INTERNATIONAL STANDARD

ISO/IEC 18013-4

First edition
2011-11-01

Information technology — Personal identification — ISO-compliant driving licence —

Part 4: Test methods

Technologies de l'information — Identification des personnes — Permis de conduire conforme à l'ISO —

Partie 4: Méthodes d'essai

Reference number
ISO/IEC 18013-4:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 18013-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

ISO/IEC 18013 consists of the following parts, under the general title *Information technology — Personal identification — ISO-compliant driving licence*:

— *Part 1: Physical characteristics and basic data set*

— *Part 2: Machine-readable technologies*

— *Part 3: Access control, authentication and integrity validation*

— *Part 4: Test methods*

Introduction

ISO/IEC 18013 establishes guidelines for the design format and data content of an ISO-compliant driving licence (IDL) with regard to human-readable features (ISO/IEC 18013-1), machine-readable technologies (ISO/IEC 18013-2), and access control, authentication and integrity validation (ISO/IEC 18013-3). It creates a common basis for international use and mutual recognition of the IDL without impeding individual countries/states to apply their privacy rules and national/community/regional motor vehicle authorities in taking care of their specific needs.

ISO/IEC 18013-1 defines the basic terms for ISO/IEC 18013, including physical characteristics, basic data element set, visual layout, and physical security features.

ISO/IEC 18013-2 specifies the technologies that may be used for ISO/IEC 18013, including the logical data structure and data mapping for each technology.

ISO/IEC 18013-3 specifies the electronic security features that may be incorporated under ISO/IEC 18013, including mechanisms for controlling access to data, verifying the origin of an IDL, and confirming data integrity.

This part of ISO/IEC 18013 prescribes requirements for testing the compliance of the machine-readable data content on an IDL and the mechanisms for controlling access to data recorded in the machine-readable technology on an IDL with the requirements of ISO/IEC 18013-2 and ISO/IEC 18013-3, respectively.

Information technology — Personal identification — ISO-compliant driving licence —

Part 4: Test methods

1 Scope

This part of ISO/IEC 18013 specifies the test methods used for conformity testing, that is methods for determining whether a driving licence can be considered to comply with the requirements of ISO/IEC 18013 for:

- machine-readable technologies (ISO/IEC 18013-2), and
- access control, authentication and integrity validation (ISO/IEC 18013-3).

The test methods specified in this part of ISO/IEC 18013 are based on specifications defined in ISO/IEC 18013-2 and ISO/IEC 18013-3 and underlying normative specifications.

This part of ISO/IEC 18013 deals with test methods specific to ISO-compliant driving licence (IDL) requirements. Test methods applicable to (smart) cards in general (e.g. those specified in the ISO/IEC 10373 series) are outside the scope of this part of ISO/IEC 18013.

Hence, this part of ISO/IEC 18013

- provides IDL implementers with requirements for conformity evaluation,
- provides IDL issuing authorities with requirements for quality assurance, and
- provides test laboratories and test tool providers with test suite requirements.

2 Conformance

Test case specifications described in this part of ISO/IEC 18013 are intended to be performed separately and independently. A given driving licence document is not required to pass through all the tests sequentially. Also, not all tests may be applicable to a given implementation.

An IDL is considered to conform to the applicable requirements of ISO/IEC 18013-2 and ISO/IEC 18013-3 if it passes all associated tests in this part of ISO/IEC 18013. However, passing all applicable tests in this part of ISO/IEC 18013 does not guarantee that no failures will occur under operational conditions.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 3166-1:2006, *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*

ISO/IEC 7816-4:2005, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 18013-2:2008, *Information technology — Personal identification — ISO-compliant driving licence — Part 2: Machine-readable technologies*

ISO/IEC 18013-3:2009, *Information technology — Personal identification — ISO-compliant driving licence — Part 3: Access control, authentication and integrity validation*

ISO/IEC 19785-1:2006, *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*

ISO/IEC 19785-3:2007, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 18013-2, ISO/IEC 18013-3 and the following apply.

4.1
test case
description of test purpose, unique test case identifier, test inputs, test execution conditions, test steps, and the results required to pass the test

4.2
test case specification
collection of test cases, and general test data applicable to the test cases

5 Abbreviated terms

AA	active authentication
AKID	authority key identifier
AID	application identifier
APDU	application protocol data unit
BAP	basic access protection
CA	chip authentication
CE	compact encoding
DF	dedicated file
DG	data group
DO	data object

EAP	extended access protection
EF	elementary file
EF ID	elementary file identifier
ICS	implementation conformance statement
IUT	implementation under test
LDS	logical data structure
NMA	non-match alert
OID	object identifier
PA	passive authentication
PKI	public-key infrastructure
RF	radio frequency
SAI	scanning area identifier
SE	standard encoding
SIC	secure integrated circuit
SKID	subject key identifier
SMI	security mechanism indicator
SOD	document security object
TA	terminal authentication

6 Test design

6.1 General

This clause generally follows the concepts of the OSI Conformance Testing Methodology and Framework as specified in the seven parts of ISO/IEC 9646. Several basic elements referred to in or by the individual test case specifications are explained.

NOTE These elements facilitate the synchronization of additional specifications written by different organizations with this part of ISO/IEC 18013.

6.2 Test hierarchy

6.2.1 Structure

Test concepts used to describe the test design consist of the following elements:

- Implementation under test (IUT)
- Test Layer
- Test Unit
- Test Case

These elements have a hierarchical relationship as shown in Figure 1.

