SELECT response will show the status of the locked function groups.

6.2.3.29.3 Return codes

Table 60: Return codes for the LOCK command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
94 04	- File ID not found
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 > "3F" or P2 ≠ "00"
67 XX	- $L_c \neq$ "02"
90 00	- Normal ending (ACK) of the command

RC_LO_VA_01 subclause 9.4.6 c19_29

Purpose
Check that LOCK returns "90 00" if used correctly.

Preconditions
- None.

Test
Present a LOCK command with an ID of an existing transparent EF and a LOCK request for UPDATE.

Result
The expected status word is "90 00".

RC_LO_IV_01 subclause 9.4.6 c19_29

Purpose
Check that the LOCK command returns "98 04" if AC defined in the parent DF are not fulfilled.

Preconditions
- A DF with at least one EF in it is selected.
- Access Condition defined for LOCK in the current DF is not fulfilled, no cryptogram is required.

Test
Present a LOCK command with an ID of an existing transparent EF and a LOCK request for UPDATE.

Result
The expected status word is "98 04".

RC_LO_IV_02 subclause 9.4.6 c19_29

Purpose
Check that LOCK returns "92 0X" if the internal retry routine has been used.

Preconditions
- The internal memory can only be written after X retries.

Test
Present a LOCK command with an ID of an existing transparent EF and a LOCK request for UPDATE.

Result
The expected status word is "92 0X".

RC_LO_IV_03 subclause 9.4.6 c19_29

Purpose
Check that LOCK returns "92 40" if the internal memory can not be written.

Preconditions
- The internal memory can not be written.

Test

Present a LOCK command with an ID of an existing transparent EF and a LOCK request for UPDATE.

Result

The expected status word is "92 40".

RC_LO_IV_04 subclause 9.4.6 c19_29

Purpose

Check that LOCK returns "94 04" if the file ID could not be found.

Preconditions

- None.

Test

Present a LOCK command with an ID of a not existing EF and any LOCK request.

Result

The expected status word is "94 04".

RC_LO_IV_05 subclause 9.4.6 c19_29

Purpose

Check that LOCK returns "6B XX" if P1 > "3F" or P2 ≠ "00".

Preconditions

- None.

Test

Present a LOCK command with an ID of an existing transparent EF and a LOCK request for UPDATE.

Result

The expected status word is "6B XX".

RC_LO_IV_06 subclause 9.4.6 c19_29

Purpose

Check that LOCK returns "67 XX" if L_c ≠ "02".

Preconditions

- None.

Test

Present a LOCK command with an ID of an existing transparent EF and a LOCK request for UPDATE.

Result

The expected status word is "67 XX".

6.2.3.30 DECREASE (DEC)

6.2.3.30.1 Function

FU_DEC_VA_01 subclause 8.30 c19_30, c23_30, c23_1, c23_12

Purpose

Check that the DECREASE function can be performed successfully.

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known and larger than the value to deduct;

Test

Perform a DECREASE command with an arbitrary value. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE command and the original data in the EF.

6.2.3.30.2 Command

The coding of the DECREASE command is the following:

Table 61: Return codes for the DECREASE command

CLA	Class byte
INS	"30"
P1	"00"
P2	"00"
L_c field	Length of data field
Data field	Value to be deducted (+cryptogram)
L_e field	Maximum length of data expected in response

CO_DEC_VA_01 subclause 9.30 c23_30, c23_1, c23_12

Purpose

Check that the DECREASE command can be performed successfully with a small one byte value.

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known and larger than "03";

Test

Perform a DECREASE command with value "03". Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE command and the original data in the EF.

CO_DEC_VA_02 subclause 9.30 c23_30, c23_1, c23_12

Purpose

Check that the DECREASE command can be performed successfully with a two byte value.

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known and larger than "7483";

Test

Perform a DECREASE command with value "7483". Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE command and the original data in the EF.

CO_DEC_VA_03 subclause 9.30 c23_32, c23_1, c23_12

Purpose

Check that the DECREASE command can be performed successfully with a large three byte value.

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known and larger than "E27DA9";

Test

Perform a DECREASE command with value "E27DA9". Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE command and the original data in the EF.

CO_DEC_VA_04 subclause 9.30 c23_32, c23_1, c23_12

Purpose

Check that the DECREASE command can be performed successfully when the value of the L_e field is larger then the maximal response length.

Preconditions

- Writable cyclic EF with 3 byte records rexists;
- EF is selected and value of current record is known and larger than "A3AE";

Test

Perform a DECREASE command with value "A3AE" and request a 4 byte reponse. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE command and the original data in the EF.

6.2.3.30.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 62: Return codes for the DECREASE command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
98 50	- DECREASE cannot be performed (Minimum value reached)
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
94 00	- No EF selected as current
94 08	- Current file is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" or P2 ≠ "00"
67 XX	- $L_c \neq 3$ (+X)
90 00	- Normal ending (ACK) of the command
9F XX	- Length "XX" of the response data

RC_DEC_VA_01 subclause 9.4.6 c19_30, c4_9

Purpose

Check that DECREASE returns "90 00" if used correctly.

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.

Test

Present an DECREASE command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "90 00".

RC_DEC_VA_02 subclause 9.4.6 c19_30, c4_8

Purpose

Check that DECREASE returns "9F XX" if used correctly.

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.

Test

Present an DECREASE command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "9F XX".

RC_DEC_IV_01 subclause 9.4.6 c19_30

Purpose

Check that DECREASE returns "98 02" if the key associated with the file does not exist.

Preconditions

- An EF with cyclic structure with a not existing key associated to DECREASE is selected.
- The AC for DECREASE is PRO.
- A random has been asked for.

Test

Present an DECREASE command with P1 = "00", P2 = "00", L_c = "03" + X and a datafield followed by any cryptogram.

Result

The expected status word is "98 02".

RC_DEC_IV_02 subclause 9.4.6 c19_30

Purpose

Check that DECREASE returns "98 04" if the selected file has an unfulfilled access condition on DECREASE.

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is not fulfilled, no cryptogram is required.

Test

Present an DECREASE command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "98 04".

RC_DEC_IV_03 subclause 9.4.6 c19_30

Purpose

Check that DECREASE returns "98 10" if the selected file is invalidated.

Preconditions

- An invalidated EF with cyclic is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.

Test

Present an DECREASE command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "98 10".

RC_DEC_IV_04 subclause 9.4.6 c19_30

Purpose

Check that DECREASE returns "98 35" if no random has been asked for.

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is PRO.
- No random has been asked for.

Test

Present an DECREASE command with P1 = "00", P2 = "00", L_c = "03" + X and a datafield followed by any cryptogram.

Result

The expected status word is "98 35".

RC_DEC_IV_05 subclause 9.4.6 c19_30

Purpose

Check that DECREASE returns "98 50" if the minimum value has been reached.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.
- The minimum value has been reached.

Test

Present an DECREASE command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "98 50".

RC_DEC_IV_06 subclause 9.4.6 c19_30

Purpose

Check that DECREASE returns "92 0X" if the internal retry routine has been used.

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.
- The internal memory can only be written after X retries.

Test

Present an DECREASE command with P1 = "00", P2 = "00" and Lc = "03".

Result

The expected status word is "92 0X".

RC_DEC_IV_07 subclause 9.4.6 c19_30

Purpose

Check that DECREASE returns "92 40" if the internal memory can not be written.

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.
- The internal memory can not be written.

Test

Present an DECREASE command with P1 = "00", P2 = "00" and Lc = "03".

Result

The expected status word is "92 40".

RC_DEC_IV_08 subclause 9.4.6 c19_30

Purpose

Check that DECREASE returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.

Test

Present an DECREASE command with P1 = "00", P2 = "00" and Lc = "03".

Result

The expected status word is "94 00".

RC_DEC_IV_09 subclause 9.4.6 c19_30

Purpose

Check that DECREASE returns "94 08" if a file, not valid for DECREASE is selected.

Preconditions

- EF_{KEY_MAN} is selected.

Test

Present an DECREASE command with P1 = "00", P2 = "00" and Lc = "03".

Result

The expected status word is "94 08".

RC_DEC_IV_10 subclause 9.4.6 c19_30

Purpose

Check that DECREASE returns "6B XX" if P1 ≠ "00" or P2 ≠ "00".

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.

Test

Present an DECREASE command with P1 ≠ "00" or P2 ≠ "00" and Lc = "03".

Result

The expected status word is "6B XX".

RC_DEC_IV_11 subclause 9.4.6 c19_30

Purpose

Check that DECREASE returns "67 XX" if Lc ≠ 03 (+X).

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.

Test

Present an DECREASE command with P1 = "00", P2 = "00", Lc ≠ "03" with a matching datafield.

Result

The expected status word is "67 XX".

6.2.3.31 DECREASE STAMPED (DS)

6.2.3.31.1 Function

FU_DS_VA_01 subclause 8.31 c19_31, c23_31, c23_1, c23_12, c23_24

Purpose

Check that the DECREASE STAMPED function can be performed successfully.

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known and larger than the value to deduct;
- A random has been given.

Test

Perform a DECREASE STAMPED command with an arbitrary value. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the DECREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE STAMPED command and the original data in the EF.

FU_DS_VA_02 subclause 8.31 c19_31, c23_31, c23_1, c23_12, c23_24, c23_23

Purpose

Check that the DECREASE STAMPED function can be performed successfully on an EF with AC PRO for DECREASE.

Preconditions

- Writable cyclic EF with AC PRO on DECREASE exists;
- EF is selected and value of current record is known and larger than the value to deduct;
- A random has been given.
- A random has been asked for.

Test

Perform a DECREASE STAMPED command with a cryptogram created with the random of ASK RANDOM and an arbitrary value. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the DECREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE STAMPED command and the original data in the EF.

6.2.3.31.2 Command

The coding of the DECREASE command is the following:

Table 63: Return codes for the DECREASE STAMPED command

CLA	Class byte
INS	"34"
P1	"00" No Command header included in the cryptogram. "01" (CLA, INS, P1, P2) of DECREASE STAMPED is included in the cryptogram. "02" (CLA, INS, P1, P2) of INCREASE STAMPED is included in the cryptogram. "03" (CLA, INS, P1, P2) of the DECREASE command is included in the cryptogram. "04" (CLA, INS, P1, P2) of the INCREASE command is included in the cryptogram.
P2	"00"
L_c field	Length of data field
Data field	Value to be deducted (+ cryptogram)
L_e field	Maximum length of data expected in response

CO_DS_VA_01 subclause 9.2.31 c23_31, c23_1, c23_12, c23_24

Purpose

Check that the DECREASE STAMPED command can be performed successfully with a small one byte value.

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known and larger than "03";
- A random has been given.

Test

Perform a DECREASE STAMPED command with value "03" and P1 = "00". Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the DECREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE STAMPED command and the original data in the EF.

CO_DS_VA_02 subclause 9.2.31 c23_31, c23_1, c23_12, c23_24

Purpose

Check that the DECREASE STAMPED command can be performed successfully with a two byte value.

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known and larger than "7483";
- A random has been given.

Test

Perform a DECREASE STAMPED command with value "7483" and P1 = "00". Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the DECREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE STAMPED command and the original data in the EF.

