TS 101 207-2 V1.1.1 (1997-07)

Technical Specification

Identification card systems; Telecommunications IC cards and terminals; Test methods and conformance testing for EN 726-7; Part 2: Test Suite Structure and Test Purposes (TSS&TP)

European Telecommunications Standards Institute

Reference

DTS/PTS-00207-2 (b6ci0icr.PDF)

Keywords

Card, testing, ATS, TSS&TP, security

ETSI Secretariat

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

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

X.400

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

Internet

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

Contents

Intellectual Property Rights

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 726-7, as identified below:

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

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

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

Overview of ETSI deliverables on EN 726 family

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

Overview of ETSI deliverables on EN 726 conformance testing family

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

1 Scope

The present document provides Test Suite Structure and Test Purposes (TSS&TP). It applies to the Security Module (SM) defined in EN 726-7 [9] in compliance with the relevant requirements, and according to the relevant guidance given in ISO/IEC 9647-7 [14] and ETS 300 406 [12].

The set of test purposes described herein is intended to proof the compliance of a security module with the standard EN 726-7 [9] (about 140 tests) and it is seen as an extension of the test purposes made for TS 101 200-3 [8] (about 645 tests), however the number of tests and the depth of testing is not sufficient for a product qualification test.

For a product qualification at least the following tests should be added:

- User profile test

  To test whether the SM suits the need for a specific application. Here all possible scenarios should be run.

- Life cycle test

  To test the behaviour of a SM after it has been used for X transactions, where X is a multiple of the guaranteed life cycle of the programmable memory.

- Stress test

  To test the behaviour of the SM at physical stress, such as under voltage, over voltage, too high or low frequencies and spikes on the VCC/VPP line.

- Performance test

  To test whether the implementation is able to handle the defined scenarios within the defined time limits.

- Key test

  Each key in a SM should be used for its specified purpose at least once and the result should be checked.

- Additional file tests

  Each file present in the SM should be selected and read out, if possible. The answer to SELECT and the contents of the file should be checked against the specification.

Tests for additional functions

For a compliance with the specification the SM should at least be tested with:

- each allowed parameter, or at least their extreme values;
- at least one invalid parameter;
- each return code should at least be provoked once;
- the successful operation of the function should be tested.

In addition to that, tests can be added for:

- all invalid parameter combinations;
- undefined situations; etc.

2 Normative references

References may be made to:

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

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

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

d) publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

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

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

[3] 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)".

[4] 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)".

[5] 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)".

[6] 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)".

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

[8] 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".

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

[10] 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".

[11] 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".

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

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

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

[15] ISO/IEC 10202: "Financial Transaction cards: Security Architecture of financial transaction systems using Integrated Circuit Cards - Part 4: Secure Application Module".

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

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

[18] 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".

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

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

[21] 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".

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 [2],[3],[4],[5],[6];
- terms defined in TS 101 200-3 [8];
- terms defined in ISO/IEC 9646-1 [13] and in ISO/IEC 9646-7 [14].

In particular, the following terms defined in ISO/IEC 9646-1 [13] apply:

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

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

3.2 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
AP	ASK PARAMETER
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
DF	Dedicated Files
DK	Downloading of Key
EF	Elementary Files
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
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.

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 SM 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 TS 101 207-3 [21].

The voltage level for VCC (contact C1) of the SM 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 SM 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 SM.

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 single quotes ("99") in the present 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

The following statements are applicable to the test procedure clause for all test purposes contained within the present document:

- If there is a sequence control implemented, the commands have to be given in an allowed sequence. The sequence control is not tested.

- Positive return codes are SW1, SW2 = "90 00" or "9F XX", if the SM is an IC card, else every return code, that acknowledges the command.

- Negative return codes are all return codes that indicate an error has occurred.

- If "None." is stated as a precondition, that does not exclude the general statements made in this section.

- If variables are used in a table, they are only valid within that table and they have no relation with variables of the same name in other tables.

5 Test suite structure

- Security Module
  - Physical characteristics
  - Electronic signals and transmission protocols
  - Logical model
    - Permanent secrets
      - EF_{KEY_MAN} (SM)
      - EF_{KEY_OP} (SM)
      - EF_{KEY_MAN} (SM)
      - EF_{KEY_OP} (SM)
      - EF_{KEY_MAN} (UCx)
      - EF_{KEY_OP} (UCx)
    - Temporary secrets
      - EF_{DIK1} (UCx)
      - EF_{DIK2} (UCx)
    - Balance
      - EF_{AMOUNT}
    - Operating system
      - MF
      - EF_{ICC}
      - EF_{DIR}
      - DF
      - $EF_{KEYTABLE}$
  - Functions
    - Functions without any MAC
      - SELECT KEYSET
      - DIVERSIFY KEYSET
      - ASK PARAMETER
    - Functions used to compute a MAC
      - COMPUTE LOAD KEY
      - COMPUTE MAC
      - COMPUTE CRYPTOGRAM
      - DECREASE (SM)
    - Functions used to verify a MAC
      - VERIFY MAC
      - UPDATE (SM)
      - INCREASE (SM)
      - VERIFY CRYPTOGRAM
  - Downloading of keys from SM to UC

6 Test Purposes (TP)

6.1 Introduction

For each test requirement a 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. See table 1.

Table 1: TP Identifier naming convention scheme

Identifier:	**<group>_<subgroup>_<type>_<nnn>**			
<group>	=	major group	PC :	Physical characteristics
			SP :	Electronic Signals and transmission Protocols
			LM :	Logical Model
			RC :	Return Codes
			FU :	Functions
			CO :	Commands
			DK :	Downloading of Keys
<subgroup>	=	function or file	two characters to indicate the function,	
			e.g.	AP for ASK PARAMETER
				XX if function independent.
<type>	=	type	one character field representing the type of test	
			VA:	Valid behaviour test
			IV:	Invalid behaviour test
<nnn>	=	sequential number:	(01-99)	

6.1.2 Source of TP definition

The TPs were developed based on EN 726-7 [9] and TS 101 207-1 [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 should be read in conjunction with any TP, that is, 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/IXIT limitation* c<table no>_<item no>{.<subitem no>}{, }}	see table 1 subclause 0.0.0 c9_3.1, c9_3.2
Stimulus	Ensure that the SM for <command> *or* <File EF>	SELECT KEYSET $\text{EF}_{\text{KEY\_MAN}}$
Reaction	<action> <conditions>	results in, contains, ... after selecting, using parameter, if supported ...
NOTE: Text in italics will not appear in TPs and text between <> is filled in for each TP and may differ from one TP to the next.		

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 should 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 invalid commands, parameters or states are tested to see, whether the implementation shows robustness against invalid stimuli and that the returned Status Words (SW) comply with the standard.

6.2 Security Module (SM)

6.2.1 Physical characteristics

The EN 726-7 [9] does not focus on physical characteristics. If, however, the SM is a card it gives reference to TS 101 200-3 [8], where a number of details, that should be similar to or slightly different from those defined in referenced standards, are pointed out.

Therefore the required tests, or references to them, for a SM as a chipcard are found in the test standard for TS 101 200-3 [10].

6.2.2 Electronic signals and transmission protocols

The EN 726-7 [9] does not focus on electrical signals and transmission protocols characteristics It does, however, give reference to TS 101 200-3 [8], where a number of details that should be similar to or slightly different from those defined in referenced standards are pointed out.

Therefore the required tests, or references to them, for a SM as a chipcard are found in the test standard for EN 726-3 (TS 101 203-1 [10]).

6.2.3 Logical Model (LM)

6.2.3.1 Permanent secrets

LM_PS_VA_01 subclause A.4.4 c1_1, c3_1, c12_1, c16_4

Table 3: Coding of EF_{KEY_MAN}(SM) at MF-Level

<table>
<tr><td colspan="2"><b>File ID : "00 11"</b></td><td><b>Mandatory</b></td></tr>
<tr><td colspan="3">AC:
UPDATE NEV
LOAD KEY FILE Application provider
INVALIDATE Application provider
REHABILITATE Application provider</td></tr>
<tr><td><b>Bytes</b></td><td><b>Description</b></td><td><b>Length</b></td></tr>
<tr><td>1</td><td>Keyfile version</td><td>1</td></tr>
<tr><td>2</td><td>Keylength of key 1 (X)</td><td>1</td></tr>
<tr><td>3</td><td>Algorithm ID for key 1</td><td>1</td></tr>
<tr><td>4..(3 + X)</td><td>KEY 1</td><td>X</td></tr>
<tr><td>(4 + X)</td><td>Keylength of key 2 (Y)</td><td>1</td></tr>
<tr><td>(5 + X)</td><td>Algorithm ID for key 2</td><td>1</td></tr>
<tr><td>(6 + X)...</td><td>KEY 2</td><td>Y</td></tr>
<tr><td></td><td>...</td><td></td></tr>
</table>

Purpose

Ensure that the coding of the EF_{KEY_MAN}(SM) is valid at MF-Level.

Preconditions

- None.

Test

Perform a SELECT on EF_{KEY_MAN} (SM) and analyse the response of the SELECT command.

Result

SELECT response data should be in accordance with the expected values (loaded keys, their length and algorithms).

LM_PS_VA_02 subclause A.4.5 c1_1, c3_1, c12_1, c16_5

Table 4: Coding of EF$_{KEY\_OP}$(SM) at MF-Level

File ID : "00 01"		**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..(3 + X)	KEY 1	X
(4 + X)	Keylength of key 2 (Y)	1
(5 + X)	Algorithm ID for key 2	1
(6 + X)...	KEY 2	Y
	...	

Purpose

Ensure that the coding of the EF$_{KEY\_OP}$(SM) is valid at MF-Level.

Preconditions

- None.

Test

Perform a SELECT on EF$_{KEY\_OP}$ (SM) and analyse the response of the SELECT command.

Result

SELECT response data should be in accordance with the expected values (loaded keys, their length and algorithms).

LM_PS_VA_03 subclause A.3 c1_1, c3_1, c12_1, c16_4

Table 5: Coding of EF$_{KEY\_MAN}$(SM) at DF-Level

File ID : "00 11"		**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..(3 + X)	KEY 1	X
(4 + X)	Keylength of key 2 (Y)	1
(5 + X)	Algorithm ID for key 2	1
(6 + X)...	KEY 2	Y
	...	

Purpose

Ensure that the coding of the EF$_{KEY\_MAN}$(SM) is valid at DF-Level.

Preconditions

- The DF containing the keyset is selected.

Test

Perform a SELECT on EF_{KEY_MAN} (SM) and analyse the response of the SELECT command.

Result

SELECT response data should be in accordance with the expected values (loaded keys, their length and algorithms).

LM_PS_VA_04 subclause A.3 c1_1, c3_1, c12_1, c16_5

Table 6: Coding of EF_{KEY_OP}(SM) at DF-Level

File ID : "00 01"		**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..(3 + X)	KEY 1	X
(4 + X)	Keylength of key 2 (Y)	1
(5 + X)	Algorithm ID for key 2	1
(6 + X)...	KEY 2	Y
	...	

Purpose

Ensure that the coding of the EF_{KEY_OP}(SM) is valid at DF-Level.

Preconditions

- The DF containing the keyset is selected.

Test

Perform a SELECT on EF_{KEY_OP} (SM) and analyse the response of the SELECT command.

Result

SELECT response data should be in accordance with the expected values (loaded keys, their length and algorithms).