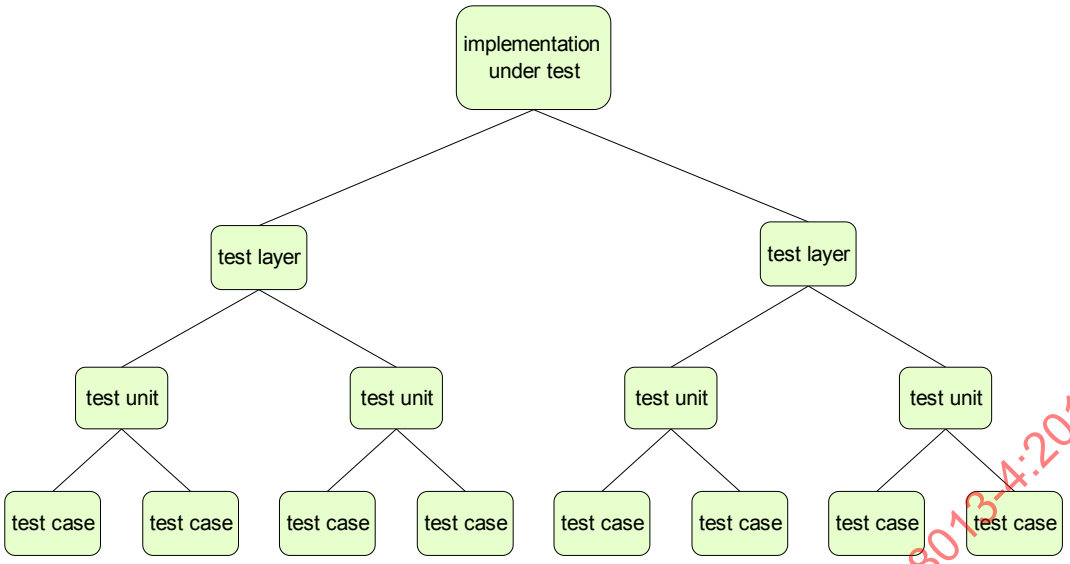

Figure 1 — Test element hierarchy

6.2.2 Implementation under test

6.2.2.1 Overview

Three IUTs are defined:

- IDL with standard encoding for SIC (see Annex C of ISO/IEC 18013-2:2008)
- IDL with compact encoding (see Annex B of ISO/IEC 18013-2:2008)
- IDL with standard encoding on Optical Memory (see Annex D of ISO/IEC 18013-2:2008)

6.2.2.2 Profile

Profiles are defined for identifying optional functionality in the IUT, which impacts the applicability of certain test layers, test units or test cases.

Profiles determine whether certain tests are applicable in the Test Layer, Test Unit or Test Case definitions. This enables the tester or test software to (automatically) select which tests should be executed to the IUT. Such selection is based upon the ICS filled out by the applicant or tester (also see 6.3.1).

The Profile specification shall include:

- Profile-ID
- Profile description

6.2.3 Test layer

6.2.3.1 Overview

The following two of the seven layers in the OSI Basic Reference Model as defined in ISO/IEC 7498-1 are addressed in this part of ISO/IEC 18013:

- Layer 7 refers to the Application Layer, and
- Layer 6 refers to the Presentation Layer.

The other layers are not applicable.

Each test layer comprises a number of test units.

6.2.3.2 Layer 7 – Logical data structure tests

Layer 7 tests cover LDS requirements. LDS requirements include:

- Presence and availability of DGs
- Presence and formatting of fields in each DG
- Access to DGs (security mechanisms)

6.2.3.3 Layer 6 – Command tests

Layer 6 tests are applicable only to IDL implementations on SIC. Layer 6 on a SIC consists of Commands. Commands for an IDL are specified in ISO/IEC 18013-2 and ISO/IEC 18013-3 and are applicable to the following IUTs:

- Compact encoding
- Standard encoding.

6.2.4 Test unit

A test unit covers an individual topic inside a layer. Each test unit contains test cases that are related to the same type of functionality of the IUT. A test unit groups together test cases that address a common issue.

Each test unit is defined by the following information:

Test Unit-ID	Uniquely identifies the test unit inside the test layer.
Purpose	Specifies the common issue addressed by test cases contained in this test unit.
References	Optionally identifies references applicable to all test cases in the test unit.

6.2.5 Test case

Each test case is defined by the following information:

Test Case-ID	Uniquely identifies the test case within the test unit.
Purpose	Specifies the requirement addressed in this test case.
Version	Version number of this test case.
References	Identifies specific reference to the requirement addressed by this test case.
Profile	Defines the profiles for which the test case is applicable. If no profile is defined (empty field), the test applies to all configurations. If the IUT does not match with each of the defined profiles, the test is skipped, and marked "not applicable" in the test report.

Preconditions	Define the state in which the IUT needs to be before the test case can be executed, including test cases that shall have been successfully passed, if any. If these preconditions are not fulfilled, the test is skipped and marked as such in the test report.
Test scenario	Defines the test steps that shall be taken. Each step covers a simple, exactly defined operation with a measurable result that can be included in the test report. The steps shall be performed in the order listed. Each test step is defined by the following information: • Test Step-ID – a consecutive number, uniquely identifying each test step and the execution order in the test case. • Description – defining the operation that has to be executed for this step. • Configuration Data – optionally specifying input data required to perform this test step.
Expected result	The expected result defines pass criteria for each test step in the test scenario. The analysis of the observed result in comparison with the expected result leads to a "Pass" or a "Fail". The results of the individual test steps and the overall result of the test case are transferred to the overall test report.

6.3 Test administration

6.3.1 Preconditions for testing

IUT. The tests in this part require a fully personalized IDL. This means that all mandatory data groups shall be present as a minimum. In addition, the IUT shall be personalised with all data required to test the optional features declared in the ICS.

Test environment. Test execution takes place in indoor conditions and provides normal temperature. All test equipment must be established properly.

Test apparatus. All equipment described in the annexes pertinent to the machine readable techonogy supported by the IUT must be available.

6.3.2 Implementation conformance statement

For each IUT described, the applicant for conformity testing shall complete the ICS which is attached to the Test Case Specification applicable to that specific IUT.

A completed ICS provides information about the Profile of the IUT (also see 6.2.2.2). Based on the completed ICS, all tests that apply to this Profile (as indicated in the Profile element in each test case; see 6.2.5) can be selected for test execution.

6.3.3 Test report

Detailed test results and ICS information shall be recorded for reference in a test report. The test report contains the test result of each

- test layer
- test unit

- test case
- test step

If a test is not applicable, this is noted.

If a test is applicable and the preconditions are fulfilled, the test result for a test step/ case/ unit/ layer can be:

- Pass – if all actually obtained results from the IUT match the expected results declared for each test step/ case/ unit/ layer AND if all post conditions are fulfilled.
- Fail – if one or more of the actually obtained results from the IUT do NOT match the expected results declared for each test step/ case/ unit/ layer OR if one or more of the post conditions are NOT fulfilled. Optionally, additional information regarding the failure can be provided.

A fail in one of the test steps leads to a fail of the entire test case; a failed test case leads to a failed test unit; etc.

The ICS and detailed test results shall be logged and retrievable. Optionally, the test execution details, including detailed observed results for each test case may be included in the test report.

7 IDL Conformity test methods

7.1 Overview

Conformity testing of IDL implementations to ISO/IEC 18013-2 and ISO/IEC 18013-3 is organised through the identification of a number of test cases.