CO_DS_VA_03 subclause 9.2.31 c23_31, c23_1, c23_12, c23_24

Purpose

Check that the DECREASE STAMPED command can be performed successfully with a large three byte value.

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known and larger than "E27DA9";
- A random has been given.

Test

Perform a DECREASE STAMPED command with value "E27DA9" and P1 = "00". Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the DECREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE STAMPED command and the original data in the EF.

CO_DS_VA_04 subclause 9.2.31 c23_31, c23_1, c23_12, c23_24

Purpose

Check that the DECREASE STAMPED command can be performed successfully if the value of the L_e field is larger than the maximal response length.

Preconditions

- Writable cyclic EF with 3 byte records exists;
- EF is selected and value of current record is known and larger than "A3AE";
- A random has been given.

Test

Perform a DECREASE STAMPED command with value "A3AE", P1 = "00" and request a 4 byte reponse. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the DECREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE STAMPED command and the original data in the EF.

CO_DS_VA_05 subclause 9.2.31 c23_31, c23_1, c23_12, c23_24

Purpose

Check that the DECREASE STAMPED command can be performed successfully with a cryptogram calculated using the command header of the DECREASE STAMPED command (P1 = "01").

Preconditions

- Writable cyclic EF exists;

- EF is selected and value of current record is known and larger than the value to deduct;
- A random has been given.

Test

Perform a DECREASE STAMPED command with P1 = "01" and an arbitrary value. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the DECREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE STAMPED command and the original data in the EF.

CO_DS_VA_06 subclause 9.2.31 c23_31, c23_1, c23_12, c23_24

Purpose

Check that the DECREASE STAMPED command can be performed successfully with a cryptogram calculated using the command header of the INCREASE STAMPED command (P1 = "02").

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known and larger than the value to deduct;
- A random has been given.

Test

Perform a DECREASE STAMPED command with P1 = "02" and an arbitrary value. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the DECREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE STAMPED command and the original data in the EF.

CO_DS_VA_07 subclause 9.2.31 c23_31, c23_1, c23_12, c23_24

Purpose

Check that the DECREASE STAMPED command can be performed successfully with a cryptogram calculated using the command header of the DECREASE command (P1 = "03").

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known and larger than the value to deduct;
- A random has been given.

Test

Perform a DECREASE STAMPED command with P1 = "03" and an arbitrary value. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the DECREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE STAMPED command and the original data in the EF.

CO_DS_VA_08 subclause 9.2.31 c23_31, c23_1, c23_12, c23_24

Purpose

Check that the DECREASE STAMPED command can be performed successfully with a cryptogram calculated using the command header of the INCREASE command (P1 = "04").

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known and larger than the value to deduct;
- A random has been given.

Test

Perform a DECREASE STAMPED command with P1 = "04" and an arbitrary value. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the DECREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the DECREASE STAMPED command and the original data in the EF.

6.2.3.31.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 64: Return codes for the DECREASE STAMPED command

Return code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 50	- DECREASE STAMPED cannot be performed (Minimum value reached)
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
94 00	- No EF selected as current
94 08	- Current file is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 > "04" or P2 ≠ "00"
67 XX	- $L_c \neq 3$ (+X)
90 00	- Normal ending (ACK) of the command
9F XX	- Length "XX" of the response data

RC_DS_VA_01 subclause 9.4.6 c19_31, c4_9

Purpose
Check that DECREASE STAMPED returns "90 00" if used correctly.

Preconditions
- An EF with cyclic structure is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.
- A random has been given.

Test
Present an DECREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result
The expected status word is "90 00".

RC_DS_VA_02 subclause 9.4.6 c19_31, c4_8

Purpose
Check that DECREASE STAMPED returns "9F XX" if used correctly.

Preconditions
- An EF with cyclic structure is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.
- A random has been given.

Test
Present an DECREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result
The expected status word is "9F XX".

RC_DS_IV_01 subclause 9.4.6 c19_31

Purpose
Check that DECREASE STAMPED returns "98 02" if the key associated with the file does not exist.

Preconditions
- An EF with cyclic structure with a not existing key associated to DECREASE is selected.
- The AC for DECREASE is PRO.
- A random has been asked for.
- A random has been given.

Test

Present an DECREASE STAMPED command with P1 = "00", P2 = "00", L_c = "03" + X and a datafield followed by any cryptogram.

Result

The expected status word is "98 02".

RC_DS_IV_02 subclause 9.4.6 c19_31

Purpose

Check that DECREASE STAMPED returns "98 04" if the selected file has an unfulfilled access condition on DECREASE.

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is not fulfilled, no cryptogram is required.
- A random has been given.

Test

Present an DECREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "98 04".

RC_DS_IV_03 subclause 9.4.6 c19_31

Purpose

Check that DECREASE STAMPED returns "98 10" if the selected file is invalidated.

Preconditions

- An invalidated EF with cyclic is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.
- A random has been given.

Test

Present an DECREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "98 10".

RC_DS_IV_04 subclause 9.4.6 c19_31

Purpose

Check that DECREASE STAMPED returns "98 35" if no random has been asked for.

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is PRO.
- No random has been asked for.
- A random has been given.

Test

Present an DECREASE STAMPED command with P1 = "00", P2 = "00", L_c = "03" + X and a datafield followed by any cryptogram.

Result

The expected status word is "98 35".

RC_DS_IV_05 subclause 9.4.6 c19_31

Purpose

Check that DECREASE STAMPED returns "98 35" if no random has been given.

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is PRO.
- A random has been asked for.
- No random has been given.

Test

Present an DECREASE STAMPED command with P1 = "00", P2 = "00", L_c = "03" + X and a datafield followed by a valid cryptogram.

Result

The expected status word is "98 35".

RC_DS_IV_06 subclause 9.4.6 c19_31

Purpose

Check that DECREASE STAMPED returns "98 50" if the minimum value has been reached.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.
- The minimum value has been reached.
- A random has been given.

Test

Present an DECREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "98 50".

RC_DS_IV_07 subclause 9.4.6 c19_31

Purpose

Check that DECREASE STAMPED returns "92 0X" if the internal retry routine has been used.

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.
- The internal memory can only be written after X retries.
- A random has been given.

Test

Present an DECREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "92 0X".

RC_DS_IV_08 subclause 9.4.6 c19_31

Purpose

Check that DECREASE STAMPED returns "92 40" if the internal memory can not be written.

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.
- The internal memory can not be written.
- A random has been given.

Test

Present an DECREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "92 40".

RC_DS_IV_09 subclause 9.4.6 c19_31

Purpose

Check that DECREASE STAMPED returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.
- A random has been given.

Test

Present an DECREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "94 00".

RC_DS_IV_10 subclause 9.4.6 c19_31

Purpose

Check that DECREASE STAMPED returns "94 08" if a file, not valid for DECREASE is selected.

Preconditions

- EF_{KEY_MAN} is selected.
- A random has been given.

Test

Present an DECREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "94 08".

RC_DS_IV_11 subclause 9.4.6 c19_31

Purpose

Check that DECREASE STAMPED returns "6B XX" if P1 > "04" or P2 ≠ "00".

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.
- A random has been given.

Test

Present an DECREASE STAMPED command with P1 > "04" or P2 ≠ "00" and L_c = "03".

Result

The expected status word is "6B XX".

RC_DS_IV_12 subclause 9.4.6 c19_31

Purpose

Check that UPDATE RECORD returns "67 XX" if L_c ≠ 03 (+X).

Preconditions

- An EF with cyclic structure is selected.
- The AC for DECREASE is fulfilled, no cryptogram is required.
- A random has been given.

Test

Present an DECREASE STAMPED command with P1 = "00", P2 = "00", L_c ≠ "03" with a matching datafield.

Result

The expected status word is "67 XX".

6.2.3.32 INCREASE (INC)

6.2.3.32.1 Function

FU_INC_VA_01 subclause 8.32 c19_32, c23_32, c23_1, c23_12

Purpose

Check that the INCREASE function can be performed successfully on a cyclic file with 3 byte records.

Preconditions

- Writable cyclic EF with 3 byte records exists;
- EF is selected and value of current record is known;

Test

Perform a INCREASE command with an arbitrary value and maximal response length. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data expected to have been written in that EF by the INCREASE command and the original data in the EF.

FU_INC_VA_02 subclause 8.32 c19_32, c23_32, c23_1, c23_12

Purpose

Check that the INCREASE function can be performed successfully on a cyclic file with 5 byte records.

Preconditions

- Writable cyclic EF with 5 byte records exists;
- EF is selected and value of current record is known;

Test

Perform a INCREASE command with an arbitrary value and maximal response length. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE command and the original data in the EF.

6.2.3.32.2 Command

The coding of the INCREASE command is the following:

Table 65: Return codes for the INCREASE command

CLA	Class byte
INS	"32"
P1	"00"
P2	"00"
L_c field	Length of data field
Data field	Value to be added (+cryptogram)
L_e field	Maximum length of data expected in response

CO_INC_VA_01 subclause 9.32 c23_32, c23_1, c23_12

Purpose

Check that the INCREASE command can be performed successfully with a small one byte value.

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known;

Test

Perform a INCREASE command with value "03". Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE command and the original data in the EF.

CO_INC_VA_02 subclause 9.32 c23_32, c23_1, c23_12

Purpose

Check that the INCREASE command can be performed successfully with a two byte value.

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known;

Test

Perform a INCREASE command with value "7483". Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE command and the original data in the EF.

CO_INC_VA_03 subclause 9.32 c23_32, c23_1, c23_12

Purpose

Check that the INCREASE command can be performed successfully with a large three byte value.

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known;

Test

Perform a INCREASE command with value "E27DA9". Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE command and the original data in the EF.

CO_INC_VA_04 subclause 9.32 c23_32, c23_1, c23_12

Purpose

Check that the INCREASE command can be performed successfully when the value of the L_e field is larger then the maximal response length.

Preconditions

- Writable cyclic EF with 3 byte records exists;
- EF is selected and value of current record is known;

Test

Perform a INCREASE command with value "A3AE" and request a 4 byte reponse. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE command and the original data in the EF.

6.2.3.32.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 66: Return codes for the INCREASE command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 50	- INCREASE cannot be performed (Maximum value reached)
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
94 00	- No EF selected as current
94 08	- Current file is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" or P2 ≠ "00"
67 XX	- $L_c \neq 3$ (+ X)
90 00	- Normal ending (ACK) of the command
9F XX	- Length "XX" of the response data

RC_INC_VA_01 subclause 9.4.6 c19_32, c4_9

Purpose

Check that INCREASE returns "90 00" if used correctly.

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.

Test

Present an INCREASE command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "90 00".

RC_INC_VA_02 subclause 9.4.6 c19_32, c4_8

Purpose

Check that INCREASE returns "9F XX" if used correctly.

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.

Test

Present an INCREASE command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "9F XX".

RC_INC_IV_01 subclause 9.4.6 c19_32

Purpose

Check that INCREASE returns "98 02" if the key associated with the file does not exist.

Preconditions

- An EF with cyclic structure with a not existing key associated to INCREASE is selected.
- The AC for INCREASE is PRO.
- A random has been asked for.