LM_PS_VA_05 subclause A.4.7 c1_1, c3_1, c12_1, c16_7

Table 7: Coding of EF_{KEY_MAN}(UC)

<table>
<tr><td colspan="2"><b>File ID : "20 XX"</b></td><td><b>Optional</b></td></tr>
<tr><td colspan="3">AC:
UPDATE NEV
LOAD KEY FILE Application provider
INVALIDATE Application provider
REHABILITATE Application provider</td></tr>
<tr><td><b>Bytes</b></td><td><b>Description</b></td><td><b>Length</b></td></tr>
<tr><td>1</td><td>Keyfile version</td><td>1</td></tr>
<tr><td>2</td><td>Keylength of key 1 (X)</td><td>1</td></tr>
<tr><td>3</td><td>Algorithm ID for key 1</td><td>1</td></tr>
<tr><td>4..(3 + X)</td><td>KEY 1</td><td>X</td></tr>
<tr><td>(4 + X)</td><td>Keylength of key 2 (Y)</td><td>1</td></tr>
<tr><td>(5 + X)</td><td>Algorithm ID for key 2</td><td>1</td></tr>
<tr><td>(6 + X)...</td><td>KEY 2</td><td>Y</td></tr>
<tr><td></td><td>...</td><td></td></tr>
</table>

Purpose

Ensure that the coding of the EF_{KEY_MAN}(UC) is valid.

Preconditions

- The DF containing the keyset is selected.

Test

Perform a SELECT on EF_{KEY_MAN} (UC) and analyse the response of the SELECT command.

Result

SELECT response data should be in accordance with the expected values (loaded keys, their length and algorithms).

LM_PS_VA_06 subclause A.4.7 c1_1, c3_1, c12_1, c16_8

Table 8: Coding of EF_{KEY_OP}(UC)

<table>
<tr><td colspan="2"><b>File ID : "21 YY"</b></td><td><b>Mandatory</b></td></tr>
<tr><td colspan="3">AC:
UPDATE NEV
LOAD KEY FILE Application provider
INVALIDATE Application provider
REHABILITATE Application provider</td></tr>
<tr><td><b>Bytes</b></td><td><b>Description</b></td><td><b>Length</b></td></tr>
<tr><td>1</td><td>Keyfile version</td><td>1</td></tr>
<tr><td>2</td><td>Keylength of key 1 (X)</td><td>1</td></tr>
<tr><td>3</td><td>Algorithm ID for key 1</td><td>1</td></tr>
<tr><td>4..(3 + X)</td><td>KEY 1</td><td>X</td></tr>
<tr><td>(4 + X)</td><td>Keylength of key 2 (Y)</td><td>1</td></tr>
<tr><td>(5 + X)</td><td>Algorithm ID for key 2</td><td>1</td></tr>
<tr><td>(6 + X)...</td><td>KEY 2</td><td>Y</td></tr>
<tr><td></td><td>...</td><td></td></tr>
</table>

Purpose

Ensure that the coding of the EF_{KEY_OP}(UC) is valid.

Preconditions

- The DF containing the keyset is selected.

Test

Perform a SELECT on EF_{KEY_OP} (UC) and analyse the response of the SELECT command.

Result

SELECT response data should be in accordance with the expected values (loaded keys, their length and algorithms).

6.2.3.2 Temporary secrets

LM_TS_VA_01 subclause A.4.10 c1_1, c3_2, c12_1, c16_11

Table 9: Coding of EF_{DIK1} (UC)

File ID : "10 00"	**Optional**
AC: UPDATE NEV LOAD KEY FILE Application provider INVALIDATE Application provider REHABILITATE Application provider	

Bytes	**Description**	**Length**
1	Keyset version	1
2	Keylength of key 1 (X)	1
3	Algorithm ID for key 1	1
4..(3 + X)	KEY 1	X
(4 + X)	Keylength of key 2 (Y)	1
(5 + X)	Algorithm ID for key 2	1
(6 + X)...	KEY 2	Y
	...	

Purpose

Ensure that the coding of the EF_{DIK1} (UC) is valid.

Preconditions

- The DF containing the keyset is selected.
- EF_{KEYMAN} is diversified using EF_{DIK1} as a destination

Test

Perform a SELECT on EF_{DIK1} (UC) and analyse the response of the SELECT command.

Result

SELECT response data should be in accordance with the expected values (loaded keys, their length and algorithms).

LM_TS_VA_02 subclause A.4.10 c1_1, c3_2, c12_1, c16_12

Table 10: Coding of EF_{DIK2}(UC)

File ID : "11 00"		**Mandatory**
AC: UPDATE NEV LOAD KEY FILE Application provider INVALIDATE Application provider REHABILITATE Application provider		
Bytes	**Description**	**Length**
1	Keyset version	1
2	Keylength of key 1 (X)	1
3	Algorithm ID for key 1	1
4..(3 + X)	KEY 1	X
(4 + X)	Keylength of key 2 (Y)	1
(5 + X)	Algorithm ID for key 2	1
(6 + X)...	KEY 2	Y
	...	

Purpose

Ensure that the coding of the EF_{DIK2}(UC) is valid.

Preconditions

- The DF containing the keyset is selected.
- EF_{KEYOP} is diversified using EF_{DIK2} as a destination

Test

Perform a SELECT on EF_{DIK2}(UC) and analyse the response of the SELECT command.

Result

SELECT response data should be in accordance with the expected values (loaded keys, their length and algorithms).

6.2.3.3 Balance

LM_BA_VA_01 subclause A.4.9 c1_1, c3_3, c12_1, c16_10

Table 11: Coding of $\text{EF}_{\text{AMOUNT}}$(SM)

File ID : "12 XX"		**Optional**
AC: READ PRO CREATE ... EXECUTE PRO DECREASE PRO INCREASE PRO INVALIDATE PRO REHABILITATE PRO		
Bytes	**Description**	**Length**
1..3	Counter value	3

Purpose

Ensure that the contents of the $\text{EF}_{\text{AMOUNT}}$(SM) is valid.

Preconditions

- None.

Test

Perform a SELECT on EF_{AMOUNT}(SM) and analyse the response of the SELECT command. Perfom a READ on that file and check the contents.

Result

SELECT response data should be in accordance with the expected values (size and access conditions), the contents shall have the expected values.

6.2.3.4 Operating system

LM_OS_VA_01 subclause A.4.1 c1_1, c3_4, c12_1, c16_1

Table 12: Coding of MF

File ID : "3F 00"	**Mandatory**
AC: DELETE FILE Application provider CREATE/EXTEND FILE Application provider INVALIDATE Application provider REHABILITATE Application provider	

Purpose

Ensure that the coding of the MF is valid.

Preconditions

- None.

Test

Apply a SELECT command [8] to the MF.

Result

The successful execution of the SELECT command shall return valid coding for a MF.

LM_OS_VA_02 subclause A.4.2 c1_1, c3_4, c12_1, c16_2

Table 13: Coding of EF_{ICC}

File ID : "00 02"		**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

Purpose
Check for existence, settings and contents of EF_{ICC}.

Preconditions

- None.

Test

Apply a SELECT and a READ BINARY to EF_{ICC}.

Result

The response to SELECT and READ BINARY shall be in accordance with defined values in TS 101 200-3 [8]. Ensure that the contents of the EF_{ICC} is valid.

LM_OS_VA_03 subclause A.4.3 c1_1, c3_4, c12_1, c16_3

Table 14: Coding of EF_{DIR}

File ID : "2F 00"		**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

Purpose

Check for existence, settings and possibly contents of EF_{DIR}.

Preconditions

- None.

Test

SELECT EF_{DIR} and if possible READ the complete contents, and try to SELECT with AID each of the DFs of the applications in EF_{DIR}.

Result

SELECT response data should be in accordance with defined values in base standard. If the file was readable then all DFs of the applications in EF_{DIR} shall be selectable.

LM_OS_VA_04 subclause A.4.6 c1_1, c3_4, c12_1, c16_6

Table 15: Coding of DFx

File ID : "XX XX"	**Mandatory**
AC: DELETE FILE Application provider CREATE/EXTEND FILE Application provider INVALIDATE Application provider REHABILITATE Application provider	

Purpose

Ensure that the DFx exists.

Preconditions

- None.

Test

Apply a SELECT command [8] to the DF.

Result

The successful execution of the SELECT command shall return valid coding for a DF.

LM_OS_VA_05 subclause A.4.8 c1_1, c3_4, c12_1, c16_9

Table 16: Coding of $EF_{KEYTABLE}$

<table>
<tr><th colspan="2">File ID : "02 XX"</th><th>Mandatory</th></tr>
<tr><td colspan="3">AC:
READ NEV
CREATE ... EXECUTE PRO
UPDATE NEV
WRITE NEV
INVALIDATE NEV
REHABILITATE NEV</td></tr>
<tr><th>Bytes</th><th>Description</th><th>Length</th></tr>
<tr><td>1</td><td>INS of the SM command</td><td>1</td></tr>
<tr><td>2</td><td>INS of the UC command which is included in the cryptogram</td><td>1</td></tr>
<tr><td>3</td><td>Key number linked to the SM command</td><td>1</td></tr>
<tr><td>4..5</td><td>File ID of the relevant file in the SM</td><td>2</td></tr>
<tr><td>6</td><td>INS of the SM command</td><td>1</td></tr>
<tr><td>7</td><td>INS of the UC command which is included in the cryptogram</td><td>1</td></tr>
<tr><td>8</td><td>Key number linked to the SM command</td><td>1</td></tr>
<tr><td>9..10</td><td>File ID of the relevant file in the SM</td><td>2</td></tr>
<tr><td>...</td><td>...</td><td></td></tr>
</table>

Purpose

Ensure that the contents of the $EF_{KEYTABLE}$ is valid.

Preconditions

- None.

Test

Apply a SELECT to $EF_{KEYTABLE}$.

Result

The result of SELECT shall return a correct size and the expected access conditions.

6.2.4 Functions

6.2.6.1 General tests

The following tests do not apply to any specific instruction, but are common to all.

RC_XX_IV_01 subclause 9.3.1.4 c1_1, c15_10

Purpose

Ensure that the SM recognizes a not allowed instruction class. See IXIT for a not allowed instruction class.

Preconditions

- None.

Test

Send any supported command such as ASK PARAMETER, with the not allowed CLA-Byte.

Result

The expected status word is "6E XX".

RC_XX_IV_02 subclause 9.3.1.4 c1_1, c15_11

Purpose
Ensure that the SM recognizes a not allowed instruction code. See IXIT for a not allowed instruction code.

Preconditions

- None.

Test
Send any byte combination with a not allowed INS-Byte, but valid CLA-Byte.

Result
The expected status word is "6D XX".

RC_XX_IV_03 subclause 9.3.1.4 c1_1, c15_12

Purpose
Ensure that the SM returns "6F XX" on technical problems.

Preconditions

- None.

Test
No test can be given for a generic implementation, so nothing is tested for technical problems.

Result
The expected status word is "6F XX".

RC_XX_IV_04 subclause 9.3.1.4 c1_1, c15_3

Purpose
Ensure that the SM checks the sequence of the commands.

Preconditions

- None.

Test
No test can be given for a generic implementation, so nothing is tested for a sequence control.

Result
The expected status word is "98 AD".