Test requirements for Commands and LDS tests conformity are defined in individual annexes. These annexes are attached to this part of ISO/IEC 18013.

7.2 Profiles

Profiles are defined to identify whether certain optional functionality is supported by the IUT. Support of these optional functions and features depend on several factors:

- Machine Readable Technologies supported
- Access control, authentication and integrity validation mechanisms supported
- Optional Data Groups supported
- Optional Data Elements supported within Data Groups

Profiles for each IUT are defined in each annex.

7.3 IDL test case specifications

7.3.1 Scope

IDL test case specifications are attached in the annexes.

Test methods for driving licence interface devices are currently not included in this part of ISO/IEC 18013.

7.3.2 Standard encoding on SIC

Test case specifications for SE on SIC cover:

- LDS tests for SE on SIC
- Chip Application Protocol tests (applicable to SE on SIC)

7.3.3 Compact encoding

Test case specifications for CE cover:

- LDS tests for CE (applicable to all machine readable technologies)
- Chip Application Protocol tests (applicable to CE on SIC)

7.3.4 Standard encoding on optical memory

Test case specifications for SE on Optical Memory cover:

- LDS tests for SE on Optical Memory

7.4 Conformance

An IUT is in conformance with the requirements of a particular layer if the IUT passes all applicable tests. All tests in a layer should be performed on the same IUT.

Annex A
(normative)

Test case specification: LDS in SE on SIC

A.1 Introduction

This annex specifies the test cases for the LDS in SE on SIC.

A.2 General test requirements

A.2.1 Preconditions for testing

The tests in this annex require a fully personalized IDL. This means that all mandatory data groups shall be present. This annex tests all mandatory and optional data groups.

All tests are mandatory unless marked as optional or conditional.

A.2.2 Test setup

For setting up these tests, any reader for communicating with SIC compliant with ISO/IEC 7816 or ISO/IEC 14443 can be used. The reader shall support extended length APDUs and command chaining.

If EAP is supported, a terminal authentication certificate chain and an IS private key are required as input for testing.

A.2.3 Implementation conformance statement

In order to set up the tests properly, Tables A.1 and A.2 shall be completed.

The ISO/IEC 18013-2 specification defines several optional elements that an IDL can support. This includes security mechanisms like BAP, EAP and AA as well as additional data groups (DG2 to DG14).

Since these elements are optional, it is not possible to define the corresponding tests as mandatory for each IDL. Therefore, this part of ISO/IEC 18013 specifies a set of profiles. Each profile covers a specific optional element. A tested IDL shall be assigned to the supported profiles in the ICS, and a test shall only be performed if the IDL supports this profile.

NOTE No profile ID's are explicitly defined for DG12 to DG14 because the EAP, AA and NMA profiles cover these data groups implicitly.

Table A.1 — Implementation conformance statement

Profile	Information for test setup	Applicable (YES or NO)	Protection level (Plain, BAP or EAP)
SMI	Security Mechanism Indicator		
DG2	IDL contains elementary file with LDS Data Group 2		
DG3	IDL contains elementary file with LDS Data Group 3		
DG4	IDL contains elementary file with LDS Data Group 4		
DG5	IDL contains elementary file with LDS Data Group 5		
DG6	IDL contains elementary file with LDS Data Group 6		
DG7	IDL contains elementary file with LDS Data Group 7		
DG8	IDL contains elementary file with LDS Data Group 8		
DG9	IDL contains elementary file with LDS Data Group 9		
DG11	IDL contains elementary file with LDS Data Group 11		
PA	Passive Authentication		
AA	Active Authentication		
AA-ECDSA	AA ECDSA algorithm		
AA-RSA	AA RSA algorithm		
NMA	Non-Match Alert		
EAP	Extended Access Protection		
CA-DH	CA Diffie-Hellman		
CA-ECDH	CA Elliptic Curve Diffie-Hellman		

Table A.2 — Configuration information

Supported Profile	Configuration information
PA	Provide the country signing certificate name:
BAP	Provide the reference string provided with the samples:
EAP	Provide the name of the certificates and IS private key
DG11	Provide the template tag.

A.3 Test Layer SE_LDS – Logical Data Structure Tests

A.3.1 Test Unit SE_LDS_COM – Tests for EF.Com

Test Unit-ID	SE_LDS_COM (Standard Encoding – Common Data Elements)
Purpose	The test cases in this test unit verify the structure and content of EF.COM in the LDS of the IDL.
References	ISO/IEC 18013-2:2008 ISO/IEC 18013-3:2009

A.3.1.1 Test Case SE_LDS_COM_001

Test Case-ID	SE_LDS_COM_001
Purpose	This test checks the template tag that the encoded EF.COM element starts with.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.COM has been retrieved from the IDL
Test Scenario	1. Check the very first byte of the EF.Com element
Expected Results	1. First byte shall be '60'

A.3.1.2 Test Case SE_LDS_COM_002

Test Case-ID	SE_LDS_COM_002
Purpose	This test checks the encoding of EF.COM element length.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.COM has been retrieved from the IDL.
Test Scenario	1. Analyze the encoding of the bytes that follow the template tag. 2. Verify the length of the EF.COM object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.COM object.

A.3.1.3 Test Case SE_LDS_COM_003

Test Case-ID	SE_LDS_COM_003
Purpose	This test checks the LDS version referred by the EF.COM element.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.COM has been retrieved from the IDL.
Test Scenario	1. Search for the LDS version (Tag '5F 01') inside EF.COM. 2. Verify the encoded length of the object with tag '5F01'. 3. Verify the LDS version.
Expected Results	1. Tag '5F 01' shall be present. 2. The encoded length shall be 02. 3. The specified LDS version shall be '01XX'h (BCD encoded).

A.3.1.4 Test Case SE_LDS_COM_004

Test Case-ID	SE_LDS_COM_004
Purpose	This test checks the Data Group Tag List referred by the EF.COM element.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 18013-3:2009, Clause 10
Profile	
Preconditions	1. EF.COM has been retrieved from the IDL
Test Scenario	1. Search for the Tag List (Tag '5C') inside EF.COM. 2. Verify the length of the object with tag '5C'. 3. Verify if mandatory data groups are present in the Data Group Tag List. 4. Verify the validity of the data group tags present in the Data Group Tag List.
Expected Results	1. Tag '5C' shall be present. 2. The bytes that follow the tag shall contain a valid length encoding. 3. The Data Group Tag List shall at least contain the tags for the mandatory data groups '61'. 4. The list shall contain only valid data group tags as specified in [1] and [2], i.e. '61', '6B', '6C', '65', '67', '75', '63', '76', '70', '71', '6F', and '6E'.