Test

Present an INCREASE command with P1 = "00", P2 = "00", L_c = "03" + X and a datafield followed by any cryptogram.

Result

The expected status word is "98 02".

RC_INC_IV_02 subclause 9.4.6 c19_32

Purpose

Check that INCREASE returns "98 04" if the selected file has an unfulfilled access condition on INCREASE.

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is CHV1 and not fulfilled.

Test

Present an INCREASE command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "98 04".

RC_INC_IV_03 subclause 9.4.6 c19_32

Purpose

Check that INCREASE returns "98 04" if wrong cryptogram is presented.

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is PRO

Test

Present an INCREASE command with wrong cryptogram.

Result

The expected status word is "98 04".

RC_INC_IV_04 subclause 9.4.6 c19_32

Purpose

Check that INCREASE returns "98 10" if the selected file is invalidated.

Preconditions

- An invalidated EF with cyclic is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.

Test

Present an INCREASE command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "98 10".

RC_INC_IV_05 subclause 9.4.6 c19_32

Purpose

Check that INCREASE returns "98 35" if no random has been asked for.

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is PRO.
- No random has been asked for.

Test

Present an INCREASE command with P1 = "00", P2 = "00", L_c = "03" + X and a datafield followed by any cryptogram.

Result

The expected status word is "98 35".

RC_INC_IV_06 subclause 9.4.6 c19_32

Purpose

Check that INCREASE returns "98 50" if the maximum value has been reached.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.
- The maximum value has been reached.

Test

Present an INCREASE command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "98 50".

RC_INC_IV_07 subclause 9.4.6 c19_32

Purpose

Check that INCREASE returns "92 0X" if the internal retry routine has been used.

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.
- The internal memory can only be written after X retries.

Test

Present an INCREASE command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "92 0X".

RC_INC_IV_08 subclause 9.4.6 c19_32

Purpose

Check that INCREASE returns "92 40" if the internal memory can not be written.

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.
- The internal memory can not be written.

Test

Present an INCREASE command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "92 40".

RC_INC_IV_09 subclause 9.4.6 c19_32

Purpose

Check that INCREASE returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.

Test

Present an INCREASE command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "94 00".

RC_INC_IV_10 subclause 9.4.6 c19_32

Purpose

Check that INCREASE returns "94 08" if a file, not valid for INCREASE is selected.

Preconditions

- EF_{KEY_MAN} is selected.

Test

Present an INCREASE command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "94 08".

RC_INC_IV_11 subclause 9.4.6 c19_32

Purpose

Check that INCREASE returns "6B XX" if P1 ≠ "00" or P2 ≠ "00".

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.

Test

Present an INCREASE command with P1 ≠ "00" or P2 ≠ "00" and L_c = "03".

Result

The expected status word is "6B XX".

RC_INC_IV_12 subclause 9.4.6 c19_32

Purpose

Check that INCREASE returns "67 XX" if L_c ≠ 03 (+X).

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.

Test

Present an INCREASE command with P1 = "00", P2 = "00", L_c ≠ "03" with a matching datafield.

Result

The expected status word is "67 XX".

6.2.3.33 INCREASE STAMPED (IS)

6.2.3.33.1 Function

FU_IS_VA_01 subclause 8.33 c19_33, c23_33, c23_1, c23_12, c23_24

Purpose

Check that the INCREASE STAMPED function can be performed successfully on a cyclic file with 3 byte records.

Preconditions

- Writable cyclic EF with 3 byte records exists;
- EF is selected and value of current record is known;
- A random has been given.

Test

Perform a INCREASE STAMPED command with an arbitrary value and maximal response length. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the INCREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE STAMPED command and the original data in the EF.

FU_IS_VA_02 subclause 8.33 c19_33, c23_33, c23_1, c23_12, c23_24

Purpose

Check that the INCREASE STAMPED function can be performed successfully on a cyclic file with 5 byte records.

Preconditions

- Writable cyclic EF with 5 byte records exists;
- EF is selected and value of current record is known;
- A random has been given.

Test

Perform a INCREASE STAMPED command with an arbitrary value and maximal response length. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the INCREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE STAMPED command and the original data in the EF.

FU_IS_VA_03 subclause 8.33 c19_33, c23_33, c23_1, c23_12, c23_24, c23_23

Purpose

Check that the INCREASE STAMPED function can be performed successfully on an EF with AC PRO for INCREASE.

Preconditions

- Writable cyclic EF with AC PRO on INCREASE exists;
- EF is selected and value of current record is known;
- A random has been given.
- A random has been asked for.

Test

Perform a INCREASE STAMPED command with a cryptogram created with the random of ASK RANDOM and an arbitrary value. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the INCREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE STAMPED command and the original data in the EF.

6.2.3.33.2 Command

The coding of the INCREASE STAMPED command is the following:

Table 67: Return codes for the INCREASE STAMPED command

CLA	Class byte
INS	"36"
P1	"00" No Command header included in the cryptogram. "01" (CLA, INS, P1, P2) of DECREASE STAMPED is included in the cryptogram. "02" (CLA, INS, P1, P2) of INCREASE STAMPED is included in the cryptogram. "03" (CLA, INS, P1, P2) of the DECREASE command is included in the cryptogram. "04" (CLA, INS, P1, P2) of the INCREASE command is included in the cryptogram.
P2	"00"
L_c field	Length of data field
Data field	Value to be added (+ cryptogram)
L_e field	Maximum length of data expected in response

CO_IS_VA_01 subclause 9.2.33 c23_33, c23_1, c23_12, c23_24

Purpose

Check that the INCREASE STAMPED command can be performed successfully with a small one byte value.

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known;
- A random has been given.

Test

Perform an INCREASE STAMPED command with value "03". Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the INCREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE STAMPED command and the original data in the EF.

CO_IS_VA_02 subclause 9.2.33 c23_33, c23_1, c23_12, c23_24

Purpose

Check that the INCREASE STAMPED command can be performed successfully with a two byte value.

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known;
- A random has been given.

Test

Perform an INCREASE STAMPED command with value "7483". Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the INCREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE STAMPED command and the original data in the EF.

CO_IS_VA_03 subclause 9.2.33 c23_33, c23_1, c23_12, c23_24

Purpose

Check that the INCREASE STAMPED command can be performed successfully with a large three byte value.

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known;
- A random has been given.

Test

Perform an INCREASE STAMPED command with value "E27DA9". Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the INCREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE STAMPED command and the original data in the EF.

CO_IS_VA_04 subclause 9.2.33 c23_33, c23_1, c23_12, c23_24

Purpose

Check that the INCREASE STAMPED command can be performed successfully if the value of the L_e field is larger than the maximal response length.

Preconditions

- Writable cyclic EF with 3 byte records exists;
- EF is selected and value of current record is known;
- A random has been given.

Test

Perform an INCREASE STAMPED command with value "A3AE" and request a 4 byte reponse. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the INCREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE STAMPED command and the original data in the EF.

CO_IS_VA_05 subclause 9.2.33 c23_33, c23_1, c23_12, c23_24

Purpose

Check that the INCREASE STAMPED command can be performed successfully with a cryptogram calculated using the command header of the DECREASE STAMPED command (P1 = "01").

Preconditions

- Writable cyclic EF exists;

- EF is selected and value of current record is known;
- A random has been given.

Test

Perform an INCREASE STAMPED command with P1 = "01" and an arbitrary value. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the INCREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE STAMPED command and the original data in the EF.

CO_IS_VA_06 subclause 9.2.33 c23_33, c23_1, c23_12, c23_24

Purpose

Check that the INCREASE STAMPED command can be performed successfully with a cryptogram calculated using the command header of the INCREASE STAMPED command (P1 = "02").

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known;
- A random has been given.

Test

Perform an INCREASE STAMPED command with P1 = "02" and an arbitrary value. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the INCREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE STAMPED command and the original data in the EF.

CO_IS_VA_07 subclause 9.2.31 c23_33, c23_1, c23_12, c23_24

Purpose

Check that the INCREASE STAMPED command can be performed successfully with a cryptogram calculated using the command header of the DECREASE command (P1 = "03").

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known;
- A random has been given.

Test

Perform an INCREASE STAMPED command with P1 = "03" and an arbitrary value. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the INCREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE STAMPED command and the original data in the EF.

CO_IS_VA_08 subclause 9.2.31 c23_31, c23_1, c23_12, c23_24

Purpose

Check that the INCREASE STAMPED command can be performed successfully with a cryptogram calculated using the command header of the INCREASE command (P1 = "04").

Preconditions

- Writable cyclic EF exists;
- EF is selected and value of current record is known;
- A random has been given.

Test

Perform an INCREASE STAMPED command with P1 = "04" and an arbitrary value. Double check the returned value by means of a READ RECORD command.

Result

Both commands shall have a positive return code and the cryptogram returned by the INCREASE STAMPED command shall be correct. The data returned by the card after the READ RECORD command was performed shall be in accordance with the data written in that EF by the INCREASE STAMPED command and the original data in the EF.

6.2.3.33.3 Return codes

In the following test cases +X refers to the length of the cryptogram, which is algorithm dependent.

Table 68: Return codes for the INCREASE STAMPED command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
98 50	- INCREASE STAMPED cannot be performed (Maximum value reached)
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
94 00	- No EF selected as current
94 08	- Current file is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 > "04" or P2 ≠ "00"
67 XX	- $L_c \neq 3$ (+X)
90 00	- Normal ending (ACK) of the command
9F XX	- Length "XX" of the response data

RC_IS_VA_01 subclause 9.4.6 c19_33, c4_9

Purpose
Check that INCREASE STAMPED returns "90 00" if used correctly.

Preconditions
- An EF with cyclic structure is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.
- A random has been given.

Test
Present an INCREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result
The expected status word is "90 00".

RC_IS_VA_02 subclause 9.4.6 c19_33, c4_8

Purpose
Check that INCREASE STAMPED returns "9F XX" if used correctly.

Preconditions
- An EF with cyclic structure is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.
- A random has been given.

Test
Present an INCREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result
The expected status word is "9F XX".

RC_IS_IV_01 subclause 9.4.6 c19_33

Purpose
Check that INCREASE STAMPED returns "98 02" if the key associated with the file does not exist.

Preconditions
- An EF with cyclic structure with a not existing key associated to INCREASE is selected.
- The AC for INCREASE is PRO.
- A random has been asked for.
- A random has been given.

Test

Present an INCREASE STAMPED command with P1 = "00", P2 = "00", L_c = "03" + X and a datafield followed by any cryptogram.

Result

The expected status word is "98 02".

RC_IS_IV_02 subclause 9.4.6 c19_33

Purpose

Check that INCREASE STAMPED returns "98 04" if the selected file has an unfulfilled access condition on INCREASE.

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is not fulfilled, no cryptogram is required.
- A random has been given.

Test

Present an INCREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "98 04".

RC_IS_IV_03 subclause 9.4.6 c19_33

Purpose

Check that INCREASE STAMPED returns "98 10" if the selected file is invalidated.

Preconditions

- An invalidated EF with cyclic is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.
- A random has been given.

Test

Present an INCREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "98 10".

RC_IS_IV_04 subclause 9.4.6 c19_33

Purpose

Check that INCREASE STAMPED returns "98 35" if no random has been asked for.