6.2.4.1 Without MAC

6.2.4.1.1 SELECT KEYSET

FU_SK_VA_01 subclause 8.1.1 c9_1, c14_1.8, c15_15

Table 17: Key qualifier (in case of a MF in the UC)

Bytes	Description	M/O	Length
1..4	IC card manufacturing references (coded according to EN726-3 [8])	M	4
5	Card personalizer ID (coded according to TS 101 200-3 [8])	M	1
6..7	File ID of the EF_{KEY}	M	2
8	Keyfile version (coded according to TS 101 200-3 [8])	M	1

Purpose
Ensure that the SM with SELECT KEYSET is able to select a keyset from the MF in the SM.

Preconditions

- A keyset for the MF of the UC exists in the SM.

Test
Send a SELECT KEYSET command with a parameter field containing the keyset description for the MF.

Result
The expected status word is "90 00".

FU_SK_VA_02 subclause 8.1.1 c9_1, c14_1.8, c15_15

Table 18: Key qualifier (in case of a DF in the UC)

Bytes	Description	M/O	Length
1..X	AID (coded according to TS 101 200-3 [8])	M	1 - 16
(X + 1) .. (X + 2)	File ID of the EF_{KEY}	M	2
X + 3	Keyfile version (coded according to TS 101 200-3 [8])	M	1

Purpose
Ensure that the SM with SELECT KEYSET is able to select a keyset from a DF in the SM.

Preconditions

- A keyset for the DF of the UC exists in the SM.

Test
Send a SELECT KEYSET command with a parameter field containing the keyset description for the DF.

Result
The expected status word is "90 00".

FU_SK_VA_03 subclause 8.1.1 c9_1.1, c14_1.8, c15_15

Purpose

Ensure that the SM with SELECT KEYSET is able to select a specific keyset from a DF of the SM.

Preconditions

– A second keyset for the DF of the UC exists in the SM.

Test

Send a SELECT KEYSET command with a parameter field containing the keyset description for the second keyset in the DF.

Result

The expected status word is "90 00".

Table 19: Coding of the SELECT KEYSET command

CLA	Class byte
INS	"50"
P1	"00"
P2	"00"
L_c field	Length of data field
Data field	Key qualifier (see above)
L_e field	Empty

CO_SK_IV_01 subclause A.5.2.1, 8.1.1 c1_1, c9_1, c18_1, c14_1.2, c15_8

Purpose

Ensure that the SM checks the availability of a file, when using the SELECT KEYSET command and that it fails when a not existing application identifier is used.

Preconditions

– A description for a not existing keyset exists (Wrong AID).

Test

Send a SELECT KEYSET command with a parameter field containing the not existing keyset.

Result

The expected status word is "94 04".

CO_SK_IV_02 subclause A.5.2.1, 8.1.1 c1_1, c9_1, c18_1, c14_1.2, c15_8

Purpose
Ensure that the SM checks the availability of a file, when using the SELECT KEYSET command and that it fails when a not existing file identifier is used.

Preconditions

- A keyset exists.

Test
Send a SELECT KEYSET command with a parameter field containing a different file ID.

Result
The expected status word is "94 04".

CO_SK_IV_03 subclause A.5.2.1, 8.1.1 c1_1, c9_1, c18_1, c14_1.2, c15_8

Purpose
Ensure that the SM checks the availability of a file, when using the SELECT KEYSET command and that it fails when containing not existing manufacturing references are used.

Preconditions

- A keyset exists on MF level.

Test
Send a SELECT KEYSET command with a parameter field containing not existing manufacturing references.

Result
The expected status word is "94 04".

CO_SK_IV_04 subclause A.5.2.1, 8.1.1 c1_1, c9_1, c18_1, c14_1.2, c15_8

Purpose
Ensure that the SM checks the availability of a file, when using the SELECT KEYSET command and that it fails when containing a not existing Card personalizer ID is used.

Preconditions

- A keyset exists on MF level.

Test
Send a SELECT KEYSET command with a parameter field containing not existing Card personalizer ID.

Result
The expected status word is "94 04".

CO_SK_IV_05 subclause A.5.2.1, 8.1.1 c1_1, c9_1, c18_1, c14_1.2, c15_8

Purpose

Ensure that the SM checks the availability of a file, when using the SELECT KEYSET command and that it fails when containing a not existing keyfile version number is used.

Preconditions

- A keyset exists.

Test

Send a SELECT KEYSET command with a parameter field containing not existing keyfile version number.

Result

The expected status word is "94 04".

Table 20: Return codes for SELECT KEYSET

Return Code	Error description
98 AD	- Command out of sequence
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 ≠ "08" in case of a key qualifier for the MF - L_C < "04" or L_C > "13" in case of a key qualifier for a DF
90 00	- Normal ending (ACK) of the command

RC_SK_IV_01 subclause A.5.2.1, 8.1.1 c1_1, c9_1, c18_1, c14_1.6, c15_13

Purpose

Ensure that the SM checks the value of P1 and P2 to be "00".

Preconditions

- A keyset exists.

Test

Send a SELECT KEYSET command with a parameter P1 ≠ 0 or P2 ≠ 0.

Result

The expected status word is "6B XX".

RC_SK_IV_02 subclause A.5.2.1, 8.1.1 c1_1, c9_1, c18_1, c14_1.7, c15_14

Purpose
Ensure that the SM checks the value of Lc to be "08" for a keyfile in the MF.

Preconditions

- A keyset exists.

Test
Send a SELECT KEYSET command with a parameter Lc ≠ "08".

Result
The expected status word is "67 XX".

RC_SK_IV_03 subclause A.5.2.1, 8.1.1 c1_1, c9_1, c18_1, c14_1.7, c15_14

Purpose
Ensure that the SM checks the value of Lc to be between "04" and "13" for a keyfile in the DF.

Preconditions

- A keyset exists.

Test
Send a SELECT KEYSET command with a parameter Lc < "04" or Lc > "13".

Result
The expected status word is "67 XX".

6.2.4.1.2 DIVERSIFY KEYSET

FU_DK_VA_01 subclause 8.1.2 c9_1, c9_2,c14_2.9,c15_15

Table 21: Diversification data

Bytes	Description	M/O	Length
1..X	Diversification data (application dependent)	M	1 - 16

Purpose
Ensure that the SM with DIVERSIFY KEYSET is able to derive temporary keys from all the master keys of the previously selected keyset.

Preconditions

- A SELECT KEYSET on a keyset containing master keys has been done successfully.

Test
Send a DIVERSIFY KEYSET command with a parameter field containing valid diversification data.

Result
The expected status word is "90 00".

FU_DK_IV_01 subclause 8.1.2 c9_2.2, c14_2.2, c15_6

Purpose
Ensure that the SM requires a SELECT KEYSET before a DIVERSIFY KEYSET can be performed.

Preconditions

- A SELECT KEYSET has not been done.

Test
Send a DIVERSIFY KEYSET command with a parameter field containing valid diversification data.

Result
The expected status word is "94 00".

Table 22: Coding of the DIVERSIFY KEYSET command

CLA	Class byte
INS	"52"
P1	"00" EF_{DIK} number 1 temporary keys selected as active keyset for all following commands "01" EF_{DIK} number 2 temporary keys to be downloaded
P2	"00"
L_c field	Length of data field
Data field	Algorithm ID for diversification diversification data
L_e field	Empty

CO_DK_VA_01 subclause 8.1.2 c1_1, c9_1, c9_2, c14_2.9, c15_15

Purpose
Ensure that the SM with DIVERSIFY KEYSET is able to derive temporary keys from all the master keys of the previously selected keyset and uses EF_{DIK1} for storing the diversified keys.

Preconditions

- A SELECT KEYSET on a keyset containing master keys has been done successfully.

Test
Send a DIVERSIFY KEYSET command with a parameter field containing valid diversification data and P1 = "00".

Result
The expected status word is "90 00".

CO_DK_VA_02 subclause 8.1.2 c1_1, c9_1, c9_2,c14_2.9,c15_15

Purpose

Ensure that the SM with DIVERSIFY KEYSET is able to derive temporary keys from all the master keys of the previously selected keyset and uses EF_{DIK2} for storing the diversified keys.

Preconditions

– A SELECT KEYSET on a keyset containing master keys has been done successfully.

Test

Send a DIVERSIFY KEYSET command with a parameter field containing valid diversification data and P1 = "01".

Result

The expected status word is "90 00".

Table 23: Return codes for DIVERSIFY KEYSET

Return Code	Error description
98 AD	- Command out of sequence
94 00	- No EF selected
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" and P1 ≠ "01" or P2 ≠ "00"
67 XX	- No test is foreseen for this status word
90 00	- Normal ending (ACK) of the command

RC_DK_IV_01 subclause A.5.2.2, 8.1.2 c1_1, c9_1, c9_2, c14_2.3, c15_9, c18_1, c18_2

Purpose

Ensure that the SM checks the type of the selected EF.

Preconditions

– A SELECT KEYSET on a keyset containing diversified keys has been done successfully.

Test

Send a DIVERSIFY KEYSET command with a parameter field containing valid diversification data.

Result

The expected status word is "94 08".

RC_DK_IV_02 subclause A.5.2.2, 8.1.2 c1_1, c9_1, c9_2, c18_1, c18_2, c14_2.7, c15_13

Purpose

Ensure that the SM checks the value of P1 to be "00" or "01" and P2 to be "00"

Preconditions

- A SELECT KEYSET on a keyset containing master keys has been done successfully.

Test

Send a DIVERSIFY KEYSET command with a parameter field containing valid diversification data, but P1 ≠ "00" and "01" or P2 ≠ "00".

Result

The expected status word is "6B XX".

6.2.4.1.3 ASK PARAMETER

FU_AP_VA_01 subclause 8.1.3 c9_1, c9_3, c11_4, c14_3.8, c15_15

Table 24: Returned value

Bytes	Description	M/O	Length
1 - X	Challenge	M	X

Purpose

Ensure that the SM keeps the challenge until the next function requires it.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done successfully.

Test

Send an ASK PARAMETER command, followed by a VERIFY CRYPTOGRAM or any other command requiring an ASK PARAMETER.

Result

The expected status word is "90 00" for all commands.

FU_AP_VA_02 subclause 8.1.3 c9_1, c9_3.1, c11_1,c14_3.8, c14_8.9, c15_15

Purpose

Ensure that the SM keeps the challenge as long only VERIFY MAC is used.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done successfully.

Test

Send an ASK PARAMETER command, followed by two VERIFY MAC commands.

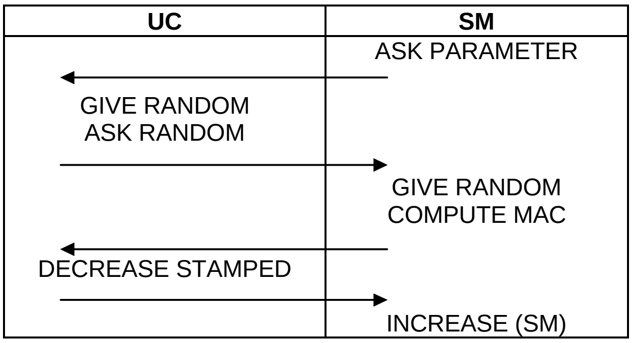
Result

The expected status word is "90 00" for all commands.

FU_AP_VA_03 subclause 8.1.3 c9_1, c9_3.1, c10_2, c11_3, c12_1, c14_3.8, c14_6.8, c14_10.12, c15_15

For a SM supporting the INCREASE (SM) command it is necessary to keep the random number at least during a GIVE RANDOM and the COMPUTE MAC command.