A.3.1.5 Test Case SE_LDS_COM_005

Test Case-ID	SE_LDS_COM_005
Purpose	This test checks the consistency of the Data Group Tag List with the actual data groups present.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 18013-3:2009, Clause 10
Profile	
Preconditions	1. EF.COM has been retrieved from the IDL.
Test Scenario	1. Check that all Data groups that are indicated by the tag list in EF.COM are present.
Expected Results	1. All Data groups that are indicated by the tag list in EF.COM shall be present.

A.3.1.6 Test Case SE_LDS_COM_006

Test Case-ID	SE_LDS_COM_006
Purpose	This test checks the consistency of the actual data groups present with the Data Group Tag List.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 18013-3:2009, Clause 10
Profile	
Preconditions	1. EF.COM has been retrieved from the IDL.
Test Scenario	1. Check that all Data groups that are NOT indicated by the tag list in EF.COM are absent.
Expected Results	1. All Data groups that are NOT indicated by the tag list in EF.COM shall be absent.

A.3.1.7 Test Case SE_LDS_COM_007

Test Case-ID	SE_LDS_COM_007
Purpose	This test checks the encoding of SMI (Tag '86') element length.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 18013-3:2009, Clause 10
Profile	SMI
Preconditions	1. EF.COM has been retrieved from the IDL.
Test Scenario	1. Search for the SMI (Tag '86') inside EF.COM. 2. Analyze the encoding of the bytes that follow the template tag. 3. Verify the encoded length of the Tag '86'.
Expected Results	1. Tag '86' shall be present. 2. The bytes that follow the Tag '86' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the given Tag '86'.

A.3.1.8 Test Case SE_LDS_COM_008

Test Case-ID	SE_LDS_COM_008
Purpose	This test checks the encoding of SMI (Tag '86').
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 18013-3:2009, Clause 9
Profile	SMI
Preconditions	1. EF.COM has been retrieved from the IDL. 2. The SMI has been retrieved from EF.COM.
Test Scenario	1. Check the DER-TLV encoding of the SMI. 2. Check the content of the object with Tag '86'.
Expected Results	1. The SMI shall be encoded in a valid DER structure (according to ASN.1 encoding rules). 2. For each security mechanism indicated in the SMI, the data groups indicated shall exist in the IDL.

A.3.1.9 Test Case SE_LDS_COM_009

Test Case-ID	SE_LDS_COM_009
Purpose	This test checks the encoding of the AA Security Mechanism in the SMI.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 18013-3:2009, Clause 8
Profile	SMI
Preconditions	1. EF.COM has been retrieved from the IDL. 2. The SMI has been retrieved from EF.COM. 3. The SMI has a valid DER TLV structure.
Test Scenario	Perform the following checks for the security mechanism in the SMI that specifies the AA security mechanism (if present): 1. Check the encoding of the parameters for the mechanism id-sm-AA. 2. Check the version of the AA parameters. 3. Check the publicKeyDG of the AA parameters. 4. Check the consistency of publicKeyDG and the Taglist in EF.COM.
Expected Results	1. The parameters for the mechanism id-sm-AA shall be encoded as specified in ISO/IEC 18013-3:2009, 8.2.4.4. 2. The version shall be '00' (V1). 3. The publicKeyDG shall be 13 (hex '0D'). 4. The data group indicated by publicKeyDG shall occur in the Taglist.

A.3.1.10 Test Case SE_LDS_COM_010

Test Case-ID	SE_LDS_COM_010
Purpose	This test checks the encoding of the NMA mechanism in the SMI.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 18013-3:2009, Clause 8
Profile	SMI
Preconditions	1. EF.COM has been retrieved from the IDL. 2. The SMI has been retrieved from EF.COM. 3. The SMI has a valid DER TLV structure.
Test Scenario	Perform the following checks for the security mechanism in the SMI that specifies the NMA mechanism (if present): 1. Check the encoding of the parameters for the mechanism id-sm-NMA. 2. Check the version of the NMA parameters. 3. Check the SAI_inputmethod of the NMA parameters. 4. Check the presence of the Tag for DG12 in the Taglist in EF.COM.
Expected Results	1. The parameters for the mechanism id-sm-NMA shall be encoded as specified in ISO/IEC 18013-3:2009, 8.4.4.3. 2. The version shall be '00' (V1). 3. The SAI_inputmethod field shall be set to the corresponding value in DG12. If the SAI_inputmethod field is not present in DG12, the field shall also not be included in EF.COM. 4. The tag '71' (DG12 tag) shall occur in the Taglist.

A.3.1.11 Test Case SE_LDS_COM_011

Test Case-ID	SE_LDS_COM_011
Purpose	This test checks the encoding of the EAP mechanism in the SMI.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 18013-3:2009
Profile	SMI
Preconditions	1. EF.COM has been retrieved from the IDL. 2. The SMI has been retrieved from EF.COM. 3. The SMI has a valid DER TLV structure.
Test Scenario	Perform the following checks for the security mechanism in the SMI that specifies the EAP mechanism: 1. Check the presence of the mechanism id-sm-EAP. 2. Check the encoding of the parameters for the mechanism id-sm-EAP. 3. Check the version of the EAP parameters. 4. Check the chipAuthPublicKeyDG field of the EAP parameters. 5. Check the consistency of chipAuthPublicKeyDG and the Taglist in EF.COM. 6. Check the smConfiguration field of the EAP parameters. 7. Check the currentTrustRoot field of the EAP parameters. 8. Check the alternateTrustRoot field of the EAP parameters.
Expected Results	1. The mechanism id-sm-EAP shall be present. 2. The parameters for the mechanism id-sm-EAP shall be encoded as specified in ISO/IEC 18013-3:2009, C.6. 3. The version shall be '00' (V1). 4. The chipAuthPublicKeyDG field shall be set to '0E' (DG14). 5. The data group indicated by chipAuthPublicKeyDG shall occur in the Taglist. 6. The smConfiguration field shall use one of the identifiers from ISO/IEC 18013-3:2009, B.8 (i.e. oid_bap_config_1, oid_bap_config_2, oid_bap_config_3, or oid_bap_config_4). 7. The currentTrustRoot field shall be set to the current trust root's SKID, formatted as in the corresponding card-verifiable certificate, including the preceding length byte. The currentTrustRoot field shall be 17 bytes length. If the resulting octet string is shorter than 17 bytes, it shall be padded to the right with '00' bytes. 8. The alternateTrustRoot field shall be set to the alternate trust root's SKID, formatted as in the corresponding card-verifiable certificate, including the preceding length byte. The alternateTrustRoot field shall be 17 bytes length. If the resulting octet string is shorter than 17 bytes, it shall be padded to the right with '00' bytes.