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is PRO.
- No random has been asked for.
- A random has been given.

Test

Present an INCREASE STAMPED command with P1 = "00", P2 = "00", L_c = "03" + X and a datafield followed by any cryptogram.

Result

The expected status word is "98 35".

RC_IS_IV_05 subclause 9.4.6 c19_33

Purpose

Check that INCREASE STAMPED returns "98 35" if no random has been given.

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is PRO.
- A random has been asked for.
- No random has been given.

Test

Present an INCREASE STAMPED command with P1 = "00", P2 = "00", L_c = "03" + X and a datafield followed by a valid cryptogram.

Result

The expected status word is "98 35".

RC_IS_IV_06 subclause 9.4.6 c19_33

Purpose

Check that INCREASE STAMPED returns "98 50" if the maximum value has been reached.

Preconditions

- An EF with linear fixed structure is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.
- The maximum value has been reached.

Test

Present an INCREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "98 50".

RC_IS_IV_07 subclause 9.4.6 c19_33

Purpose

Check that INCREASE STAMPED returns "92 0X" if the internal retry routine has been used.

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.
- The internal memory can only be written after X retries.
- A random has been given.

Test

Present an INCREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "92 0X".

RC_IS_IV_08 subclause 9.4.6 c19_33

Purpose

Check that INCREASE STAMPED returns "92 40" if the internal memory can not be written.

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.
- The internal memory can not be written.
- A random has been given.

Test

Present an INCREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "92 40".

RC_IS_IV_09 subclause 9.4.6 c19_33

Purpose

Check that INCREASE STAMPED returns "94 00" if no EF is selected.

Preconditions

- A DF or the MF is selected.
- A random has been given.

Test

Present an INCREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "94 00".

RC_IS_IV_10 subclause 9.4.6 c19_33

Purpose

Check that INCREASE STAMPED returns "94 08" if a file, not valid for INCREASE is selected.

Preconditions

- EF_{KEY_MAN} is selected.
- A random has been given.

Test

Present an INCREASE STAMPED command with P1 = "00", P2 = "00" and L_c = "03".

Result

The expected status word is "94 08".

RC_IS_IV_11 subclause 9.4.6 c19_33

Purpose

Check that INCREASE STAMPED returns "6B XX" if P1 > "04" or P2 ≠ "00".

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.
- A random has been given.

Test

Present an INCREASE STAMPED command with P1 > "04" or P2 ≠ "00" and L_c = "03".

Result

The expected status word is "6B XX".

RC_IS_IV_12 subclause 9.4.6 c19_33

Purpose

Check that INCREASE STAMPED returns "67 XX" if L_c ≠ 03 (+X).

Preconditions

- An EF with cyclic structure is selected.
- The AC for INCREASE is fulfilled, no cryptogram is required.
- A random has been given.

Test

Present an INCREASE STAMPED command with P1 = "00", P2 = "00", L_c ≠ "03" with a matching datafield.

Result

The expected status word is "67 XX".

6.2.3.34 LOAD KEY FILE (LKF)

6.2.3.34.1 Function

FU_LKF_VA_01 subclause 8.34 c19_34, c23_34, c23_1, c23_23, c23_25

Purpose

Check that the LOAD KEYFILE function performs correctly on key 0 from EF_{KEY_OP}.

Preconditions

- A transparent EF with known contents exists.
- AC for READ is AUT
- The key associated to AC READ is key 0.
- A random has been asked for.
- EF_{KEY_OP}

Test

Present a LOAD KEYFILE function.

Present an ASK RANDOM command

Present an EXTERNAL AUTHENTICATION command

Present a READ BINARY function on the transparent file.

Result

The expected status word for both functions is "90 00". The cryptogram has to be valid using the newly downloaded key.

FU_LKF_VA_02 subclause 8.34 c19_34, c23_34, c23_1, c23_23, c23_11

Purpose

Check that the LOAD KEYFILE function performs correctly on key 1 from EF_{KEY_OP}.

Preconditions

- A transparent EF with known contents is selected.
- The key associated to AC READ is key 1.
- A random has been asked for.

Test

Present a LOAD KEYFILE function.

Present a READ BINARY STAMPED function on the transparent file.

Result

The expected status word for both functions is "90 00". The cryptogram has to be valid using the newly downloaded key.

FU_LKF_VA_03 subclause 8.34 c19_34, c23_34, c23_1, c23_23, c23_25, c23_4

Purpose

Check that the LOAD KEYFILE function performs correctly on a key from EF_{KEY_MAN}.

Preconditions

- The AC for DELETE FILE is AUT.
- A file which can be deleted is available.
- A random has been asked for.

Test

Present a LOAD KEYFILE function.

Present an ASK RANDOM function.

Present an EXTERNAL AUTHENTICATION function using the newly downloaded key.

Present a DELETE FILE function.

Result

The expected status word is "90 00" for all functions.

6.2.3.34.2 Command

The coding of the LOAD KEYFILE command is the following:

Table 69: Return codes for the LOAD KEYFILE command

CLA	Class byte
INS	"D8"
P1	"00" Download a key to EF_{KEY_MAN} "01" Download a key to EF_{KEY_OP}
P2	Key Number "00" - "0F"
L_c field	Length of the data
Data field	Data to be sent to the card
L_e field	Empty

No tests are foreseen to test the LOAD KEYFILE command other than those defined in the functions subclause.

6.2.3.34.3 Return codes

Table 70: Return codes for the LOAD KEYFILE command

Return Code	Error description
98 02	- No key defined
98 04	- AC not fulfilled
98 10	- In contradiction with the invalidation status
98 35	- No ASK RANDOM / GIVE RANDOM before
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
94 00	- No EF selected as current
94 08	- Current file type is inconsistent with the command
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 > "01"
67 XX	- $L_c \neq$ "1A" for P2 = "01" .. "0F" - $L_c \neq$ "1B" for P2 = "00"
90 00	- Normal ending (ACK) of the command

RC_LKF_VA_01 subclause 9.4.6 c19_34

Purpose

Check that LOAD KEYFILE returns "90 00" if used correctly.

Preconditions

- EF_{KEY_OP} is selected.
- A random has been asked for.

Test

Present a LOAD KEYFILE command with P1 = "01".

Result

The expected status word is "90 00".

RC_LKF_IV_01 subclause 9.4.6 c19_34

Purpose

Check that LOAD KEYFILE returns "98 02" if the key associated with the AC LOAD KEYFILE does not exist.

Preconditions

- EF_{KEY_OP} is selected.
- A random has been asked for.
- The key for LOAD KEYFILE does not exist.

Test

Present a LOAD KEYFILE command with P1 = "01".

Result

The expected status word is "98 02".

RC_LKF_IV_02 subclause 9.4.6 c19_34

Purpose

Check that LOAD KEYFILE returns "98 04" if the AC for LOAD KEYFILE is not fulfilled.

Preconditions

- EF_{KEY_OP} is selected.
- A random has been asked for.

Test

Present a LOAD KEYFILE command with P1 = "01" and a wrong cryptogram.

Result

The expected status word is "98 04".

RC_LKF_IV_03 subclause 9.4.6 c19_34

Purpose

Check that LOAD KEYFILE returns "98 10" if EF_{KEY_OP} is invalidated.

Preconditions

- EF_{KEY_OP} is selected.
- A random has been asked for.
- EF_{KEY_OP} is invalidated.

Test

Present a LOAD KEYFILE command with P1 = "01".

Result

The expected status word is "98 10".

RC_LKF_IV_04 subclause 9.4.6 c19_34

Purpose

Check that LOAD KEYFILE returns "98 35" if no random has been asked for.

Preconditions

- EF_{KEY_OP} is selected.
- No random has been asked for.

Test

Present a LOAD KEYFILE command with P1 = "01" and any cryptogram.

Result

The expected status word is "98 35".

RC_LKF_IV_05 subclause 9.4.6 c19_34

Purpose

Check that LOAD KEYFILE returns "92 0X" if the internal retry routine has been used.

Preconditions

- EF_{KEY_OP} is selected.
- A random has been asked for.
- The internal memory can only be written after X retries.

Test

Present a LOAD KEYFILE command with P1 = "01".

Result

The expected status word is "92 0X".

RC_LKF_IV_06 subclause 9.4.6 c19_34

Purpose

Check that LOAD KEYFILE returns "92 40" if the internal memory can not be written.

Preconditions

- EF_{KEY_OP} is selected.
- A random has been asked for.
- The internal memory can not be written.

Test
Present a LOAD KEYFILE command with P1 = "01".

Result
The expected status word is "92 40".

RC_LKF_IV_07 subclause 9.4.6 c19_34

Purpose
Check that LOAD KEYFILE returns "94 00" if no EF is selected.

Preconditions
- A DF or the MF is selected.
- A random has been asked for.

Test
Present a LOAD KEYFILE command with P1 = "01".

Result
The expected status word is "94 00".

RC_LKF_IV_08 subclause 9.4.6 c19_34

Purpose
Check that LOAD KEYFILE returns "94 08" if a file with the wrong file type is selected.

Preconditions
- EF_{KEY_OP} is selected.
- A random has been asked for.

Test
Present a LOAD KEYFILE command with P1 = "00".

Result
The expected status word is "94 08".

RC_LKF_IV_09 subclause 9.4.6 c19_34

Purpose
Check that LOAD KEYFILE returns "94 08" if a file with the wrong file type is selected.

Preconditions
- EF_{ICC} is selected.
- A random has been asked for.

Test
Present a LOAD KEYFILE command with P1 = "00".

Result
The expected status word is "94 08".

RC_LKF_IV_10 subclause 9.4.6 c19_34

Purpose
Check that LOAD KEYFILE returns "6B XX" if P1 > "01".

Preconditions
- EF_{KEY_OP} is selected.
- A random has been asked for.

Test

Present a LOAD KEYFILE command with P1 > "01".

Result

The expected status word is "6B XX".

RC_LKF_IV_11 subclause 9.4.6 c19_34

Purpose

Check that LOAD KEYFILE returns "67 XX" if $L_c \neq$ "1B" for P2 = 0 or $L_c \neq$ "1A" for P2 = "01" .. "0F".

Preconditions

- EF_{KEY_OP} is selected.
- A random has been asked for.

Test

Present a LOAD KEYFILE command with P2 = "00", $L_c \neq$ "1B" and a matching datafield.

Result

The expected status word is "67 XX".

6.2.3.35 GET RESPONSE (GR)

6.2.3.35.1 Function

As there is no function GET RESPONSE specified in the base standard, there are no tests foreseen for that.

6.2.3.35.2 Command

The coding of the GET RESPONSE command is the following:

Table 71: Return codes for the GET RESPONSE command

CLA	Class byte
INS	"C0"
P1	"00" (other values are RFU)
P2	"00" (other values are RFU)
L_c field	Empty
Data field	Empty
L_e field	Maximum length of data expected in the response

CO_GET_VA_01 subclause 9.2.35 c23_35, c4_8

Purpose

Check that GET RESPONSE is able to return response data.

Preconditions

- A SELECT has been performed on EF_{ICC}.

Test

Perform a GET RESPONSE command with L_e = SW2 of previous status word.