The following scenario is tested for the SM :



UC

SM

ASK PARAMETER

GIVE RANDOM
ASK RANDOM

GIVE RANDOM
COMPUTE MAC

DECREASE STAMPED

INCREASE (SM)

Purpose
Ensure that the SM keeps the challenge until a function uses it.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done successfully.

Test

Send an ASK PARAMETER command, asking for a random.
Send a GIVE RANDOM, with a random number from a UC.
Send a COMPUTE MAC with a data field for DECREASE STAMPED.
Send a INCREASE (SM) command, with the data returned from the UC.

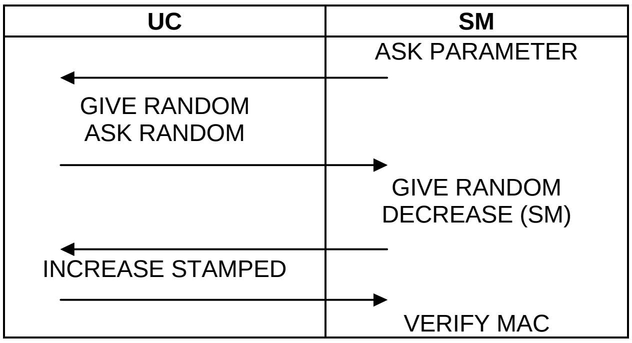
Result

The expected status word is "90 00" for all commands.

FU_AP_VA_04 subclause 8.1.3 c9_1, c9_3.1, c10_4, c11_1, c12_1, c14_3.8, c14_8.9, c14_11.11, c15_15

For a SM supporting the DECREASE (SM) command it is necessary to keep the random number at least during a GIVE RANDOM and the DECREASE (SM) command.

The following scenario is tested for the SM :



UC

SM

ASK PARAMETER

GIVE RANDOM
ASK RANDOM

GIVE RANDOM
DECREASE (SM)

INCREASE STAMPED

VERIFY MAC

Purpose
Ensure that the SM keeps the challenge until a function uses it.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done successfully.

Test

Send an ASK PARAMETER command, asking for a random.
Send a GIVE RANDOM, with a random number from a UC.
Send a DECREASE (SM) with a data field for INCREASE STAMPED.
Send a VERIFY MAC command, with the data returned from the UC.

Result

The expected status word is "90 00" for all commands.

FU_AP_VA_05 subclause 8.1.3 c9_3, c14_3.8, c15_15

Purpose
Ensure that the SM sends different random values.

Preconditions

- An ASK PARAMETER to ask for a random has been done.

Test

Send an ASK PARAMETER to ask for a random.

Result

The expected status word is "90 00". The returned random values shall be different.

FU_AP_VA_06 subclause 8.1.3 c9_1, c9_3.2.1, c14_3.8, c15_15

Purpose
Ensure that the SM uses separate counters for individual keysets.

Preconditions

- An ASK PARAMETER to ask for a counter value has been done.
- A SELECT KEYSET has been done successfully.

Test

Send a SELECT KEYSET for another keyset.

Send an ASK PARAMETER to ask for a counter.

Result

The expected status words are "90 00". The returned counter value shall not be the successor of the counter value returned before.

FU_AP_VA_07 subclause 8.1.3 c9_1, c9_3.3, c14_3.8, c15_15

Purpose

Ensure that the SM uses the same counter for individual keysets.

Preconditions

- An ASK PARAMETER to ask for a counter value has been done.
- A SELECT KEYSET has been done successfully.

Test

Send a SELECT KEYSET for another keyset.

Send an ASK PARAMETER to ask for a counter.

Result

The expected status words are "90 00". The returned counter value shall be the successor of the counter value returned before.

FU_AP_IV_01 subclause 8.1.3 c9_1, c9_3.1, c11_4, c14_8.3, c15_2

Purpose

Ensure that the SM keeps the challenge only until the next function requires it.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done successfully.
- An ASK PARAMETER has been done.
- A VERIFY CRYPTOGRAM command or any other command requiring an ASK PARAMETER except VERIFY MAC has been given.

Test

Send a VERIFY CRYPTOGRAM command or any other command requiring an ASK PARAMETER except VERIFY MAC commands.

Result

The expected status word is "98 35".

Table 25: Coding of the ASK PARAMETER command

CLA	Class byte
INS	"54"
P1	"00" random number "01" counter related to the selected keyset containing masterkeys
P2	"00"
L_c field	Empty
Data field	Empty
L_e field	Maximum length of data expected in response

CO_AP_IV_01 subclause A.5.3.1, 8.1.3 c1_1, c9_1, c9_3, c18_1, c18_3, c14_3.2, c15_7

Purpose
Ensure that the SM checks the range of the counter.

Preconditions

– A SELECT KEYSET on a keyset containing master keys has been done successfully.

– The counter value is "FF".

Test
Send an ASK PARAMETER (counter) with a response length of one byte.

Result
The expected status word is "94 02".

Table 26: Return codes for ASK PARAMETER

Return Code	Error description
98 AD	- Command out of sequence
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
94 02	- Out of range (invalid address)
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 P1 ≠ "01" or P2 ≠ "00"
67 XX	- Le = 0
90 00	- Normal ending (ACK) of the command

RC_AP_IV_01 subclause A.5.3.1, 8.1.3 c1_1, c9_3, c18_3, c14_3.6, c15_13

Purpose
Ensure that the SM checks the value of P1 ≠ "00" and P1 ≠ "01" or P2 ≠ "00".

Preconditions

- None.

Test
Send an ASK PARAMETER with P1 ≠ "00" and P1 ≠ "01" or P2 ≠ "00".

Result
The expected status word is "6B XX".

6.2.4.2 To compute a MAC

6.2.4.2.1 COMPUTE LOAD KEY

Table 27: Structure of COMPUTE LOAD KEY

Bytes	Description	M/O	Length
-X..0	Command Header		X + 1
1	INS byte of the following LOAD KEY FILE command sent to the UC (coded according to TS 101 200-3 [8])	M	1
2	P1 of the following LOAD KEY FILE command sent to the UC (coded according to TS 101 200-3 [8])	M	1
3	P2 of the following LOAD KEY FILE command sent to the UC (coded according to TS 101 200-3 [8])	M	1
4	Lc of the following LOAD KEY FILE command sent to the UC (coded according to TS 101 200-3 [8])	M	1
5	Key file version (only present if key number 1)	M	1
6	Key length	M	1
7	Algorithm identifier	M	1
8..Y	Command Trailer		Y-7

Table 28: Answer to COMPUTE LOAD KEY

Bytes	Description	M/O	Length
1 .. 16	Enciphered key	M	16
17 .. 24	MAC	M	8

FU_CL_VA_01 subclause 8.2.1 c9_1, c10_1.1, c10_1.2, c12_1, c14_12.8, c15_15

Purpose
Ensure that the SM is able to calculate the proper answer to load a key into a UC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done successfully.

- A GIVE RANDOM has been sent.

Test

Send a COMPUTE LOAD KEY command.

Result

The expected status word is "90 00". The returned value is checked against the expected values.

FU_CL_VA_02 subclause 8.2.1 c2_2, c9_1, c10_1.1, c10_1.2, c12_1, c14_12.9, c15_16

Purpose

Ensure that the SM is able to calculate the proper answer to load a key into a UC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done successfully.
- A GIVE RANDOM has been sent.

Test

Send a COMPUTE LOAD KEY command.

Result

The expected status word is "9F XX". The returned value is checked against the expected values.

FU_CL_IV_01 subclause 8.2.1 c9_1, c12_1, c10_1.3, c14_12.2, c15_2

Purpose

Ensure that the SM requires a Random number to compute the load key.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done successfully.
- A GIVE RANDOM has not been sent.

Test

Send a COMPUTE LOAD KEY command.

Result

The expected status word is "98 35".

FU_CL_IV_02 subclause 8.2.1 c10_1.4, c12_1, c15_6

Purpose

Ensure that the SM checks that a keyset has been selected.

Preconditions

- A SELECT KEYSET has not been done.
- A GIVE RANDOM has been sent.

Test

Send a COMPUTE LOAD KEY command.

Result

The expected status word is "94 00".

FU_CL_IV_03 subclause 8.2.1 c9_1, c10_1.4.1, c12_1, c15_9

Purpose

Ensure that the SM checks that the keyset contains diversified keys.

Preconditions

- A SELECT KEYSET on a keyset containing master keys has been done.
- A GIVE RANDOM has been sent.

Test

Send a COMPUTE LOAD KEY command.

Result

The expected status word is "94 08".

Table 29: Coding of the COMPUTE LOAD KEY command

CLA	Class byte
INS	"70"
P1	"00" EF$_{DIK}$ number 1 is the source for the keys to download "01" EF$_{DIK}$ number 2 is the source for the keys to download
P2	Key number of the load key in the active keyset
L$_c$ field	"07" key number 1 is computed "06" for all other keys
Data field	"D8" (coded according to TS 101 200-3 [8]) EF$_{KEY}$ type (coded according to TS 101 200-3 [8]) Key to download (coded according to TS 101 200-3 [8]) L$_C$ of the command sent to the UC (coded according to TS 101 200-3 [8]) Key file version (only present if key number 1) Key length Algorithm identifier
L$_e$ field	Maximum length of data expected in response

CO_CL_IV_01 subclause A.5.4.1, 8.2.1 c1_1, c9_1, c10_1, c12_1, c14_12.7, c15_14, c18_1, c18_4

Purpose

Ensure that the SM checks the value of L$_c$ to be "07", if key number 1 is to be computed.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test

Send a COMPUTE LOAD KEY command with a data field and L$_c$ longer than 7 bytes, but the first 7 bytes contain a valid coding.

Result

The expected status word is "67 XX".

CO_CL_IV_02 subclause A.5.4.1, 8.2.1 c1_1, c9_1, c10_1, c12_1, c14_12.7, c15_14, c18_1, c18_4

Purpose

Ensure that the SM checks the value of L_c to be "06", if any other key than key 1 is to be computed.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test

Send a COMPUTE LOAD KEY command with a data field and L_c longer than 6 byte, but the first 6 bytes contain a valid coding.

Result

The expected status word is "67 XX".

CO_CL_IV_03 subclause A.5.4.1, 8.2.1 c1_1, c9_1, c10_1, c12_1, c15_8, c18_1, c18_4

Purpose

Ensure that the SM checks the coding of the data field (key number).

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test

Send a COMPUTE LOAD KEY command with a data field containing a not existing key number.

Result

The expected status word is "94 04".

CO_CL_IV_04 subclause A.5.4.1, 8.2.1 c1_1, c9_1, c10_1, c12_1, c15_8, c18_1, c18_4

Purpose

Ensure that the SM checks the coding of the data field (key version).

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test

Send a COMPUTE LOAD KEY command with a data field containing a not existing key version.

Result

The expected status word is "94 04".

CO_CL_IV_05 subclause A.5.4.1, 8.2.1 c1_1, c9_1, c10_1, c12_1, c15_8, c18_1, c18_4

Purpose
Ensure that the SM checks the coding of the data field (algo ID).

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test
Send a COMPUTE LOAD KEY command with a data field containing a not existing algo ID.

Result
The expected status word is "94 04".

CO_CL_IV_06 subclause A.5.4.1, 8.2.1 c1_1, c9_1, c10_1, c15_8, c12_1, c18_1, c18_4

Purpose
Ensure that the SM checks the coding of the data field (key length).

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test
Send a COMPUTE LOAD KEY command with a data field containing an existing key with an invalid length.

Result
The expected status word is "94 04".