A.3.1.12 Test Case SE_LDS_COM_012

Test Case-ID	SE_LDS_COM_012
Purpose	This test checks the presence of the EAP mechanism in the SMI.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 18013-3:2009
Profile	SMI EAP NOT supported
Preconditions	1. EF.COM has been retrieved from the IDL. 2. The SMI has been retrieved from EF.COM. 3. The SMI has a valid DER TLV structure.
Test Scenario	1. Check the presence of the mechanism id-sm-EAP if EAP is NOT supported.
Expected Results	1. The mechanism id-sm-EAP shall be absent.

A.3.2 Test Unit SE_LDS_DG1 – Tests for EF.DG1

Test Unit-ID	SE_LDS_DG1 (Standard Encoding – Data Group 1)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Data Group 1.
References	ISO/IEC 18013-2:2008 ISO/IEC 8859-1:1998 ISO 3166-1:2006

A.3.2.1 Test Case SE_LDS_DG1_001

Test Case-ID	SE_LDS_DG1_001
Purpose	This test checks the template tag that the encoded EF.DG1 element starts with.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL.
Test Scenario	1. Check the very first byte of the EF.DG1 element.
Expected Results	1. First byte shall be '61'.

A.3.2.2 Test Case SE_LDS_DG1_002

Test Case-ID	SE_LDS_DG1_002
Purpose	This test checks the encoding of EF.DG1 element length.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL.
Test Scenario	1. Analyze the encoding of the bytes that follow the template tag. 2. Verify the length of the EF.DG1 object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.DG1 object.

A.3.2.3 Test Case SE_LDS_DG1_003

Test Case-ID	SE_LDS_DG1_003
Purpose	This test checks the encoding of Mandatory Demographic Data (Tag '5F1F') in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL.
Test Scenario	1. Search for the Mandatory Demographic Data (Tag '5F 1F') inside EF.DG1. 2. Analyze the encoding of the bytes that follow the template tag. 3. Verify the length of the DO with Tag '5F1F'.
Expected Results	1. Tag '5F 1F' shall be present. 2. The bytes that follow the Tag '5F1F' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the DO with the Tag '5F1F'.

A.3.2.4 Test Case SE_LDS_DG1_004

Test Case-ID	SE_LDS_DG1_004
Purpose	This test checks the encoding of the Family Name referred by the Mandatory Demographic Data (Tag '5F1F) in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL.
Test Scenario	1. Check the Family Name field length. 2. Check the Family Name format.
Expected Results	1. The first byte of the Mandatory Data Elements object shall have a value in the range '00'h .. '24'h. 2. Family Name shall not contain numeric characters.

A.3.2.5 Test Case SE_LDS_DG1_005

Test Case-ID	SE_LDS_DG1_005
Purpose	This test checks the encoding of the Given Name referred by the Mandatory Demographic Data (Tag '5F1F) in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Mandatory Data Elements object has been retrieved from EF.DG1. 3. The Family Name has been retrieved from the Mandatory Data Elements object.
Test Scenario	1. Check the Given Name field length. 2. Check the Given Name format.
Expected Results	1. The first byte following the Family Name field in the Mandatory Data Elements object shall have a value in the range '00'h .. '24'h. 2. Given Name shall not contain numeric characters.

A.3.2.6 Test Case SE_LDS_DG1_006

Test Case-ID	SE_LDS_DG1_006
Purpose	This test checks the encoding of the Date of Birth referred by the Mandatory Demographic Data (Tag '5F1F) in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Mandatory Data Elements object has been retrieved from EF.DG1. 3. The Family Name has been retrieved from the Mandatory Data Elements object. 4. The Given Name has been retrieved from the Mandatory Data Elements object.
Test Scenario	1. Check the Date of Birth field length. 2. Check the Date Of Birth encoding. 3. Check that the Date of Birth element contains a valid date.
Expected Results	1. The Date Of Birth field shall be encoded on the 4 bytes following the Given Name field in the Mandatory Data Elements object. 2. Date of Birth shall be encoded in YYYYMMDD BCD format. 3. The Date of Birth shall be reasonable. It shall specify an existing day. 4. The Date of Birth shall be reasonable. It should be in the past.

A.3.2.7 Test Case SE_LDS_DG1_007

Test Case-ID	SE_LDS_DG1_007
Purpose	This test checks the encoding of the Date of Issue referred by the Mandatory Demographic Data (Tag '5F1F) in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Mandatory Data Elements object has been retrieved from EF.DG1. 3. The Family Name has been retrieved from the Mandatory Data Elements object. 4. The Given Name has been retrieved from the Mandatory Data Elements object. 5. The Date of Birth has been retrieved from the Mandatory Data Elements object.
Test Scenario	1. Check the Date of Issue field length. 2. Check the Date Of Issue encoding. 3. Check that the Date of Issue element contains a valid date.
Expected Results	1. The Date Of Issue field shall be encoded on the 4 bytes following the Date of Birth field in the Mandatory Data Elements object. 2. Date of Issue shall be encoded in YYYYMMDD BCD format. 3. The Date of Issue shall be reasonable. It shall specify an existing day. 4. The Date of Issue shall be reasonable. It should be the current date or in the past.

A.3.2.8 Test Case SE_LDS_DG1_008

Test Case-ID	SE_LDS_DG1_008
Purpose	This test checks the encoding of the Date of Expiry referred by the Mandatory Demographic Data (Tag '5F1F) in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL 2. The Mandatory Data Elements object has been retrieved from EF.DG1. 3. The Family Name has been retrieved from the Mandatory Data Elements object. 4. The Given Name has been retrieved from the Mandatory Data Elements object. 5. The Date of Birth has been retrieved from the Mandatory Data Elements object. 6. The Date of Issue has been retrieved from the Mandatory Data Elements object.
Test Scenario	1. Check the Date of Expiry field length. 2. Check the Date Of Expiry encoding. 3. Check that the Date of Expiry element contains a valid date.
Expected Results	1. The Date Of Expiry field shall be encoded on the 4 bytes following the Date of Issue field in the Mandatory Data Elements object. 2. Date of Expiry shall be encoded in YYYYMMDD BCD format. 3. The Date of Expiry shall be reasonable. It shall specify an existing day. 4. The Date of Expiry shall be reasonable. It shall specify a date after the Date of Issue.