Result

The returned data has to be that of the previous SELECT command.

6.2.3.35.3 Return codes

Table 72: Return codes for the GET RESPONSE command

Return Code	Error description
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" or P2 ≠ "00"
67 XX	- no test is foreseen for this status word
92 40	- no test is foreseen for this status word
90 00	- Normal ending (ACK) of the command
9F XX	- Length "XX" of the response data

RC_GET_VA_01 subclause 9.4.6 c23_35, c4_8

Purpose

Check that GET RESPONSE returns "90 00", if used correctly.

Preconditions

- A SELECT has been performed before on EF_{ICC}.

Test

Perform a GET RESPONSE command with L_e = SW2 of previous command.

Result

The expected status word is "90 00".

RC_GET_VA_02 subclause 9.4.6 c23_35, c4_8

Purpose

Check that GET RESPONSE returns "9F XX", if not all data are read.

Preconditions

- A SELECT has been performed before on EF_{ICC}.

Test

Perform a GET RESPONSE command with L_e = (SW2 - 1), with SW2 of previous command.

Result

The expected status word is "9F 01".

RC_GET_IV_01 subclause 9.4.6 c23_35, c4_8

Purpose

Check that GET RESPONSE returns "6B XX" if P1 ≠ "00" or P2 ≠ "00".

Preconditions

- A SELECT has been performed before on EF_{ICC}.

Test

Perform a GET RESPONSE command with L_e = SW2 of previous command.

Result

The expected status word is "6B XX".

6.2.3.36 ENVELOPE PUT (EP)

6.2.3.36.1 Function

As there is no function ENVELOPE PUT specified in the base standard, there are no tests foreseen for that.

6.2.3.36.2 Command

The coding of the ENVELOPE PUT command is the following:

Table 73: Return codes for the ENVELOPE PUT command

CLA	Class byte
INS	"C2"
P1	"00" (other values are RFU)
P2	"00" (other values are RFU)
L_c field	Number of data bytes
Data field	Data sent to the card
L_e field	Empty

CO_EP_VA_01 subclause 9.2.36 c23_36, c4_8

Purpose

Check that it is possible to send data with ENVELOPE PUT to the chip card.

Preconditions

- None.

Test

Send data with ENVELOPE PUT.

Result

The expected status word is "9F XX".

NOTE: It might be necessary to perform additional implementation specific tests

Specification for this is under responsibility of the development team.

6.2.3.36.3 Return codes

Table 74: Return codes for the ENVELOPE PUT command

Return Code	Error description
6E XX	- Wrong instruction class given in the command
6D XX	- Unknown instruction code given in the command
6F XX	- Technical problem with no diagnostic given (command aborted)
6B XX	- P1 ≠ "00" or P2 ≠ "00"
67 XX	- no test is foreseen for this status word
92 40	- no test is foreseen for this status word
90 00	- Normal ending (ACK) of the command

RC_EP_VA_01 subclause 9.4.6 c23_36, c4_8

Purpose
Check that ENVELOPE PUT returns "90 00", if used correctly.

Preconditions
- None.

Test
Send data with ENVELOPE PUT.

Result
The expected status word is "90 00".

RC_EP_IV_01 subclause 9.4.6 c23_36, c4_8

Purpose
Check that ENVELOPE PUT returns "6B XX" if P1 ≠ "00" or P2 ≠ "00".

Preconditions
- None.

Test
Send data with ENVELOPE PUT.

Result
The expected status word is "6B XX".

6.2.3.37 General tests on return codes

RC_XX_IV_01 subclause 9.4.4

Purpose
Check that the UC returns "6E XX" if an unknown class is used.

Preconditions
- None.

Test
Reset the UC and present any command with a not supported CLA byte.

Result
The expected status word is "6E XX".

RC_XX_IV_02 subclause 9.4.4

Purpose
Check that the UC returns "6D XX" if an instruction is used, which is unsupported within that context.

Preconditions
- None.

Test
Reset the UC and present a command with at least 4 bytes and unsupported INS byte.

Result
The expected status word is "6D XX".

RC_XX_IV_03 subclause 9.4.4

Purpose
Check that the UC returns "6F XX" if technical problem occurs.

Preconditions
- None.

Test
Unknown.

Result
The expected status word is "6F XX".

NOTE: Actual tests for this condition are implementation dependent.

6.2.4 Data structure and pointers

This subclause focuses on the consistency of the file and record pointers.

IC cards contain a data structure to organize the files (EFs, MF and DFs). Furthermore a number of pointers are maintained to keep the state of records within linear fixed or cyclic files.

DISCLAIMER:

The management processes for allocating and free-ing memory space for created and deleted files are not tested within this subclause as they are not part of the base standard.

The following pointers are considered in this subclause:

Context = Session	Context = EF
Current File (last selected DF or EF)	Current record (for linear and cyclic EFs only)
Current DF	Oldest record (for cyclic EFs only)
Current EF	

Both file and record pointers are tested by the exchange of commands to:

1. Try to change data structure or pointers in a correct or incorrect way.
2. Verify of the successful or unsuccessful changes.

6.2.4.1 File pointers

6.2.4.1.1 Current File (CF)

DP_CF_VA_01 subclause 8.1c23_10
Purpose
Check that the EF pointer is undefined after reset.

Preconditions
- At least one EF with known file id within the MF exists

Test

Reset the card

Present an READ BINARY command on a EF within the MF.

Result

Status word "94 00" and no response data shall be returned.

DP_CF_VA_01 subclause 8.1c23_1, c23_4, c23_10

Purpose

Check that the EF pointer is undefined after deletion of an EF.

Preconditions

- At least one EF with known file id within the MF exists

Test

Present a SELECT FILE on the known EF.

Present a DELETE FILE with this file id

Present a READ command.

Result

SELECT and DELETE FILE command shall return status work "90 00".

Status word "94 00" and no response data shall be returned by READ command.

6.2.4.1.2 Current DF (CD)

The following tests verify the correct changing of the DF pointer. For this purpose the STATUS command is used. If this command is not supported the tests could alternatively be made by exclusive use of the select command as well.

DP_CD_VA_01 subclause 8.1c23_1, c23_2

Purpose

Check that the DF pointer is correctly changed when an EF is selected in another DF by means of a select-by-path.

Preconditions

- EF exists in DF other than MF;
- DF pointer on DF other than DF above EF to select;

Test

Select the EF and then perform the STATUS command.

Result

The response to the STATUS command shall reflect the characteristics of the DF above the EF.

DP_CD_VA_02 subclause 8.1c23_1, c23_2

Purpose

Check that the DF pointer remains unchanged when an EF is selected in the same DF.

Preconditions

- DF pointer on DF other than MF;
- EF exists in current DF;

Test

Select the EF and then perform the STATUS command.

Result

The response to the STATUS command shall reflect the characteristics of the DF above the EF.

DP_CD_VA_03 subclause 8.1c23_1, c23_2, c23_4

Purpose

Check that the DF pointer is set to the MF after reset.

Preconditions

- At least one EF with known file id within the MF exists

Test

Reset the card

Present a SELECT FILE command on a EF within the MF.

Result

Response Data shall be as expected and status word is "90 00".

DP_CD_VA_04 subclause 8.1c23_7, c23_8

Purpose

Check that the deletion of a DF does not have any effect on the DF pointer.

Preconditions

- At least one DF with known file id within the MF exists.
- MF is selected.

Test

Present a DELETE FILE on the known DF.

Present a STATUS command.

Result

DELETE FILE command shall return status word "90 00".

STATUS command shall return information about MF.

DP_CD_IV_01 subclause 8.1c23_1, c23_2

Purpose

Check that the DF pointer is not changed when an non existing EF is selected in another DF by means of a select-by-path.

Preconditions

- EF does not exist in DF other than MF;
- DF pointer on DF other than DF above EF to select;

Test
Select the EF and then perform the STATUS command.

Result
The response to the STATUS command shall reflect the characteristics of the original DF.

DP_CD_IV_02 subclause 8.1c23_1, c23_2

Purpose
Check that the DF pointer is not changed when a non existing DF is selected under the current DF.

Preconditions
- DF pointer on arbitrary DF;
- DF to be selected does not exist;

Test
Try to select the DF and then perform the STATUS command.

Result
The response to the STATUS command shall reflect the characteristics of the original DF.

6.2.4.1.3 Current EF (CE)

DP_CE_VA_01 subclause 8.1c23_1, c23_10

Purpose
Check that the EF pointer is correctly changed when an EF is selected.

Preconditions
- Transparent readable EF with known contents exists;

Test
Select the EF and then try to read a few bytes.

Result
Both commands shall have a positive return code.

DP_CE_IV_01 subclause 8.1c23_1, c23_10

Purpose
Check that the EF pointer is not assigned just after a reset.

Preconditions
- Transparent readable EF with known contents exists;
- No select command has been performed after reset yet;

Test
Try to read a few bytes from the current EF.

Result
The response to the READ command shall indicate that no EF was selected (code "94 00").

DP_CE_IV_02 subclause 8.1c23_1, c23_10

Purpose
Check that the EF pointer is not changed when a non existing EF is selected.

Preconditions
- EF pointer on transparent readable EF with known contents;
- EF to be selected does not exist;

Test

Try to select the non existing EF and then try to read a few bytes from the current EF.

Result

The response to the READ command shall be successful.

DP_CE_IV_03 subclause 8.1c23_1, c23_10

Purpose

Check that the EF pointer becomes unassigned when a DF is selected.

Preconditions

- EF pointer on transparent readable EF;
- DF exists;

Test

Select the DF and then try to read a few bytes from the current EF.

Result

The response to the READ command shall indicate that no EF was selected (code "94 00").

6.2.4.2 Record pointers

6.2.4.2.1 Current Record Pointer (CRP)

DP_CRP_VA_01 subclause 8.12 c23_1, c23_12

Purpose

Check that the Current Record Pointer is unchanged when a READ RECORD in ABSOLUTE mode is performed.

Preconditions

- Linear readable EF with known contents selected;
- Current record assigned at an arbitrary record ;

Test

Perform a READ RECORD in ABSOLUTE mode and then a READ RECORD in NEXT mode.

Result

Both commands shall have a **positive return code**. The response data for the last command shall be in accordance with the next record of the originally selected record.

DP_CRP_VA_02 subclause 8.14 c23_1, c23_12, c23_14

Purpose

Check that the Current Record pointer is changed when a successful SEEK command is performed.

Preconditions

- Linear readable EF with known contents selected;
- Current record assigned at an arbitrary record ;

Test

Perform a SEEK for a matching pattern command and then a READ RECORD in CURRENT mode.

Result

Both commands shall have a **positive return code**. The response data for the READ RECORD command shall be in accordance with the originally selected record.

DP_CRP_VA_03 subclause 8.14 c23_1, c23_12, c23_9

Purpose

Check that the Current Record pointer is changed when a successful CREATE RECORD command is performed.

Preconditions

- Linear readable incomplete EF with known contents selected;
- Current record assigned at an arbitrary record not at the end of the file;

Test

Perform a CREATE RECORD command and then a READ RECORD in CURRENT mode.

Result

Both commands shall have a **positive return code**. The response data for the READ RECORD command shall be in accordance with the just created record.