Table 30: Return codes for COMPUTE LOAD KEY

Return Code	Error description
98 35	- No ASK PARAMETER/GIVE RANDOM before
98 AD	- Command out of sequence
94 00	- No EF selected
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" and P1 ≠ "01"
67 XX	- L_C ≠ "06" and L_C ≠ "07"
90 00	- Normal ending (ACK) of the command
9F XX	- Length "XX" of the response data

RC_CL_IV_01 subclause A.5.4.1, 8.2.1 c1_1, c9_1, c10_1, c12_1, c18_1, c18_4, c14_12.6, c15_13

Purpose
Ensure that the SM checks the value of P1 to be "00" or "01".

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test
Send a COMPUTE LOAD KEY command with a parameter P1 ≠ "00" and P1 ≠ "01".

Result
The expected status word is "6B XX".

6.2.4.2.2 COMPUTE MAC

Table 31: Structure of COMPUTE MAC

Bytes	Description	M/O	Length
-X..0	Command Header		X + 1
1	INS byte of the following command sent to the UC (coded according to TS 101 200-3 [8])	M	1
2	P1 of the following command sent to the UC (coded according to TS 101 200-3 [8])	M	1
3	P2 of the following command sent to the UC (coded according to TS 101 200-3 [8])	M	1
4	Lc of the following command sent to the UC (coded according to TS 101 200-3 [8])	M	1
5 .. (4 + Z)	The data field of the following command sent to the UC (coded according to TS 101 200-3 [8])	M	Z
(5 + Z) ...	Command Trailer		

Table 32: Answer to COMPUTE MAC

Bytes	Description	M/O	Length
1 .. X	MAC	M	X

FU_CM_VA_01 subclause 8.2.2 c9_1, c12_1, c10_2.1, c14_12.8, c15_15

Purpose

Ensure that the SM is able to calculate a proper MAC for the UC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test

Send a COMPUTE MAC command with an allowed UC command.

Result

The expected status word is "90 00". The returned value is checked against the expected values.

FU_CM_VA_02 subclause 8.2.2 c2_2, c9_1, c12_1, c10_2.1, c14_6.9, c15_16

Purpose

Ensure that the SM is able to calculate a proper MAC for the UC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test

Send a COMPUTE MAC command with an allowed UC command.

Result

The expected status word is "9F XX". The returned value is checked against the expected values.

FU_CM_IV_01 subclause 8.2.2 c9_1, c10_2.2, c14_6.2, c15_2

Purpose

Ensure that the SM requires a Random number to compute the MAC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has not been sent.

Test

Send a COMPUTE MAC command with an allowed UC command.

Result

The expected status word is "98 35".

FU_CM_IV_02 subclause 8.2.2 c12_1, c10_2.3, c15_6

Purpose
Ensure that the SM checks that a keyset has been selected.

Preconditions

- A SELECT KEYSET has not been done.
- A GIVE RANDOM has been sent.

Test
Send a COMPUTE MAC command with an allowed UC command.

Result
The expected status word is "94 00".

FU_CM_IV_03 subclause 8.2.2 c9_1, c12_1, c10_2.3.1, c15_9

Purpose
Ensure that the SM checks that the keyset contains diversified keys.

Preconditions

- A SELECT KEYSET on a keyset containing master keys has been done.
- A GIVE RANDOM has been sent.

Test
Send a COMPUTE MAC command with an allowed UC command.

Result
The expected status word is "94 08".

FU_CM_IV_04 subclause 8.2.2 c9_1, c12_1, c10_2, c15_9

Purpose
Ensure that the SM checks that the given function is allowed.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test
Send a COMPUTE MAC command with a not allowed UC command.

Result
The expected status word is "94 08".

Table 33: Coding of the COMPUTE MAC command

CLA	Class byte
INS	"8A"
P1	"00"
P2	Key number
L_c field	Length of the data field (≥ "04")
Data field	INS of following UC command (coded according to TS 101 200-3 [8]) P1 of following UC command (coded according to TS 101 200-3 [8]) P2 of following UC command (coded according to TS 101 200-3 [8]) L_c of following UC command (coded according to TS 101 200-3 [8]) data field of following UC command (coded according to TS 101 200-3 [8])
L_e field	Maximum length of data expected in response

Table 34: Return codes for COMPUTE MAC

Return Code	Error description
98 35	- No ASK PARAMETER/GIVE RANDOM before
98 AD	- Command out of sequence
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"
67 XX	- L_c < "04"
90 00	- Normal ending (ACK) of the command
9F XX	- Length "XX" of the response data

RC_CM_IV_01 subclause A.5.4.2, 8.2.2 c1_1, c9_1, c12_1, c10_2, c18_1, c18_5, c14_6.6, c15_13

Purpose

Ensure that the SM checks the value of P1 to be "00".

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test

Send a COMPUTE MAC command with a parameter P1 ≠ "00".

Result

The expected status word is "6B XX".

RC_CM_IV_02 subclause A.5.4.2, 8.2.2 c1_1, c9_1, c12_1, c10_2, c14_6.7, c15_14, c18_1, c18_5

Purpose
Ensure that the SM checks the value of $L_c \geq$ "04".

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test
Send a COMPUTE MAC command with a L_c of less than 4 and a matching data field.

Result
The expected status word is "67 XX".

6.2.4.2.3 COMPUTE CRYPTOGRAM

The command COMPUTE CRYPTOGRAM corresponds to the UC command EXTERNAL AUTHENTICATION.

Table 35: Answer to COMPUTE CRYPTOGRAM

Bytes	Description	M/O	Length
1 .. X	Cryptogram	M	X

FU_CC_VA_01 subclause 8.2.3 c9_1, c12_1, c10_3.1, c14_4.8, c15_15

Purpose
Ensure that the SM is able to calculate a proper cryptogram for the UC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test
Send a COMPUTE CRYPTOGRAM command.

Result
The expected status word is "90 00". The returned value is checked against the expected values.

FU_CC_VA_02 subclause 8.2.3 c2_2, c9_1, c12_1, c10_3.1, c14_12.9, c15_16, c14_4.9, c15_16

Purpose

Ensure that the SM is able to calculate a proper cryptogram for the UC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test

Send a COMPUTE CRYPTOGRAM command.

Result

The expected status word is "9F XX". The returned value is checked against the expected values.

FU_CC_IV_01 subclause 8.2.3 c9_1, c10_3.2, c14_4.2, c15_2

Purpose

Ensure that the SM requires a Random number to compute the cryptogram.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has not been sent.

Test

Send a COMPUTE CRYPTOGRAM command.

Result

The expected status word is "98 35".

FU_CC_IV_02 subclause 8.2.3 c12_1, c10_3.3, c15_6

Purpose

Ensure that the SM checks that a keyset has been selected.

Preconditions

- A SELECT KEYSET has not been done.
- A GIVE RANDOM has been sent.

Test

Send a COMPUTE CRYPTOGRAM command.

Result

The expected status word is "94 00".

FU_CC_IV_03 subclause 8.2.3 c9_1, c12_1, c10_3.3.1, c15_9

Purpose

Ensure that the SM checks that the keyset contains diversified keys.

Preconditions

- A SELECT KEYSET on a keyset containing master keys has been done.
- A GIVE RANDOM has been sent.

Test

Send a COMPUTE CRYPTOGRAM command.

Result

The expected status word is "94 08".

Table 36: Coding of the COMPUTE CRYPTOGRAM command

CLA	Class byte
INS	"56"
P1	"00"
P2	Key number
L_c field	Empty
Data field	Empty
L_e field	Maximum length of data expected in response

Table 37: Return codes for COMPUTE CRYPTOGRAM

Return Code	Error description
98 35	- No ASK PARAMETER/GIVE RANDOM before
98 AD	- Command out of sequence
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"
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

RC_CC_IV_01 subclause A.5.4.2, 8.2.2 c1_1, c9_1, c12_1, c10_3, c18_1, c18_6, c14_4.6, c15_13

Purpose

Ensure that the SM checks the value of P1 to be "00".

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.

Test

Send a COMPUTE CRYPTOGRAM command with a parameter P1 ≠ "00".

Result

The expected status word is "6B XX".

6.2.4.2.4 DECREASE (SM)

Table 38: Structure of DECREASE (SM)

Bytes	Description	M/O	Length
-X..0	Command Header		X + 1
1	INS byte of the following INCREASE or INCREASE STAMPED command sent to the UC (coded according to TS 101 200-3 [8])	M	1
2	P1 of the following INCREASE or INCREASE STAMPED command sent to the UC (coded according to TS 101 200-3 [8])	M	1
3	P2 of the following INCREASE or INCREASE STAMPED command sent to the UC (coded according to TS 101 200-3 [8])	M	1
4	Lc of the following INCREASE or INCREASE STAMPED command sent to the UC (coded according to TS 101 200-3 [8])	M	1
5 .. (4 + Z)	The data field of the following INCREASE or INCREASE STAMPED command sent to the UC (coded according to TS 101 200-3 [8])	M	Z
(5 + Z) ...	Command Trailer		

Table 39: Answer to DECREASE (SM)

Bytes	Description	M/O	Length
1 .. X	MAC	M	X

FU_DS_VA_01 subclause 8.3.4 c9_1, c12_1, c10_4.5, c14_11.11, c15_15

Purpose

Ensure that the SM is able to calculate a MAC for the UC and to decrease the amount stored in the counter of the SM.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.
- A SELECT on the counter to be decreased has been performed.

Test

Send a DECREASE (SM) command with valid data.
Send a READ RECORD command to read the contents.

Result

The expected status word for DECREASE (SM) is "90 00". The MAC shall be correct. The returned value of the READ RECORD command shall be the expected one.

FU_DS_VA_02 subclause 8.3.4 c2_2, c9_1, c12_1, c10_4.5, c14_11.12, c15_16

Purpose

Ensure that the SM is able to calculate a MAC for the UC and to decrease the amount stored in the counter of the SM.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.
- A SELECT on the counter to be decreased has been performed.
- The contents should be known

Test

Send a DECREASE (SM) command with valid data.
Send a READ RECORD command to read the contents.

Result

The expected status word for DECREASE (SM) is "9F XX". The MAC shall be correct. The returned value of the READ RECORD command shall be the expected one.

FU_DS_IV_01 subclause 8.3.4 c9_1, c12_1, c10_4.1, c14_11.5, c15_9

Purpose

Ensure that the SM checks the indicated key.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.
- A SELECT on the counter to be decreased has been performed.

Test

Send a DECREASE (SM) command with valid data, but invalid key.

Result

The expected status word is "94 08".

FU_DS_IV_02 subclause 8.3.4 c9_1, c12_1, c10_4, c14_11.5, c15_9

Purpose

Ensure that the SM checks that an INCREASE or INCREASE STAMPED will be used.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.
- A SELECT on the counter to be decreased has been performed.

Test

Send a DECREASE (SM) command with valid data, but invalid INS for the UC command.

Result

The expected status word is "94 08".

FU_DS_IV_03 subclause 8.3.4 c9_1, c12_1, c10_4.2, c14_11.2, c15_2

Purpose

Ensure that the SM requires a Random number to compute the MAC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has not been sent.
- A SELECT on the counter to be decreased has been performed.

Test

Send a DECREASE (SM) command with valid data.

Result

The expected status word is "98 35".

FU_DS_IV_04 subclause 8.3.4 c9_1, c12_1, c10_4.3, c14_11.4, c15_6

Purpose

Ensure that the SM checks that a keyset has been selected.