A.3.2.9 Test Case SE_LDS_DG1_009

Test Case-ID	SE_LDS_DG1_009
Purpose	This test checks the encoding of the Issuing Country referred by the Mandatory Demographic Data (Tag '5F1F) in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO 3166-1:2006
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Mandatory Data Elements object has been retrieved from EF.DG1. 3. The Family Name has been retrieved from the Mandatory Data Elements object. 4. The Given Name has been retrieved from the Mandatory Data Elements object. 5. The Date of Birth has been retrieved from the Mandatory Data Elements object. 6. The Date of Issue has been retrieved from the Mandatory Data Elements object. 7. The Date of Expiry has been retrieved from the Mandatory Data Elements object.
Test Scenario	1. Check the Issuing Country field length. 2. Check the Issuing Country encoding. 3. Check that the Issuing Country element is valid.
Expected Results	1. The Issuing Country field shall be encoded on the 3 bytes following the Date of Expiry field in the Mandatory Data Elements object. 2. Issuing Country shall be encoded in Alpha characters only. 3. The Issuing Country shall be a valid value as defined in ISO 3166-1.

A.3.2.10 Test Case SE_LDS_DG1_010

Test Case-ID	SE_LDS_DG1_010
Purpose	This test checks the encoding of the Issuing Authority referred by the Mandatory Demographic Data (Tag '5F1F) in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 8859-1:1998
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Mandatory Data Elements object has been retrieved from EF.DG1. 3. The Family Name has been retrieved from the Mandatory Data Elements object. 4. The Given Name has been retrieved from the Mandatory Data Elements object. 5. The Date of Birth has been retrieved from the Mandatory Data Elements object. 6. The Date of Issue has been retrieved from the Mandatory Data Elements object. 7. The Date of Expiry has been retrieved from the Mandatory Data Elements object. 8. The Issuing Country has been retrieved from the Mandatory Data Elements object.
Test Scenario	1. Check the Issuing Authority field length. 2. Check the Issuing Authority format.
Expected Results	1. The first byte following the Issuing Country field in the Mandatory Data Elements object shall have a value in the range '00'h .. '41'h. 2. Issuing Authority shall be coded according to ISO/IEC 8859-1.

A.3.2.11 Test Case SE_LDS_DG1_011

Test Case-ID	SE_LDS_DG1_011
Purpose	This test checks the encoding of the Licence Number referred by the Mandatory Demographic Data (Tag '5F1F) in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Mandatory Data Elements object has been retrieved from EF.DG1. 3. The Family Name has been retrieved from the Mandatory Data Elements object. 4. The Given Name has been retrieved from the Mandatory Data Elements object. 5. The Date of Birth has been retrieved from the Mandatory Data Elements object. 6. The Date of Issue has been retrieved from the Mandatory Data Elements object. 7. The Date of Expiry has been retrieved from the Mandatory Data Elements object. 8. The Issuing Country has been retrieved from the Mandatory Data Elements object. 9. The Issuing Authority has been retrieved from the Mandatory Data Elements object.
Test Scenario	1. Check the Licence Number field length. 2. Check the Licence Number format.
Expected Results	1. The first byte following the Issuing Authority field in the Mandatory Data Elements object shall have a value in the range '00'h .. '19'h. 2. Licence Number shall be coded on Alpha and Numeric characters only.

A.3.2.12 Test Case SE_LDS_DG1_012

Test Case-ID	SE_LDS_DG1_012
Purpose	This test checks the encoding of Categories of Vehicles/Restrictions/Conditions (Tag '7F63') in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL
Test Scenario	1. Search for the Categories of Vehicles/Restrictions/Conditions (Tag '7F 63') inside EF.DG1. 2. Analyze the encoding of the bytes that follow the template tag. 3. Verify the length of the DO with Tag '7F 63'.
Expected Results	1. Tag '7F 63' shall be present. 2. The bytes that follow the Tag '7F63' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the DO with the Tag '7F63'.

A.3.2.13 Test Case SE_LDS_DG1_013

Test Case-ID	SE_LDS_DG1_013
Purpose	This test checks the "Number of Entries" DO in the "Categories of Vehicles/Restrictions/Conditions" DO (Tag '7F63') in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, A.4 ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Categories of Vehicles/Restrictions/Conditions object has been retrieved from EF.DG1.
Test Scenario	1. Search for the Number of Entries (Tag '02') inside Categories of Vehicles/Restrictions/Conditions object. 2. Analyze the encoding of the length of the Number of Entries DO coded with tag '02'. 3. Check the value encoded in the Number of Entries DO.
Expected Results	1. Tag '02' shall be present. 2. The length encoded in the Number of Entries DO shall be '01'h. 3. The Number of Entries (01) shall match the number of occurrences of tag '87' in the Categories of Vehicles/Restrictions/Conditions object.

A.3.2.14 Test Case SE_LDS_DG1_014

Test Case-ID	SE_LDS_DG1_014
Purpose	This test checks the length of each "Category of Vehicle/Restriction/Condition" entry in the "Categories of Vehicles/Restrictions/Conditions" DO (Tag '7F63') in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, A.4 ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Categories of Vehicles/Restrictions/Conditions object has been retrieved from EF.DG1.
Test Scenario	Perform the following checks for each of the "Category of Vehicle/Restriction/Condition" entries : 1. Analyze the encoding of the bytes that follow the tag '87'. 2. Verify the length of the DO with Tag '87'. 3. Check the number of sub fields in the value of the DO with Tag '87'.
Expected Results	1. The bytes that follow the Tag '87' shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the DO with the Tag '87'. 3. The value of the DO with Tag '87' contains 6 sub-fields, separated by a sub-field delimiters ";"

A.3.2.15 Test Case SE_LDS_DG1_015

Test Case-ID	SE_LDS_DG1_015
Purpose	This test checks the Vehicle Category Code of each "Category of Vehicle/Restriction/Condition" entry in the "Categories of Vehicles/Restrictions/Conditions" DO (Tag '7F63') in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, A.4 ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Categories of Vehicles/Restrictions/Conditions object has been retrieved from EF.DG1.
Test Scenario	Perform the following checks for each of the "Category of Vehicle/Restriction/Condition" entries: 1. Check the length of the Vehicle Category Code (sub-field #1). 2. Check the format of the Vehicle Category Code (sub-field #1).
Expected Results	1. The Vehicle Category Code has a length of 1 or 2 or 3 bytes. 2. The Vehicle Category Code contains Alpha-Numeric characters only.