DP_CRP_VA_04 subclause 8.14 c23_1, c23_12

Purpose

Check that the Current Record pointer is set to the last written record when a cyclic EF is selected.

Preconditions

- Cyclic readable EF incomplete with known contents exists;

Test

Select the EF and then a perform a READ RECORD in CURRENT mode.

Result

Both commands shall have a **positive return code**. The response data for the READ RECORD command shall be in accordance with the last written record.

DP_CRP_VA_05 subclause 8.14 c23_1, c23_12, c8_1

Purpose

Check that the Current EF and Current Record Pointer are not changed when another linear file is read via another channel.

Preconditions

- Linear readable EFs with known contents selected;
- Another linear readable EF exists.
- Current record assigned at an arbitrary record not at the beginning of the file;

Test

Perform in another channel a SELECT command and then a READ RECORD in CURRENT mode. Then perform in the original channel a READ RECORD command in CURRENT mode.

Result

All commands shall have a **positive return code**. The response data for the first READ RECORD command shall reflect the first record of that EF, while the last READ RECORD command shall be in accordance with previously selected record of the original EF.

DP_CRP_IV_01 subclause 8.12 c23_1, c23_12, c23_14

Purpose

Check that the Current Record pointer is unchanged when an unsuccessful SEEK command is performed.

Preconditions

- Linear readable EF with known contents selected;
- Current record assigned at an arbitrary record ;

Test

Perform a SEEK command for a non-matching pattern and then a READ RECORD in CURRENT mode.

Result

Only the READ RECORD command shall have a **positive return code**. The response data for that command shall be in accordance with the originally selected record.

DP_CRP_IV_02 subclause 8.12 c23_1, c23_12

Purpose

Check that the Current Record pointer is unchanged when an unsuccessful SELECT command is performed.

Preconditions

- Linear readable EF with known contents selected;
- Current record assigned at an arbitrary record ;

Test

Perform a SELECT command for a non-existing EF and then a READ RECORD in CURRENT mode.

Result

Only the READ RECORD command shall have a **positive return code**. The response data for that command shall be in accordance with the originally selected record.

6.2.4.2.2 Oldest Record (OR)

DP_ORP_VA_01 subclause 8.12 c23_1, c23_12, c23_30

Purpose

Check that the Oldest Record pointer is changed when a DECREASE command is performed.

Preconditions

- Cyclic EF with known contents selected;

Test

Perform a DECREASE command and then a READ RECORD in ABSOLUTE mode for records no. 2.

Result

Both commands shall have a **positive return code**. The response data for the last command shall be in accordance with the contents of the last written record before.

6.2.5 Access Conditions (AC)

This subclause is dedicated to test the functionality of setting access conditions to group of functions on individual EFs or DFs. In order to test a wide variety of combinations, but not to test all valid combinations, the following selection has been chosen:

Transparent EF:

AC	FUNCTION
ALW	READ
CHV1	READ
CHV2	READ
PRO	UPDATE
AUT	READ
CHV1 / PRO	UPDATE
CHV2 / PRO	UPDATE
CHV1 / AUT	READ
CHV2 / AUT	READ
NEV	READ

Linear fix structured EF:

FUNCTION	AC
READ	CHV1
UPDATE	PRO
WRITE	PRO
INCREASE	AUT
DECREASE	AUT
CREATE RECORD	CHV1
REHABILITATE	PRO
INVALIDATE	PRO

DF:

FUNCTION	AC
DELETE FILE	PRO
CREATE FILE	PRO
REHABILITATE	CHV1
INVALIDATE	CHV1

EF_{KEY_OP}:

FUNCTION	AC
LOAD KEYFILE	CHV1 / PRO
UPDATE	CHV1 / PRO
REHABILITATE	CHV1
INVALIDATE	CHV1

The tests always start after a reset, with no access condition fulfilled. The function to be tested is then applied, the expected result normally will be Access Condition (AC) not fulfilled. Then the AC will be fulfilled and the command will be applied again, but this time the command shall succeed.

AC_XX_VA_01 subclause 7 c23_10, c23_1

Purpose
Check that the Access Condition ALW works properly.

Preconditions
- A transparent file with AC ALW on READ is selected.
- No AC is fulfilled.

Test
Perform a READ BINARY on that file.

Result
The expected status word is "90 00", the file contents is read successfully.

AC_XX_VA_02 subclause 7 c23_10, c23_1, c23_15

Purpose
Check that the Access Condition CHV1 works properly.

Preconditions
- A transparent file with AC CHV1 on READ is selected.
- No AC is fulfilled.

Test
Perform a READ BINARY on that file.

Perform a VERIFY CHV for CHV1.

Perform a READ BINARY on that file.

Result
The expected status word is "98 04" for the first command and "90 00" for the other 2. The file contents is read successfully.

AC_XX_VA_03 subclause 7 c23_10, c23_1, c23_15

Purpose
Check that the Access Condition CHV2 works properly.

Preconditions
- A transparent file with AC CHV2 on READ is selected.
- No AC is fulfilled.

Test
Perform a READ BINARY on that file.

Perform a VERIFY CHV for CHV2.

Perform a READ BINARY on that file.

Result
The expected status word is "98 04" for the first command and "90 00" for the other 2. The file contents is read successfully.

AC_XX_VA_04 subclause 7 c23_7, c23_1, c23_23

Purpose
Check that the Access Condition PRO works properly.

Preconditions
- A transparent file with AC PRO on UPDATE is selected.

- No AC is fulfilled.
- A random has been asked for.

Test

Perform an UPDATE BINARY with wrong cryptogram on that file.

Perform an ASK RANDOM.

Perform an UPDATE BINARY with a valid cryptogram on that file.

Result

The expected status word is "98 04" for the first command and "90 00" for the other.

AC_XX_VA_05 subclause 7 c23_10, c23_1, c23_25, c23_23

Purpose

Check that the Access Condition AUT works properly.

Preconditions

- A transparent file with AC AUT on READ is selected.
- No AC is fulfilled.

Test

Perform a READ BINARY on that file.

Perform an ASK RANDOM.

Perform an EXTERNAL AUTHENTICATION with the relevant key.

Perform a READ BINARY on that file.

Result

The expected status word is "98 04" for the first command and "90 00" for the other 3. The file contents is read successfully.

AC_XX_VA_06 subclause 7 c23_7, c23_1, c23_23, c23_15

Purpose

Check that the Access Condition CHV1/PRO works properly.

Preconditions

- A transparent file with AC CHV1/PRO on UPDATE is selected.
- No AC is fulfilled.

Test

Perform an UPDATE BINARY without cryptogram on that file.

Perform a VERIFY CHV for CHV1.

Perform an UPDATE BINARY without cryptogram on that file.

Perform an ASK RANDOM.

Perform an UPDATE BINARY with a valid cryptogram on that file.

Result

The expected status word is "98 04" for the first two UPDATE BINARY commands and "90 00" for all other commands.

AC_XX_VA_07 subclause 7 c23_7, c23_1, c23_23, c23_15

Purpose

Check that the Access Condition CHV2/PRO works properly.

Preconditions

- A transparent file with AC CHV2/PRO on UPDATE is selected.
- No AC is fulfilled.
- A random has been asked for.

Test

Perform an UPDATE BINARY with a wrong cryptogram on that file.

Perform a VERIFY CHV for CHV2.

Perform an UPDATE BINARY without cryptogram on that file.

Perform an ASK RANDOM.

Perform an UPDATE BINARY with a valid cryptogram on that file.

Result

The expected status word is "98 04" for the first two UPDATE BINARY commands and "90 00" for all other commands.

AC_XX_VA_08 subclause 7 c23_10, c23_1, c23_25, c23_23, c23_15

Purpose

Check that the Access Condition CHV1/AUT works properly.

Preconditions

- A transparent file with AC CHV1/AUT on READ is selected.
- No AC is fulfilled.

Test

Perform a READ BINARY on that file.

Perform an ASK RANDOM.

Perform an EXTERNAL AUTHENTICATION with the relevant key.

Perform a READ BINARY on that file.

Perform a VERIFY CHV for CHV1.

Perform a READ BINARY on that file.

Result

The expected status word is "98 04" for the first two READ BINARY commands and "90 00" for all other commands. The file contents is read successfully.

AC_XX_VA_09 subclause 7 c23_10, c23_1, c23_25, c23_23, c23_15

Purpose

Check that the Access Condition CHV2/AUT works properly.

Preconditions

- A transparent file with AC CHV2/AUT on READ is selected.
- No AC is fulfilled.

Test

Perform a READ BINARY on that file.

Perform an ASK RANDOM.

Perform an EXTERNAL AUTHENTICATION with the relevant key.

Perform a READ BINARY on that file.

Perform a VERIFY CHV for CHV2.

Perform a READ BINARY on that file.

Result

The expected status word is "98 04" for the first two READ BINARY commands and "90 00" for all other commands. The file contents is read successfully.

AC_XX_VA_10 subclause 7 c23_10, c23_1, c23_25, c23_23, c23_15

Purpose

Check that the Access Condition NEV works properly.

Preconditions

- A transparent file with AC NEV on READ is selected.
- No AC is fulfilled.

Test

Perform a READ BINARY on that file.

Perform an ASK RANDOM.

Perform an EXTERNAL AUTHENTICATION with the relevant key.

Perform a READ BINARY on that file.

Perform a VERIFY CHV for CHV1.

Perform a READ BINARY on that file.

Perform a VERIFY CHV for CHV2.

Perform a READ BINARY on that file.

Result

The expected status word is "98 04" for all READ BINARY commands and "90 00" for all other commands.

AC_XX_VA_11 subclause 7 c23_12, c23_1, c23_15

Purpose

Check that an Access Condition on READ/SEEK works properly.

Preconditions

- A linear fix structured file with AC CHV1 on READ is selected.
- No AC is fulfilled.

Test

Perform a READ RECORD on that file.

Perform a VERIFY CHV for CHV1.

Perform a READ RECORD on that file.

Result

The expected status word is "98 04" for the first command and "90 00" for the other 2. The file contents is read successfully.

AC_XX_VA_12 subclause 7 c23_8, c23_1, c23_23

Purpose

Check that an Access Condition on UPDATE works properly.

Preconditions

- A linear fix structured file with AC PRO on UPDATE is selected.
- No AC is fulfilled.
- A random has been asked for.

Test

Perform an UPDATE RECORD with a wrong cryptogram on that file.

Perform an ASK RANDOM.

Perform an UPDATE RECORD with a valid cryptogram on that file.

Result

The expected status word is "98 04" for the first command and "90 00" for the other.

AC_XX_VA_13 subclause 7 c23_30, c23_1, c23_23

Purpose

Check that a DECREASE command is not possible if UPDATE is selected.

Preconditions

- A linear fix structured file with AC PRO on UPDATE (DECREASE) is selected.
- No AC is fulfilled.

Test

Perform an ASK RANDOM.

Perform a DECREASE function with a valid cryptogram on that file.

Result

The expected status word is "90 00" for the first command and "94 08" for the second command.

AC_XX_VA_14 subclause 7 c23_28, c23_1, c23_23

Purpose

Check that an Access Condition on WRITE works properly.