Preconditions

- A SELECT KEYSET has not been done.
- A GIVE RANDOM has been sent.
- A SELECT on the counter to be decreased has been performed.

Test

Send a DECREASE (SM) command with valid data.

Result

The expected status word is "94 00".

FU_DS_IV_05 subclause 8.3.4 c9_1, c12_1, c10_4.3.1, c14_11.5, c15_9

Purpose

Ensure that the SM checks that the keyset contains diversified keys.

Preconditions

- A SELECT KEYSET on a keyset containing master keys has been done.
- A GIVE RANDOM has been sent.
- A SELECT on the counter to be decreased has been performed.

Test

Send a DECREASE (SM) command with valid data.

Result

The expected status word is "94 08".

FU_DS_IV_06 subclause 8.3.4 c9_1, c12_1, c10_4.4, c14_11.4, c15_6

Purpose

Ensure that the SM checks that a counter to be decreased is selected.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.
- A SELECT on the counter to be decreased has not been performed.

Test

Send a DECREASE (SM) command with valid data.

Result

The expected status word is "94 00".

Table 40: Coding of the DECREASE (SM) command

CLA	Class byte
INS	"5E"
P1	"00"
P2	Key number
L_c field	Length of the data field (≥ "04")
Data field	INS of following INCREASE or INCREASE STAMPED command sent to the UC (coded according to TS 101 200-3 [8]) P1 of following INCREASE or INCREASE STAMPED command sent to the UC (coded according to TS 101 200-3 [8]) P2 of following INCREASE or INCREASE STAMPED command sent to the UC (coded according to TS 101 200-3 [8]) L_c of following INCREASE or INCREASE STAMPED command sent to the UC (coded according to TS 101 200-3 [8]) data field of following INCREASE or INCREASE STAMPED command sent to the UC (coded according to TS 101 200-3 [8])
L_e field	Maximum length of data expected in response

Table 41: Return codes for DECREASE (SM)

Return Code	Error description
98 35	- No ASK PARAMETER/GIVE RANDOM before
98 AD	- Command out of sequence
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
94 00	- No EF selected
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"
67 XX	- L_c < "04"
90 00	- Normal ending (ACK) of the command
9F XX	- Length "XX" of the response data

RC_DS_IV_01 subclause A.5.6.2, 8.3.4 c1_1, c9_1, c12_1, c10_4, c18_1, c18_11, c14_11.9, c15_13

Purpose

Ensure that the SM checks the value of P1 to be "00".

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.
- A SELECT on the counter to be decreased has been performed.

Test

Send a DECREASE (SM) command with a parameter P1 ≠ "00".

Result

The expected status word is "6B XX".

RC_DS_IV_02 subclause A.5.6.2, 8.3.4 c1_1, c9_1, c12_1, c10_4, c14_11.10, c15_14, c18_1, c18_11

Purpose

Ensure that the SM checks the value of $L_c \geq$ "04".

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.
- A SELECT on the counter to be decreased has been performed.

Test

Send a DECREASE (SM) command with a L_c of less than 4 and a matching data field.

Result

The expected status word is "67 XX".

RC_DS_IV_03 subclause A.5.6.2, 8.3.4 c9_1, c12_1, c10_4, c15_4

Purpose

Ensure that the SM is able to report the memory problems, when writing.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.
- A SELECT on the counter to be decreased has been performed.
- The memory can be written, after using the internal retry routine X times.

Test

Send a DECREASE (SM) command with valid data.

Result

The expected status word for DECREASE (SM) is "92 0X". The MAC shall be correct.

RC_DS_IV_04 subclause A.5.6.2, 8.3.4 c9_1, c12_1, c10_4, c15_5

Purpose

Ensure that the SM is able to report the memory problems, when writing.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- A GIVE RANDOM has been sent.
- A SELECT on the counter to be decreased has been performed.
- The memory can not be written.

Test

Send a DECREASE (SM) command with valid data.

Result

The expected status word for DECREASE (SM) is "92 40".

6.2.4.2.5 COMPUTE MAC EW

Table 42: Structure of COMPUTE MAC EW

Bytes	Description	M/O	Length
-X..0	Command Header		X + 1
1 .. Z	Data	M	Z
(Z + 1) ...	Command Trailer		

Table 43: Answer to COMPUTE MAC EW

Bytes	Description	M/O	Length
1 .. X	MAC	M	X

FU_CME_VA_01 subclause 8.2.3 c9_1, c12_1, c10_5.1, c14_7.8, c15_15

Purpose
Ensure that the SM is able to calculate a proper MAC for the data.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- The selected key has the flag "AUTHENTICATION ALLOWED" set.
- An ASK PARAMETER command has been used.

Test
Send a COMPUTE MAC EW command with any data without chaining.

Result
The expected status word is "90 00". The returned value is checked against the expected values.

FU_CME_VA_02 subclause 8.2.3 c2_2, c9_1, c12_1, c10_5.1, c14_7.9, c15_16

Purpose
Ensure that the SM is able to calculate a proper MAC for the data.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- The selected key has the flag "AUTHENTICATION ALLOWED" set.
- An ASK PARAMETER command has been used.

Test
Send a COMPUTE MAC EW command with any data without chaining.

Result
The expected status word is "9F XX". The returned value is checked against the expected values.

FU_CME_VA_03 subclause 8.2.3 c9_1, c12_1, c10_5.1, c10_5.2, c14_7.8, c14_7.9, c15_15, c15_16

Purpose

Ensure that the SM is able to calculate a proper MAC for the data using chaining.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- The selected key has the flag "AUTHENTICATION ALLOWED" set.
- An ASK PARAMETER command has been used.

Test

Send a COMPUTE MAC EW command with the first part of the data with chaining.
Send a COMPUTE MAC EW command with the second part of the data without chaining.

Result

The expected status word is "90 00" for both commands, only the second response includes the MAC. The returned value is checked against the expected values.

FU_CME_VA_04 subclause 8.2.3 c2_2, c9_1, c12_1, c10_5.1, c10_5.2, c14_7.8, c14_7.9, c15_15, c15_16

Purpose

Ensure that the SM is able to calculate a proper MAC for the data using chaining.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- The selected key has the flag "AUTHENTICATION ALLOWED" set.
- An ASK PARAMETER command has been used.

Test

Send a COMPUTE MAC EW command with the first part of the data with chaining.
Send a COMPUTE MAC EW command with the second part of the data without chaining.

Result

The expected status word is "90 00" for the first command and "9F XX" for the second command. The returned value is checked against the expected values.

FU_CME_IV_01 subclause 8.2.3 c9_1, c10_5.2, c14_7.2, c15_2

Purpose
Ensure that the SM requires a Random number to compute the MAC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- The selected key has the flag "AUTHENTICATION ALLOWED" set.
- An ASK PARAMETER command has not been used.

Test
Send a COMPUTE MAC EW command with any data without chaining.

Result
The expected status word is "98 35".

FU_CME_IV_02 subclause 8.2.3 c12_1, c10_5.3, c15_6

Purpose
Ensure that the SM checks that a keyset has been selected.

Preconditions

- A SELECT KEYSET has not been done.
- The selected key has the flag "AUTHENTICATION ALLOWED" set.
- An ASK PARAMETER command has been used.

Test
Send a COMPUTE MAC EW command with any data without chaining.

Result
The expected status word is "94 00".

FU_CME_IV_03 subclause 8.2.3 c9_1, c12_1, c10_5.3, c15_9

Purpose
Ensure that the SM checks that the keyset contains diversified keys.

Preconditions

- A SELECT KEYSET on a keyset containing master keys has been done.
- The selected key has the flag "AUTHENTICATION ALLOWED" set.
- An ASK PARAMETER command has been used.

Test
Send a COMPUTE MAC command with any data without chaining.

Result
The expected status word is "94 08".

FU_CME_IV_04 subclause 8.2.3 c9_1, c12_1, c10_2, c15_9

Purpose

Ensure that the SM checks that the selected key is allowed for authentication.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- The selected key has the flag "AUTHENTICATION ALLOWED" cleared.
- An ASK PARAMETER command has been used.

Test

Send a COMPUTE MAC EW command with any data without chaining.

Result

The expected status word is "94 08" (key-type is inconsistent with the command).

Table 44: Coding of the COMPUTE MAC EW command

CLA	Class byte
INS	"XX"
P1	"00" No chaining or last block "01" Chaining
P2	Key number
L_c field	Length of the data field
Data field	Any data
L_e field	Maximum length of data expected in response

Table 45: Return codes for COMPUTE MAC EW

Return Code	Error description
98 35	- No ASK PARAMETER/GIVE RANDOM before
98 AD	- Command out of sequence
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 P1≠ "01"
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

RC_CME_IV_01 subclause A.5.4.3, 8.2.3 c1_1, c9_1, c12_1, c10_5, c18_1, c18_12, c14_7.6, c15_13

Purpose
Ensure that the SM checks the value of P1 to be "00" or "01".

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- The selected key has the flag "AUTHENTICATION ALLOWED" set.

Test
Send a COMPUTE MAC EW command with a parameter P1 ≠ "00" and P1 ≠ "01".

Result
The expected status word is "6B XX".

6.2.4.3 To verify a MAC

6.2.4.3.1 VERIFY MAC

Table 46: Structure of VERIFY MAC

Bytes	Description	M/O	Length
-X..0	Command Header		X + 1
1	INS byte of the previous command sent to the UC (coded according to TS 101 200-3 [8])	M	1
2	P1 of the previous command sent to the UC (coded according to TS 101 200-3 [8])	M	1
3	P2 of the previous command sent to the UC (coded according to TS 101 200-3 [8])	M	1
4	Le of the previous command sent to the UC (coded according to TS 101 200-3 [8])	M	1
5 .. (4 + Z)	The data field of the previous response sent by the UC (coded according to TS 101 200-3 [8])	M	Z
(5 + Z) ...	Command Trailer		

FU_VM_VA_01 subclause 8.3.1 c9_1, c9_3, c11_1, c14_8.9, c15_15

Purpose
Ensure that the SM is able to verify a MAC from the UC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.

Test
Send a VERIFY MAC command with valid data.

Result
The expected status word is "90 00".

FU_VM_IV_01 subclause 8.3.1 c9_1, c9_3, c11_1, c14_8.2, c15_1

Purpose
Ensure that the SM really verifies the MAC from the UC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.

Test
Send a VERIFY MAC command with valid data, but invalid MAC.

Result
The expected status word is "98 04".

FU_VM_IV_02 subclause 8.3.1 c9_1, c9_3, c11_1.1, c15_8

Purpose
Ensure that the SM checks the indicated key.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.

Test
Send a VERIFY MAC command with valid data, but an invalid key.

Result
The expected status word "94 04".

FU_VM_IV_03 subclause 8.3.1 c9_1, c9_3, c11_1, c15_9

Purpose

Ensure that the SM checks the function codes.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.

Test

Send a VERIFY MAC command with valid data, but an invalid INS for the UC command.

Result

The expected status word "94 08". (INS-code inconsistent with the command)

FU_VM_IV_04 subclause 8.3.1 c9_1, c11_1.2, c14_8.3, c15_2

Purpose

Ensure that the SM requires a Random number to verify the MAC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has not been used.

Test

Send a VERIFY MAC command with valid data.

Result

The expected status word is "98 35".

FU_VM_IV_05 subclause 8.3.1 c9_3, c11_1.3, c15_8

Purpose

Ensure that the SM checks that a keyset has been selected.