A.3.2.16 Test Case SE_LDS_DG1_016

Test Case-ID	SE_LDS_DG1_016
Purpose	This test checks the Date of Issue (if present) of each "Category of Vehicle/Restriction/Condition" entry in the "Categories of Vehicles/Restrictions/Conditions" DO (Tag '7F63') in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, A.4 ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Categories of Vehicles/Restrictions/Conditions object has been retrieved from EF.DG1.
Test Scenario	Perform the following checks for each of the "Category of Vehicle/Restriction/Condition" entries: 1. Check the length of the Date of Issue (sub-field #2). 2. Check the format of the Date of Issue. 3. Check that the Date of Issue field contains a valid date.
Expected Results	1. The Date of Issue has a length of 4 bytes. 2. Date of Issue shall be encoded in YYYYMMDD BCD format. 3. The Date of Issue shall be reasonable. It shall specify an existing date.

A.3.2.17 Test Case SE_LDS_DG1_017

Test Case-ID	SE_LDS_DG1_017
Purpose	This test checks the Date of Expiry (if present) of each "Category of Vehicle/Restriction/Condition" entry in the "Categories of Vehicles/Restrictions/Conditions" DO (Tag '7F63') in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, A.4 ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Categories of Vehicles/Restrictions/Conditions object has been retrieved from EF.DG1.
Test Scenario	Perform the following checks for each of the "Category of Vehicle/Restriction/Condition" entries: 1. Check the length of the Date of Expiry (sub-field #3). 2. Check the format of the Date of Expiry. 3. Check that the Date of Expiry field contains a valid date.
Expected Results	1. The Date of Expiry has a length of 4 bytes. 2. Date of Expiry shall be encoded in YYYYMMDD BCD format. 3. The Date of Expiry shall be reasonable. It shall specify an existing date.

A.3.2.18 Test Case SE_LDS_DG1_018

Test Case-ID	SE_LDS_DG1_018
Purpose	This test checks the Code field (if present) of each "Category of Vehicle/Restriction/Condition" entry in the "Categories of Vehicles/Restrictions/Conditions" DO (Tag '7F63') in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, A.4 ISO/IEC 18013-2:2008, A.5.1 ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Categories of Vehicles/Restrictions/Conditions object has been retrieved from EF.DG1.
Test Scenario	Perform the following checks for each of the "Category of Vehicle/Restriction/Condition" entries: 1. Check the length of the Code (sub-field #4). 2. Check the format of the Code. 3. Check the value of the Code.
Expected Results	1. The Code has a maximum length of 5 bytes. 2. Code shall be encoded in a maximum of 5 ANS characters. 3. The value of the Code is one of the values specified in ISO/IEC 18013-2:2008, A.5.1 (i.e. "01", "03", "78", "S01", "S02", "S03", "S04" or "S05").

A.3.2.19 Test Case SE_LDS_DG1_019

Test Case-ID	SE_LDS_DG1_019
Purpose	This test checks the Sign field (if present) of each "Category of Vehicle/Restriction/Condition" entry in the "Categories of Vehicles/Restrictions/Conditions" DO (Tag '7F63') in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, A.4 ISO/IEC 18013-2:2008, A.5.1 ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Categories of Vehicles/Restrictions/Conditions object has been retrieved from EF.DG1.
Test Scenario	Perform the following checks for each of the "Category of Vehicle/Restriction/Condition" entries: 1. Check the length of the Sign (sub-field #5). 2. Check the format of the Sign. 3. Check the value of the Sign. 4. Check the Sign only occurs in combination with an applicable Code. 5. Check the Sign only occurs in combination with a Value field.
Expected Results	1. The Sign has a length of 1 - 2 bytes. 2. Sign shall be encoded in a Special characters. 3. The value of the Sign is one of the values specified in ISO/IEC 18013-2:2008, A.5.1 (i.e. "<","=",">","<=","=<","<>","><",">=","=>","=="). 4. The value of the Code is one of the following values specified in ISO/IEC 18013-2:2008, A.5.1 (i.e. "S01", "S02", "S03" or "S04"). 5. The Value field is not empty.

A.3.2.20 Test Case SE_LDS_DG1_020

Test Case-ID	SE_LDS_DG1_020
Purpose	This test checks the Value field (if present) of each "Category of Vehicle/Restriction/Condition" entry in the "Categories of Vehicles/Restrictions/Conditions" DO (Tag '7F63') in EF.DG1.
Version	1.0
References	ISO/IEC 18013-2:2008, A.4 ISO/IEC 18013-2:2008, A.5.1 ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Categories of Vehicles/Restrictions/Conditions object has been retrieved from EF.DG1.
Test Scenario	Perform the following checks for each of the "Category of Vehicle/Restriction/Condition" entries: 1. Check the format of the Value. 2. Check the Value only occurs in combination with a Code. 3. Check the Value only occurs in combination with a Sign.
Expected Results	1. The Value field shall be encoded in BCD format. 2. The Code field is not empty. 3. The Sign field is not empty.

A.3.3 Test Unit SE_LDS_DG2 – Tests for EF.DG2

Test Unit-ID	SE_LDS_DG2 (Standard Encoding – Data Group 2)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Data Group 2.
References	ISO/IEC 18013-2:2008

A.3.3.1 Test Case SE_LDS_DG2_001

Test Case-ID	SE_LDS_DG2_001
Purpose	This test checks the template tag that the encoded EF.DG2 element starts with.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG2
Preconditions	1. EF.DG2 has been retrieved from the IDL.
Test Scenario	1. Check the very first byte of the EF.DG2 element.
Expected Results	1. First byte shall be '6B'.

A.3.3.2 Test Case SE_LDS_DG2_002

Test Case-ID	SE_LDS_DG2_002
Purpose	This test checks the encoding of EF.DG2 element length.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG2
Preconditions	1. EF.DG2 has been retrieved from the IDL.
Test Scenario	1. Analyze the encoding of the bytes that follow the template tag. 2. Verify the length of the EF.DG2 object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.DG2 object.