Preconditions

- A linear fix structured file with AC PRO on WRITE is selected.
- No AC is fulfilled.
- A random has been asked for.

Test

Perform an WRITE RECORD with a wrong cryptogram on that file.

Perform an ASK RANDOM.

Perform an WRITE RECORD with a valid cryptogram on that file.

Result

The expected status word is "98 04" for the first command and "90 00" for the other.

AC_XX_VA_15 subclause 7 c23_32, c23_1, c23_23

Purpose

Check that an INCREASE command is not possible if WRITE is selected.

Preconditions

- A linear fix structured file with AC PRO on WRITE (INCREASE) is selected.
- No AC is fulfilled.

Test

Perform an ASK RANDOM.

Perform an INCREASE function with a valid cryptogram on that file.

Result

The expected status word is "90 00" for the first command and "94 08" for the second command.

AC_XX_VA_16 subclause 7 c23_32, c23_1, c23_25, c23_23

Purpose

Check that an Access Condition on INCREASE works properly.

Preconditions

- A linear fix structured file with AC AUT on INCREASE is selected.
- No AC is fulfilled.

Test

Perform an INCREASE on that file.

Perform an ASK RANDOM.

Perform an EXTERNAL AUTHENTICATION with the relevant key.

Perform an INCREASE on that file.

Result

The expected status word is "98 04" for the first command and "90 00" for the other 3.

AC_XX_VA_17 subclause 7 c23_28, c23_1, c23_23, c23_25

Purpose

Check that a WRITE command is not possible if INCREASE is selected.

Preconditions

- A linear fix structured file with AC PRO on INCREASE(WRITE) is selected.
- No AC is fulfilled.

Test

Perform an ASK RANDOM.

Perform an EXTERNAL AUTHENTICATION with the relevant key.

Perform a WRITE function on that file.

Result

The expected status word is "90 00" for the first two commands and "94 08" for the third command.

AC_XX_VA_18 subclause 7 c23_30, c23_1, c23_25, c23_23

Purpose

Check that an Access Condition on DECREASE works properly.

Preconditions

- A linear fix structured file with AC AUT on DECREASE is selected.
- No AC is fulfilled.

Test

Perform a DECREASE on that file.

Perform an ASK RANDOM.

Perform an EXTERNAL AUTHENTICATION with the relevant key.

Perform a DECREASE on that file.

Result

The expected status word is "98 04" for the first command and "90 00" for the other 3.

AC_XX_VA_19 subclause 7 c23_28, c23_1, c23_23, c23_25

Purpose

Check that an UPDATE command is not possible if DECREASE is selected.

Preconditions

- A linear fix structured file with AC AUT on DECREASE(UPDATE) is selected.
- No AC is fulfilled.

Test

Perform an ASK RANDOM.

Perform an EXTERNAL AUTHENTICATION with the relevant key.

Perform an UPDATE function on that file.

Result

The expected status word is "90 00" for the first two commands and "94 08" for the third command.

AC_XX_VA_20 subclause 7 c23_9, c23_1, c23_15, c23_12

Purpose

Check that an Access Condition on CREATE RECORD works properly.

Preconditions

- A linear fix structured file with AC CHV1 on CREATE RECORD is selected.
- The number of records in that file is known.
- No AC is fulfilled.

Test

Perform a CREATE RECORD on that file.

Perform a VERIFY CHV for CHV1.

Perform a CREATE RECORD on that file.

Perform a READ RECORD on the newly created record.

Result

The expected status word is "98 04" for the first command and "90 00" for the other 3. The new record shall be read correctly.

AC_XX_VA_21 subclause 7 c23_21, c23_1, c23_23

Purpose

Check that an Access Condition on REHABILITATE works properly.

Preconditions

- A linear fix structured file with AC PRO on REHABILITATE is selected.

- That file is invalidated.
- No AC is fulfilled.
- A random has been asked for.

Test

Perform a REHABILTATE with a wrong cryptogram on that file.

Perform an ASK RANDOM.

Perform a REHABILTATE with a correct cryptogram on that file.

Result

The expected status word is "98 04" for the first command and "90 00" for the other 2.

AC_XX_VA_22 subclause 7 c23_20, c23_1, c23_23

Purpose

Check that an Access Condition on INVALIDATE works properly.

Preconditions

- A linear fix structured file with AC PRO on INVALIDATE is selected.
- That file is not invalidated.
- No AC is fulfilled.
- A random has been asked for.

Test

Perform a INVALIDATE with a wrong cryptogram on that file.

Perform an ASK RANDOM.

Perform a INVALIDATE with a correct cryptogram on that file.

Result

The expected status word is "98 04" for the first command and "90 00" for the other 2.

AC_XX_VA_23 subclause 7 c23_4, c23_1, c23_23

Purpose

Check that an Access Condition on DELETE FILE works properly.

Preconditions

- A DF with AC PRO on DELETE FILE is selected.
- No AC is fulfilled.
- An EF which can be deleted exists.
- A random has been asked for.

Test

Perform a DELETE FILE command with a wrong cryptogram on that EF.

Perform an ASK RANDOM.

Perform a DELETE FILE command with a valid cryptogram on that EF.

Result

The expected status word is "98 04" for the first command and "90 00" for the other.

AC_XX_VA_24 subclause 7 c23_3, c23_1, c23_23

Purpose

Check that an Access Condition on CREATE FILE works properly.

Preconditions

- A DF with AC PRO on CREATE FILE is selected.
- No AC is fulfilled.
- Enough room to create a file is available.
- A random has been asked for.

Test

Perform a CREATE FILE command with a wrong cryptogram.

Perform an ASK RANDOM.

Perform a CREATE FILE command with a valid cryptogram.

Result

The expected status word is "98 04" for the first command and "90 00" for the other.

AC_XX_VA_25 subclause 7 c23_21, c23_1, c23_15

Purpose

Check that an Access Condition on REHABILITATE works properly.

Preconditions

- A DF with AC CHV1 on REHABILITATE is selected.
- No AC is fulfilled.
- The DF is invalidated.

Test

Perform a REHABILITATE on that file.

Perform a VERIFY CHV for CHV1.

Perform a REHABILITATE on that file.

Result

The expected status word is "98 04" for the first command and "90 00" for the other 2.

AC_XX_VA_26 subclause 7 c23_20, c23_1, c23_15

Purpose

Check that an Access Condition on INVALIDATE works properly.

Preconditions

- A DF with AC CHV1 on INVALIDATE is selected.
- No AC is fulfilled.

- The DF is not invalidated.

Test

Perform a INVALIDATE on that file.

Perform a VERIFY CHV for CHV1.

Perform a INVALIDATE on that file.

Result

The expected status word is "98 04" for the first command and "90 00" for the other 2.

AC_XX_VA_27 subclause 7 c23_34, c23_1, c23_15, c23_23

Purpose

Check that an Access Condition on LOAD KEYFILE works properly.

Preconditions

- EF_{KEY_OP} with AC CHV1/PRO on LOAD KEYFILE is selected.
- No AC is fulfilled.
- A random has been asked for.

Test

Perform a LOAD KEYFILE command with a wrong cryptogram.

Perform a VERIFY CHV for CHV1.

Perform a LOAD KEYFILE command without cryptogram.

Perform an ASK RANDOM command.

Perform a LOAD KEYFILE command with a valid cryptogram.

Result

The expected status word is "98 04" for the first two LOAD KEYFILE commands and "90 00" for the other commands.

AC_XX_VA_28 subclause 7 c23_7, c23_1, c23_15, c23_23

Purpose

Check that an Access Condition on UPDATE works properly.

Preconditions

- EF_{KEY_OP} with AC CHV1/PRO on UPDATE is selected.
- No AC is fulfilled.
- A random has been asked for.

Test

Perform an UPDATE BINARY command with a wrong cryptogram.

Perform a VERIFY CHV for CHV1.

Perform an UPDATE BINARY command without cryptogram.

Perform an ASK RANDOM command.

Perform an UPDATE BINARY command with a valid cryptogram.

Result

The expected status word is "98 04" for the first two UPDATE BINARY commands and "90 00" for the other commands.

AC_XX_VA_29 subclause 7 c23_21, c23_1, c23_15

Purpose

Check that an Access Condition on REHABILITATE works properly.

Preconditions

- EF_{KEY_OP} with AC CHV1 on REHABILITATE is selected.
- That file is invalidated.
- No AC is fulfilled.

Test

Perform a REHABILTATE command on that file.

Perform a VERIFY CHV on CHV1.

Perform a REHABILTATE command on that file.

Result

The expected status word is "98 04" for the first command and "90 00" for the other 2.

AC_XX_VA_30 subclause 7 c23_20, c23_1, c23_15

Purpose

Check that an Access Condition on INVALIDATE works properly.

Preconditions

- EF_{KEY_OP} with AC CHV1 on INVALIDATE is selected.
- That file is not invalidated.
- No AC is fulfilled.

Test

Perform an INVALIDATE command on that file.

Perform a VERIFY CHV on CHV1.

Perform an INVALIDATE command on that file.

Result

The expected status word is "98 04" for the first command and "90 00" for the other 2.

AC_XX_VA_31 subclause 7 c23_34, c23_1, c23_23

Purpose

Check that if EF_{KEY_MAN} is empty, the relevant keys are found on the next higher level.

Preconditions

- A DF different from the MF with an empty EF_{KEY_MAN} is selected.
- EF_{KEY_OP} with AC PRO on LOAD KEYFILE is selected.
- No AC is fulfilled.

Test

Perform an ASK RANDOM command.

Perform a LOAD KEYFILE command with a valid cryptogram using keys on the next higher level.

Result

The expected status word is "90 00" for all commands.

AC_XX_VA_32 subclause 7 c23_8, c23_1, c23_23

Purpose

Check that if EF_{KEY_OP} is missing, the relevant keys are found on the next higher level.

Preconditions

- A DF different from the MF without an EF_{KEY_OP} is selected.
- A linear fix structured file with AC PRO on UPDATE is selected.
- No AC is fulfilled.

Test

Perform an ASK RANDOM.

Perform an UPDATE RECORD with a valid cryptogram using keys on the next higher level.

Result

The expected status word is "90 00" for all commands.

AC_XX_VA_33 subclause 7 c23_12, c23_1, c23_15

Purpose

Check that the achieved AC is maintained as long as the selection still refers to the same relevant CHV.

Preconditions

- DF1 contains the relevant EF_{CHV1} for DF2.
- EF1 has the AC CHV1 on READ and resides in DF2.
- EF2 has the AC CHV1 on READ and resides in DF1.
- No AC is fulfilled.

Test

Perform a SELECT on EF1.

Perform a VERIFY CHV.

Perform a READ RECORD command.

Perform a SELECT on EF2.

Perform a READ RECORD command.

Result

The expected status word is "90 00" for all commands.

AC_XX_VA_34 subclause 7 c23_12, c23_1, c23_15

Purpose

Check that the achieved AC is maintained as long as the selection still refers to the same relevant CHV.

Preconditions

- DF1 contains the relevant EF_{CHV1} for DF2 and DF3.
- EF1 has the AC CHV1 on READ and resides in DF2.
- EF2 has the AC CHV1 on READ and resides in DF3.
- No AC is fulfilled.