Preconditions

- A SELECT KEYSET has not been done.
- An ASK PARAMETER command has been used.

Test

Send a VERIFY MAC command with valid data.

Result

The expected status word is "94 04".

FU_VM_IV_06 subclause 8.3.1 c9_1, c9_3, c11_1.3.1, c15_9

Purpose

Ensure that the SM checks that the keyset contains diversified keys.

Preconditions

- A SELECT KEYSET on a keyset containing master keys has been done.
- An ASK PARAMETER command has been used.

Test

Send a VERIFY MAC command with valid data.

Result

The expected status word is "94 08".

Table 47: Coding of the VERIFY MAC command

CLA	Class byte
INS	"8E"
P1	"00"
P2	Key number
L_c field	Length of data field (L_c > "04")
Data field	INS of previous UC command (coded according to TS 101 200-3 [8]) P1 of previous UC command (coded according to TS 101 200-3 [8]) P2 of previous UC command (coded according to TS 101 200-3 [8]) L_e of previous UC command (coded according to TS 101 200-3 [8]) response of previous UC command (coded according to TS 101 200-3 [8])
L_e field	Empty

Table 48: Return codes for VERIFY MAC

Return Code	Error description
98 04	- Wrong cryptogram verification
98 35	- No ASK PARAMETER/GIVE RANDOM before
98 AD	- Command out of sequence
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"
67 XX	- L_c < "04"
90 00	- Normal ending (ACK) of the command

RC_VM_IV_01 subclause A.5.5.1, 8.3.1 c1_1, c9_1, c9_3, c11_1.3, c14_8.7, c15_13, c18_1, c18_3, c18_7

Purpose
Ensure that the SM checks the value of P1 to be "00".

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.

Test
Send a VERIFY MAC command with a parameter P1 ≠ "00".

Result
The expected status word is "6B XX".

RC_VM_IV_02 subclause A.5.5.1, 8.3.1 c1_1, c9_1, c9_3, c11_1.3, c14_8.8, c15_14, c18_1, c18_3, c18_7

Purpose
Ensure that the SM checks the value of L_c ≥ "04".

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.

Test
Send a VERIFY MAC command with a L_c of less than 4 and a matching data field.

Result
The expected status word is "67 XX".

6.2.4.3.2 UPDATE (SM)

Table 49: Structure of UPDATE (SM)

Bytes	Description	M/O	Length
-X..0	Command Header		X + 1
1	INS byte of the previous READ RECORD STAMPED command sent to the UC (coded according to TS 101 200-3 [8])	M	1
2	P1 of the previous READ RECORD STAMPED command sent to the UC (coded according to TS 101 200-3 [8])	M	1
3	P2 of the previous READ RECORD STAMPED command sent to the UC (coded according to TS 101 200-3 [8])	M	1
4	Le of the previous READ RECORD STAMPED command sent to the UC (coded according to TS 101 200-3 [8])	M	1
5 .. (4 + Z)	The data field of the of the previous READ RECORD STAMPED response sent by the UC (coded according to TS 101 200-3 [8])	M	Z
(5 + Z) ...	Command Trailer		

FU_US_VA_01 subclause 8.3.2 c9_1, c9_3, c12_1, c11_2, c14_9.13, c15_15

Purpose
Ensure that the SM is able to verify a MAC from the UC and to update the information in the SM.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the file to be updated has been performed.

Test
Send an UPDATE (SM) command with valid data.
Send a READ RECORD command.

Result
The expected status word is "90 00". The read contents should be the one expected (5 .. (4 + Z)).

FU_US_IV_01 subclause 8.3.2 c9_1, c9_3, c12_1, c11_2.1, c14_9.2, c15_1

Purpose

Ensure that the SM really verifies the MAC from the UC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the file to be updated has been performed.

Test

Send an UPDATE (SM) command with valid data, but invalid MAC.

Result

The expected status word is "98 04".

FU_US_IV_02 subclause 8.3.2 c9_1, c9_3, c12_1, c11_2.1, c14_9.2, c15_1

Purpose

Ensure that the SM does not update the information, if used with invalid data.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the file to be updated has been performed.
- The contents should be known.

Test

Send an UPDATE (SM) command with valid data, but invalid MAC.
Send a READ RECORD command.

Result

The expected status word is "98 04" on UPDATE (SM). The read contents should be the original contents.

FU_US_IV_03 subclause 8.3.2 c9_1, c9_3, c12_1, c11_2.2, c15_8

Purpose

Ensure that the SM checks the indicated key.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the file to be updated has been performed.

Test

Send an UPDATE (SM) command with valid data, but invalid key.

Result

The expected status word is "94 04".

FU_US_IV_04 subclause 8.3.2 c9_1, c9_3, c12_1, c11_2, c14_9.7, c15_9

Purpose

Ensure that the SM checks that a READ RECORD STAMPED was used.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the file to be updated has been performed.

Test

Send an UPDATE (SM) command with valid data, but an invalid INS for the UC command and a valid MAC.

Result

The expected status word is "94 08".

FU_US_IV_05 subclause 8.3.2 c9_1, c12_1, c11_2.3, c14_9.3, c15_2

Purpose

Ensure that the SM requires a Random number to verify the MAC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has not been used.
- A SELECT on the file to be updated has been performed.

Test

Send an UPDATE (SM) command with valid data.

Result

The expected status word is "98 35".

FU_US_IV_06 subclause 8.3.2 c9_3, c12_1, c11_2.4, c14_9.6, c15_6

Purpose
Ensure that the SM checks that a keyset has been selected.

Preconditions

- A SELECT KEYSET has not been done.
- An ASK PARAMETER command has been used.
- A SELECT on the file to be updated has been performed.

Test
Send an UPDATE (SM) command with valid data.

Result
The expected status word is "94 00".

FU_US_IV_07 subclause 8.3.2 c9_1, c9_3, c12_1, c11_2.4.1, c14_9.7, c15_9

Purpose
Ensure that the SM checks that the keyset contains diversified keys.

Preconditions

- A SELECT KEYSET on a keyset containing master keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the file to be updated has been performed.

Test
Send an UPDATE (SM) command with valid data.

Result
The expected status word is "94 08".

FU_US_IV_08 subclause 8.3.2 c9_1, c9_3, c12_1, c11_2.5, c14_9.6, c15_6

Purpose
Ensure that the SM checks that an EF to be updated is selected.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- No EF is selected.

Test
Send an UPDATE (SM) command with valid data.

Result
The expected status word is "94 00".

Table 50: Coding of the UPDATE (SM) command

CLA	Class byte
INS	"5A"
P1	"00"
P2	Key number.
L_c field	Length of data field
Data field	"B6" (coded according to TS 101 200-3 [8]) Record no. (coded according to TS 101 200-3 [8]) Mode (coded according to TS 101 200-3 [8]) L_e of previous command (coded according to TS 101 200-3 [8]) data field of previous READ RECORD STAMPED response (coded according to TS 101 200-3 [8])
L_e field	Empty

Table 51: Return codes for UPDATE (SM)

Return Code	Error description
98 04	- Wrong cryptogram verification
98 35	- No ASK PARAMETER/GIVE RANDOM before
98 AD	- Command out of sequence
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
94 00	- No EF selected
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"
67 XX	- L_c < "04"
90 00	- Normal ending (ACK) of the command

RC_US_IV_01 subclause A.5.5.2, 8.3.2 c1_1, c9_1, c9_3, c11_2, c12_1, c18_1, c18_3, c18_8, c14_9.11, c15_13

Purpose

Ensure that the SM checks the value of P1 to be "00".

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the file to be updated has been performed.

Test

Send an UPDATE (SM) command with a parameter P1 ≠ "00"

Result

The expected status word is "6B XX".

RC_US_IV_02 subclause A.5.5.2, 8.3.2 c1_1, c9_1, c9_3, c11_2, c12_1, c14_9.12, c15_14, c18_1, c18_3, c18_8, c14_9.12, c15_14

Purpose

Ensure that the SM checks the value of $L_c \geq$ "04".

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the file to be updated has been performed.

Test

Send an UPDATE (SM) command with a L_c of less than 4 and a matching data field.

Result

The expected status word is "67 XX".

RC_US_IV_03 subclause A.5.5.2, 8.3.2 c1_1, c9_1, c9_3, c11_2, c12_1, c14_9.2, c15_1, c18_1, c18_3, c18_8, c15_1

Purpose

Ensure that the SM checks the AC of the file to update.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the file to be updated has been performed.
- The AC of the file for UPDATE is NEV.

Test

Send an UPDATE (SM) command with valid data.

Result

The expected status word is "98 04".

RC_US_IV_04 subclause A.5.5.2, 8.3.2 c1_1, c9_1, c9_3, c11_2, c12_1, c18_1, c18_3, c18_8, c14_9.4, c15_4

Purpose

Ensure that the SM returns "92 0X", if the internal retry routine has been used.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the file to be updated has been performed.
- The memory can be written, after using the internal retry routine X times.

Test

Send an UPDATE (SM) command with valid data.

Result

The expected status word is "92 0X".

RC_US_IV_05 subclause A.5.5.2, 8.3.2 c1_1, c9_1, c9_3, c11_2, c12_1, c18_1, c18_3, c18_8, c14_9.5, c15_5

Purpose

Ensure that the SM returns "92 40", if the memory can not be written.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the file to be updated has been performed.
- The memory can not be written.

Test

Send an UPDATE (SM) command with valid data.

Result

The expected status word is "92 40".

6.2.4.3.3 INCREASE (SM)

Table 52: Structure of INCREASE (SM)

Bytes	Description	M/O	Length
-X..0	Command Header		X + 1
1	INS byte of the previous DECREASE STAMPED sent to the UC (coded according to TS 101 200-3 [8])	M	1
2	P1 of the previous DECREASE STAMPED sent to the UC (coded according to TS 101 200-3 [8])	M	1
3	P2 of the previous DECREASE STAMPED sent to the UC (coded according to TS 101 200-3 [8])	M	1
4	Le of the previous DECREASE STAMPED sent to the UC (coded according to TS 101 200-3 [8])	M	1
5 .. (4 + Z)	The data field of the of the previous DECREASE STAMPED reponse sent by the UC (coded according to TS 101 200-3 [8])	M	Z
(5 + Z) ...	Command Trailer		

FU_IS_VA_01 subclause 8.3.3 c9_1, c9_3, c12_1, c11_3.6, c14_10.12, c15_15

Purpose
Ensure that the SM is able to verify a MAC from the UC and to increase the amount stored in the counter of the SM.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the counter to be increased has been performed.
- The contents should be known.

Test
Send an INCREASE (SM) command with valid data.
Send a READ RECORD command.

Result
The expected status word is "90 00". The read contents should be the one expected (original contents increased by the value decreased from the UC).

FU_IS_VA_02 subclause 8.3.3 c2_2, c9_1, c9_3, c12_1, c11_3.6, c14_10.13, c15_16

Purpose

Ensure that the SM is able to verify a MAC from the UC and to increase the amount stored in the counter of the SM.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the counter to be increased has been performed.
- The contents should be known.

Test

Send an INCREASE (SM) command with valid data.
Send a READ RECORD command.

Result

The expected status word is "9F XX". The read contents should be the one expected (original contents increased by the value decreased from the UC).

FU_IS_IV_01 subclause 8.3.3 c9_1, c9_3, c12_1, c11_3, c14_10.2, c15_1

Purpose

Ensure that the SM really verifies the MAC from the UC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the counter to be increased has been performed.