Test

Perform a SELECT on EF1.

Perform a VERIFY CHV.

Perform a READ RECORD command.

Perform a SELECT on EF2.

Perform a READ RECORD command.

Result

The expected status word is "90 00" for all commands.

AC_XX_VA_35 subclause 7 c23_12, c23_1, c23_15

Purpose

Check that the achieved AC is maintained as long as the selection still refers to the same relevant CHV.

Preconditions

- DF1 exists under the MF and contains an $EF_{CHV1.}$
- DF2 exists under the MF.
- EF1 has the AC CHV1 on READ and resides in DF1.
- EF2 has the AC CHV1 on READ and resides in DF2.
- No AC is fulfilled.

Test

Perform a SELECT on DF1.

Perform a SELECT on EF1.

Perform a VERIFY CHV.

Perform a READ RECORD command.

Perform a SELECT on the MF.

Perform a SELECT on DF2.

Perform a SELECT on EF2.

Perform a READ RECORD command.

Perform a SELECT on the MF.

Perform a SELECT on DF1.

Perform a SELECT on EF1.

Perform a READ RECORD command.

Result

The expected status word is "90 00" for all commands except the READ on EF2, which returns "98 04".

AC_XX_VA_36 subclause 7 c23_12, c23_1, c23_15

Purpose

Check that the achieved AC is overwritten by a local CHV.

Preconditions

- DF1 contains the relevant EF_{CHV1} for DF2.
- DF3 contains a local EF_{CHV1}, but is son of DF1
- EF1 has the AC CHV1 on READ and resides in DF2.
- EF2 has the AC CHV1 on READ and resides in DF3.
- No AC is fulfilled.

Test

Perform a SELECT on EF1.

Perform a VERIFY CHV.

Perform a READ RECORD command.

Perform a SELECT on EF2.

Perform a READ RECORD command.

Perform a VERIFY CHV.

Perform a READ RECORD command.

Result

The expected status word is "90 00" for all commands, except the first READ RECORD on EF2.

AC_XX_VA_37 subclause 7 c23_ 12, c23_1, c23_15

Purpose

Check that if EFCHV is invalidated backtracking mechanism will be used.

Preconditions

- DF1 contains EF_{CHV1}.
- DF2 contains a local but invalidated EF_{CHV1}, and is son of DF1
- CHV1 in DF2 is different from CHV1 in DF1.
- EF1 exists with known contents and has the AC CHV1 on READ and resides in DF1.
- EF2 exists with known contents and has the AC CHV1 on READ and resides in DF2.
- DF2 is selected.
- EF2 is selected.
- No AC is fulfilled.

Test

Perform a VERIFY CHV1 with CHV1 of DF2.

Perform a VERIFY CHV1 with CHV1 of DF1.

Perform a READ command.

Perform a SELECT on DF1.

Perform a SELECT on EF1.

Perform a READ command.

Result

The first VERIFY CHV command returns status word "98 04"

All other commands return status word "90 00" and READ commands return the expected data.

6.2.6 Elementary Files (EF)

The base standard defines a number of special EFs. This *subclause* intends to test their existence and, depending on their readability, to some extent their contents.

The test method always issueing a SELECT command that may be followed by a READ BINARY. The responses to these commands shall be in accordance with the base standard.

6.2.6.1 EF_{CHV} (CHV)

File ID: "0000" or "0100"		Optional	
AC: READ NEV CREATE..EXECUTE NEV UPDATE Application provider WRITE NEV INVALIDATE Application provider REHABILITATE Application provider			
Bytes	Description	M / O	Length
1	EFCHV activation byte	M	1
2	Way to present the CHV/UNBLOCK CHV	M	1
3	KEY number in the relevant EF_{KEY_OP}	M	1
4-11	CHV	M	8
12	CHV attempts Preset value N	M	1
13	Remaining CHV attempt counter	M	1
14-21	UNBLOCK CHV	M	8
22	Remaining UNBLOCK CHV attempt counter	M	1
23	Number of remaining UNBLOCK mechanisms use	M	1

EF_CHV_VA_01 subclause 10.1 c36_1, c23_1

Purpose

Check for existence and settings of EF_{CHV1}.

Preconditions

- None

Test

Select EF_{CHV1}

Result

Select response data shall be as expected with respect to ACs, number of remaining CHV attempts, EFCHV activation byte, Way to present the CHV, key number in the relevant EF_{KEY_OP}, number of remaining UNBLOCK CHV attempts and number of remaining UNBLOCK CHV mechanisms.

EF_CHV_VA_02 subclause 10.1 c36_1, c23_1

Purpose

Check for existence and settings of EF_{CHV2}.

Preconditions

- None.

Test

Select EF_{CHV2}

Result

Select response data shall be in accordance with defined values in base standard.

6.2.6.2 EFDIR (DIR)

File ID: "2F00"		Optional	
AC: READ Issuer/Application provider CREATE..EXECUTE NEV UPDATE Issuer/Application provider WRITE Issuer/Application provider INVALIDATE Issuer/Application provider REHABILITATE Issuer/Application provider			
Bytes	Description	M / O	Length
1	Application identifier tag "4F"	M	1
2	Application identifier length	M	1
3	Application identifier	M	1-16
	Application label tag "50"	M	1
	Application label length	M	1
	Application label (Verbal description)	M	0-16
	Path tag "51"	M	1
	Path length	M	1
	Path	M	X

EF_DIR_VA_01 subclause 10.2 c36_2, c23_1, c23_10

Purpose

Check for existence, settings and possibly contents of EFDIR.

Preconditions

- None.

Test

Select EFDIR and if possible read the complete contents, and try to select each of the applications defined.

Result

Select response data shall be in accordance with defined values in base standard. If the file was readable then all defined applications shall be selectable.

6.2.6.3 EFIC (IC)

File ID: "0005"		Optional	
AC: READ ALW CREATE..EXECUTE NEV UPDATE NEV WRITE NEV INVALIDATE NEV REHABILITATE NEV			
Bytes	Description	M / O	Length
1-4	IC serial number	M	4
5-8	IC manufacturing references	M	4

EF_IC_VA_01 subclause 10.3 c36_3, c23_1, c23_10

Purpose
Check for existence, settings and contents of EFIC.

Preconditions
- None.

Test
Select EFIC and read the complete contents.

Result
Select response and read data shall be in accordance with defined values in base standard.

6.2.6.4 EF_{ICC} (ICC)

File ID: "0002"		Mandatory	
AC: READ ALW CREATE..EXECUTE NEV UPDATE NEV WRITE NEV INVALIDATE NEV REHABILITATE NEV			
Bytes	Description	M / O	Length
1	Clockstop	M	1
2-5	IC card serial number	M	4
6-9	IC card manufacturing references	M	4
10	Card personalizer ID	M	1
11-15	Embedder/IC assembler ID	M	5
16-17	IC identifier	O	2
18	Card profile	O	1
19	Type of selection	O	1

EF_ICC_VA_01 subclause 10.4 c36_4, c23_1, c23_10

Purpose
Check for existence, settings and contents of EF_{ICC}.

Preconditions
- None.

Test

Select EF_{ICC} and read the complete contents.

Result

Select response and read data shall be in accordance with defined values in base standard and ICS.

6.2.6.5 EFID (ID)

File ID: "0003"		Mandatory	
AC: READ ALW CREATE..EXECUTE NEV UPDATE NEV WRITE NEV INVALIDATE Issuer REHABILITATE Issuer			
Bytes	Description	M / O	Length
1-10	Identification number	M	10
11-13	Date of activation	O	3
14-16	Card expiry date	O	3
17	Card sequence number	O	1
18-19	Country code	O	2

EF_ID_VA_01 subclause 10.5 c36_5, c23_1, c23_10

Purpose

Check for existence, settings and contents of EFID.

Preconditions

- None.

Test

Select EFID and read the complete contents.

Result

Select response and read data shall be in accordance with defined values in base standard.

6.2.6.6 EF_{KEY_MAN} (MAN)

File ID: "0011"		Mandatory
AC: UPDATE NEV LOAD KEY FILE Application provider INVALIDATE Application provider REHABILITATE Application provider		
Bytes	Description	Length
1	Keyfile version	1
2	Keylength of key 1 (X)	1
3	Algorithm ID for key 1	1
4	KEY 1	X
4+X	Keylength of key 2 (Y)	1
5+X	Algorithm ID for key 2	1
6+X	KEY 2	Y
6+X+Y	Keylength of key 3 (Z)	1
7+X+Y	Algorithm ID for key 3	1
	..	

EF_MAN_VA_01 subclause 10.6 c36_6, c23_1

Purpose
Check for existence and settings of EF_{KEY_MAN}.

Preconditions
- None.

Test
Select EF_{KEY_MAN}

Result
Select response data shall be as expected with respect to ACs, key file versions, keylengths, and algorithm IDs.

6.2.6.7 EF_{KEY_OP} (OP)

File ID: "0001"	Optional	
AC: UPDATE NEV LOAD KEY FILE Application provider INVALIDATE Application provider REHABILITATE Application provider		
Bytes	Description	Length
1	Keyfile version	1
2	Keylength of key 1 (X)	1
3	Algorithm ID for key 1	1
4	KEY 1	X
4+X	Keylength of key 2 (Y)	1
5+X	Algorithm ID for key 2	1
6+X	KEY 2	Y
6+X+Y	Keylength of key 3 (Z)	1
7+X+Y	Algorithm ID for key 3	1
	..	

EF_OP_VA_01 subclause 10.7 c36_7, c23_1

Purpose
Check for existence and settings of EF_{KEY_OP}.

Preconditions
- None.

Test

Select EF_{KEY_OP}

Result

Select response data shall be as expected with respect to ACs, key file versions, keylengths, and algorithm IDs.

6.2.6.8 EFLANG (LAN)

File ID: "2F05"		Optional	
AC: READ ALW CREATE..EXECUTE NEV UPDATE User WRITE Issuer INVALIDATE Issuer REHABILITATE Issuer			
Bytes	Description	M / O	Length
1-2	First language preference	O	2
3-4	Second language preference	O	2
5-6	Third language preference	O	2
7-8	Fourth language preference	O	2

EF_LAN_VA_01 subclause 10.8 c36_8, c23_1, c23_10

Purpose

Check for existence, settings and contents of EFLANG.

Preconditions

- None.

Test

Select EFLANG and read the complete contents.

Result

Select response and read data shall be in accordance with defined values in base standard.

6.2.6.9 EFNAME (NAM)

File ID: "0004"		Optional	
AC: READ AUT CREATE..EXECUTE NEV UPDATE Issuer WRITE Issuer INVALIDATE Issuer REHABILITATE Issuer			
Bytes	Description	M / O	Length
1-X	Card holder name	O	X

EF_NAM_VA_01 subclause 10.9 c36_9, c23_1, c23_10, c23_23, c23_25, c41_1

Purpose

Check for existence, settings and contents of EFNAM.

Preconditions

- None.

Test

Select EFNAM, perform an external authentication and read the complete contents.

Result

Select response and read data shall be in accordance with defined values in base standard.

History

Document history		
V1.1.1	July 1997	Publication

ISBN 2-7437-1540-5
Dépôt légal : Juillet 1997