Test

Send an INCREASE (SM) command with valid data, but invalid MAC.

Result

The expected status word is "98 04".

FU_IS_IV_02 subclause 8.3.3 c9_1, c9_3, c12_1, c11_3.5, c14_10.2, c15_1

Purpose

Ensure that the SM does not increase the counter, if used with invalid data.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the counter to be increased has been performed.
- The contents should be known.

Test

Send an INCREASE (SM) command with valid data, but invalid MAC.
Send a READ RECORD command.

Result

The expected status word is "98 04" for INCREASE (SM). The read contents should be the original contents.

FU_IS_IV_03 subclause 8.3.3 c9_1, c9_3, c12_1, c11_3.1, c15_8

Purpose

Ensure that the SM checks the indicated key.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the counter to be increased has been performed.

Test

Send an INCREASE (SM) command with valid data, but invalid key.

Result

The expected status word is "94 04".

FU_IS_IV_04 subclause 8.3.3 c9_1, c9_3, c12_1, c11_3.5, c14_10.6, c15_9

Purpose

Ensure that the SM checks that a DECREASE STAMPED was used.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the counter to be increased has been performed.

Test

Send an INCREASE (SM) command with valid data, but invalid INS for the UC command.

Result

The expected status word is "94 08".

FU_IS_IV_05 subclause 8.3.3 c9_1, c12_1, c11_3.2, c14_10.3, c15_2

Purpose

Ensure that the SM requires a Random number to verify the MAC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has not been used.
- A SELECT on the counter to be increased has been performed.

Test

Send an INCREASE (SM) command with valid data.

Result

The expected status word is "98 35".

FU_IS_IV_06 subclause 8.3.3 c9_3, c12_1, c11_3.3

Purpose

Ensure that the SM checks that a keyset has been selected.

Preconditions

- A SELECT KEYSET has not been done.
- An ASK PARAMETER command has been used.
- A SELECT on the counter to be increased has been performed.

Test

Send an INCREASE (SM) command with valid data.

Result

The expected status word is "94 04".

FU_IS_IV_07 subclause 8.3.3 c9_1, c9_3, c12_1, c11_3.3.1, c14_10.6, c15_9

Purpose
Ensure that the SM checks that the keyset contains diversified keys.

Preconditions

– A SELECT KEYSET on a keyset containing master keys has been done.

– An ASK PARAMETER command has been used.

– A SELECT on the counter to be increased has been performed.

Test
Send an INCREASE (SM) command with valid data.

Result
The expected status word is "94 08".

FU_IS_IV_08 subclause 8.3.3 c9_1, c9_3, c11_3.4, c15_8

Purpose
Ensure that the SM checks that a counter to be increased is selected.

Preconditions

– A SELECT KEYSET on a keyset containing diversified keys has been done.

– An ASK PARAMETER command has been used.

– A SELECT on the counter to be increased has not been performed.

Test
Send an INCREASE (SM) command with valid data.

Result
The expected status word is "94 04".

Table 53: Coding of the INCREASE (SM) command

CLA	Class byte
INS	"8E"
P1	"00"
P2	Key number
L_c field	Length of data field
Data field	"34" (coded according to TS 101 200-3 [8]) Output mode (coded according to TS 101 200-3 [8]) "00" (coded according to TS 101 200-3 [8]) L_e of previous command (coded according to TS 101 200-3 [8]) data field of previous DECREASE STAMPED response (coded according to TS 101 200-3 [8])
L_e field	Empty

Table 54: Return codes for SELECT KEYSET

Return Code	Error description
98 04	- AC not fulfilled - Wrong cryptogram verification
98 35	- No ASK PARAMETER/GIVE RANDOM before
98 AD	- Command out of sequence
92 0X	- Update successful but after using internal retry routine X times
92 40	- Update impossible (memory problem)
94 00	- No EF selected
94 02	- Out of range (invalid address)
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	- P1 ≠ "00"
67 XX	- Lc < "04"
90 00	- Normal ending (ACK) of the command

RC_IS_IV_01 subclause A.5.6.1, 8.3.3 c1_1, c9_1, c9_3, c12_1, c11_3, c14_10.10, c15_13, c18_1, c18_3, c18_10

Purpose
Ensure that the SM checks the value of P1 to be "00".

Preconditions

– A SELECT KEYSET on a keyset containing diversified keys has been done.

– An ASK PARAMETER command has been used.

– A SELECT on the counter to be increased has been performed.

Test

Send an INCREASE (SM) command with a parameter P1 ≠ "00"

Result

The expected status word is "6B XX".

RC_IS_IV_02 subclause A.5.6.1, 8.3.3 c1_1, c9_1, c9_3, c12_1, c11_3, c14_10.11, c15_14, c18_1, c18_3, c18_10

Purpose

Ensure that the SM checks the value of $L_c \geq$ "04".

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the counter to be increased has been performed.

Test

Send an INCREASE (SM) command with a L_c of less than 4 and a matching data field.

Result

The expected status word is "67 XX".

RC_IS_IV_03 subclause A.5.6.1, 8.3.3 c1_1, c9_1, c9_3, c12_1, c11_3, c18_1, c18_3, c18_10, c15_4

Purpose

Ensure that the SM returns "92 0X", if the internal retry routine has been used.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the counter to be increased has been performed.
- The memory can be written, after using the internal retry routine X times.

Test

Send an INCREASE (SM) command with valid data.

Result

The expected status word is "92 0X".

RC_IS_IV_04 subclause A.5.6.1, 8.3.3 c1_1, c9_1, c9_3, c12_1, c11_3, c18_1, c18_3, c18_10, c15_5

Purpose
Ensure that the SM returns "92 40", if the memory can not be written.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.
- A SELECT on the counter to be increased has been performed.
- The memory can not be written.

Test
Send an INCREASE (SM) command with valid data.

Result
The expected status word is "92 40".

6.2.4.3.5 VERIFY CRYPTOGRAM

The command VERIFY CRYPTOGRAM corresponds to the UC command INTERNAL AUTHENTICATION.

FU_VC_VA_01 subclause 8.3.5 c9_1, c9_3, c11_4, c14_5.9, c15_15

Purpose
Ensure that the SM is able to verify a cryptogram from the UC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.

Test
Send an VERIFY CRYPTOGRAM command with valid data.

Result
The expected status word is "90 00".

FU_VC_IV_01 subclause 8.3.5 c9_1, c9_3, c11_4, c14_5.2, c15_1

Purpose
Ensure that the SM really verifies the cryptogram from the UC.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.

Test
Send an VERIFY CRYPTOGRAM command with valid data, but invalid cryptogram.

Result
The expected status word is "98 04".

FU_VC_IV_02 subclause 8.3.5 c9_1, c9_3, c11_4, c15_8

Purpose

Ensure that the SM checks the indicated key.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.

Test

Send an VERIFY CRYPTOGRAM command with valid data, but invalid key.

Result

The expected status word is "94 04".

FU_VC_IV_03 subclause 8.3.5 c9_1, c9_3, c11_4, c14_5.3, c15_2

Purpose

Ensure that the SM requires a Random number to verify the cryptogram.

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has not been used.

Test

Send an VERIFY CRYPTOGRAM command with valid data, but invalid key.

Result

The expected status word is "98 35".

FU_VC_IV_04 subclause 8.3.5 c9_1, c9_3, c11_4, c15_8

Purpose

Ensure that the SM checks that a keyset has been selected.

Preconditions

- A SELECT KEYSET has not been done.
- An ASK PARAMETER command has been used.

Test

Send an VERIFY CRYPTOGRAM command with valid data, but invalid key.

Result

The expected status word is "94 04".

FU_VC_IV_05 subclause 8.3.5 c9_1, c9_3, c11_4, c15_9

Purpose

Ensure that the SM checks that the keyset contains diversified keys.

Preconditions

- A SELECT KEYSET on a keyset containing master keys has been done.
- An ASK PARAMETER command has been used.

Test

Send an VERIFY CRYPTOGRAM command with valid data, but invalid key.

Result

The expected status word is "94 08".

Table 55: Coding of the VERIFY CRYPTOGRAM command

CLA	Class byte
INS	"8E"
P1	"00"
P2	Key number
L_c field	Length of data field
Data field	Cryptogram
L_e field	Empty

Table 56: Return codes for VERIFY CRYPTOGRAM

Return Code	Error description
98 04	- Wrong cryptogram verification
98 35	- No ASK PARAMETER/GIVE RANDOM before
98 AD	- Command out of sequence
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"
67 XX	- No test is foreseen for this status word
90 00	- Normal ending (ACK) of the command

RC_VC_IV_01 subclause A.5.5.3, 8.3.5 c1_1, c9_1, c9_3, c11_4, c14_5.7, c15_13, c18_1, c18_3, c18_9

Purpose

Ensure that the SM checks the value of P1 to be "00".

Preconditions

- A SELECT KEYSET on a keyset containing diversified keys has been done.
- An ASK PARAMETER command has been used.

Test

Send a VERIFY CRYPTOGRAM command with a parameter P1 ≠ "00"

Result

The expected status word is "6B XX".

6.2.6 Downloading of keys from SM to UC

DK_XX_VA_01 subclause A.7.1 c1_1, c9_1, c9_2, c10_1, c18_1, c18_2, c18_4, c15_15

Purpose

Ensure that the SM is able to download keys to an empty EF$_{KEY\_MAN}$ in UC.

Preconditions

- None.

Test

SELECT KEYSET on the EF$_{KEY\_MAN}$ on the next higher level.

DIVERSIFY KEYSET with destination EF$_{DIK1}$.

SELECT KEYSET on the EF$_{KEY\_MAN}$ containing the keys to download.

DIVERSIFY KEYSET with destination EF $_{DIK2}$.

COMPUTE LOAD KEY for each key to be downloaded.

Result

Each command shall execute successfully and the result at each COMPUTE LOAD KEY shall be correct.

DK_XX_VA_02 subclause A.7.2 c1_1, c9_1, c9_2, c10_1, c18_1, c18_2, c18_4, c15_15

Purpose

Ensure that the SM is able to exchange keys in the EF$_{KEY\_MAN}$ of the UC.

Preconditions

- None.

Test

SELECT KEYSET on the EF$_{KEY\_MAN}$ with version n.

DIVERSIFY KEYSET with destination EF$_{DIK1}$.

SELECT KEYSET on the EF$_{KEY\_MAN}$ with version (n + 1).

DIVERSIFY KEYSET with destination EF $_{DIK2}$.

COMPUTE LOAD KEY for each key to be downloaded.

Result

Each command shall execute successfully and the result at each COMPUTE LOAD KEY shall be correct.

K_XX_VA_03 subclause A.7.3 c1_1, c9_1, c9_2, c10_1, c18_1, c18_2, c18_4, c15_15

Purpose

Ensure that the SM is able to exchange keys in the EF_{KEY_OP} of the UC.

Preconditions

- None.

Test

SELECT KEYSET on the EF_{KEY_MAN}.

DIVERSIFY KEYSET with destination EF_{DIK1}.

SELECT KEYSET to the EF_{KEY_OP} with version (n + 1).

DIVERSIFY KEYSET with destination EF $_{DIK2}$.

COMPUTE LOAD KEY for each key to be downloaded.

Result

Each command shall execute successfully and the result at each COMPUTE LOAD KEY shall be correct.

History

Document history		
V1.1.1	July 1997	Publication

ISBN 2-7437-1485-9
Dépôt légal : Juillet 1997