A.3.3.3 Test Case SE_LDS_DG2_003

Test Case-ID	SE_LDS_DG2_003
Purpose	This test checks the encoding of the Tag List (Tag '5C') in EF.DG2.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG2
Preconditions	1. EF.DG2 has been retrieved from the IDL.
Test Scenario	1. Search for the Tag List (Tag '5C') inside EF.DG2. 2. Analyze the encoding of the bytes that follow the template tag. 3. Verify the length of the DO with Tag '5C'.
Expected Results	1. Tag '5C' shall be present. 2. The bytes that follow the Tag '5C' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the DO with the Tag '5C'.

A.3.3.4 Test Case SE_LDS_DG2_004

Test Case-ID	SE_LDS_DG2_004
Purpose	This test checks the consistency of the Tag List with the actual data tags present.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG2
Preconditions	1. EF.DG2 has been retrieved from the IDL. 2. Tag List has been retrieved from the EF.DG2.
Test Scenario	1. Check that all data elements that are indicated by the Tag List in EF.DG2 are present.
Expected Results	1. All data elements that are indicated by the Tag List in EF.DG2 shall be present.

A.3.3.5 Test Case SE_LDS_DG2_005

Test Case-ID	SE_LDS_DG2_005
Purpose	This test checks the consistency of the Tag List with the actual present data tags.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG2
Preconditions	1. EF.DG2 has been retrieved from the IDL. 2. Tag List has been retrieved from the EF.DG2.
Test Scenario	1. Check that only data elements that are indicated by the Tag List in EF.DG2 are present.
Expected Results	1. All data elements that are present shall be indicated in the Tag List in EF.DG2.

A.3.3.6 Test Case SE_LDS_DG2_006

Test Case-ID	SE_LDS_DG2_006
Purpose	This test checks the encoding of the Gender (Tag '5F35') in EF.DG2.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG2 Tag '5F35' is present in EF.DG2
Preconditions	1. EF.DG2 has been retrieved from the IDL.
Test Scenario	1. Search for the Gender (Tag '5F 35') inside EF.DG2. 2. Check the length of the DO with Tag '5F 35'. 3. Check the value of Gender.
Expected Results	1. Tag '5F 35' may be present. 2. The length of Gender shall be 1 byte. 3. The value of Gender shall be '00' (Unknown), '01' (Male), '02' (Female), or '09' (Not applicable) encoded in BCD format.

A.3.3.7 Test Case SE_LDS_DG2_007

Test Case-ID	SE_LDS_DG2_007
Purpose	This test checks the encoding of the Height (Tag '5F64') in EF.DG2.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG2 Tag '5F64' is present in EF.DG2
Preconditions	1. EF.DG2 has been retrieved from the IDL.
Test Scenario	1. Search for the Height field (Tag '5F 64') inside EF.DG2. 2. Check the length of the DO with Tag '5F 64'. 3. Check the encoding of the Height field.
Expected Results	1. Tag '5F 64' may be present. 2. The length of the Height field shall be 2 bytes. 3. The value of the Height field shall be encoded in BCD format.

A.3.3.8 Test Case SE_LDS_DG2_008

Test Case-ID	SE_LDS_DG2_008
Purpose	This test checks the encoding of the Weight (Tag '5F65') in EF.DG2.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG2 Tag '5F65' is present in EF.DG2
Preconditions	1. EF.DG2 has been retrieved from the IDL.
Test Scenario	1. Search for the Weight (Tag '5F 65') inside EF.DG2. 2. Check the length of the DO with Tag '5F 65'. 3. Check the encoding of the Weight field.
Expected Results	1. Tag '5F 65' may be present. 2. The length of the Weight field shall be 2 bytes. 3. The value of the Weight field shall be encoded in BCD format.

A.3.3.9 Test Case SE_LDS_DG2_009

Test Case-ID	SE_LDS_DG2_009
Purpose	This test checks the encoding of the Eye Colour (Tag '5F66') in EF.DG2.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG2 Tag '5F66' is present in EF.DG2
Preconditions	1. EF.DG2 has been retrieved from the IDL
Test Scenario	1. Search for the Eye Colour (Tag '5F 66') inside EF.DG2. 2. Check the length of the DO with Tag '5F 66'. 3. Check the encoding of Eye Colour.
Expected Results	1. Tag '5F 66' may be present. 2. The length of Eye Colour shall be 3 bytes. 3. The value of Eye Colour shall be as defined in ANSI D20-2003 (i.e. "BLK", "BLU", "BRO", "GRY", "GRN", "HAZ", "MAR", "PNK", "DIC", or "UNK").

A.3.3.10 Test Case SE_LDS_DG2_010

Test Case-ID	SE_LDS_DG2_010
Purpose	This test checks the encoding of the Hair Colour (Tag '5F67') in EF.DG2.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG2 Tag '5F67' is present in EF.DG2
Preconditions	1. EF.DG2 has been retrieved from the IDL.
Test Scenario	1. Search for the Hair Colour (Tag '5F 67') inside EF.DG2. 2. Check the length of the DO with Tag '5F 67'. 3. Check the encoding of Hair Colour.
Expected Results	1. Tag '5F 67' may be present. 2. The length of Hair Colour shall be 3 bytes. 3. The value of Hair Colour shall be as defined in ANSI D20-2003 (i.e. "BAL", "BLK", "BLN", "BRO", "GRY", "RED", "SDY", "WHI", or "UNK").

A.3.3.11 Test Case SE_LDS_DG2_011

Test Case-ID	SE_LDS_DG2_011
Purpose	This test checks the encoding of the Place of Birth (Tag '5F11') in EF.DG2.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG2 Tag '5F11' is present in EF.DG2
Preconditions	1. EF.DG2 has been retrieved from the IDL.
Test Scenario	1. Search for the Place Of Birth (Tag '5F 11') inside EF.DG2. 2. Check the length of the DO with Tag '5F 11'. 3. Check the length and format of the DO with Tag '5F 11'.. 4. Check the value of Place of Birth.
Expected Results	1. Tag '5F 11' may be present. 2. The bytes that follow the tag shall contain a valid (ASN.1) length encoding. 3. The Place of Birth field shall be encoded as ADNS on 2 - 35 bytes. 4. The value of Place of Birth shall consist of 3 fields that are separated with a sub-field delimiter (";").

A.3.3.12 Test Case SE_LDS_DG2_012

Test Case-ID	SE_LDS_DG2_012
Purpose	This test checks the encoding of the Place of Residence (Tag '5F42') in EF.DG2.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG2 Tag '5F42' is present in EF.DG2
Preconditions	1. EF.DG2 has been retrieved from the IDL.
Test Scenario	1. Search for the Place Of Residence (Tag '5F 42') inside EF.DG2. 2. Check the length of the DO with Tag '5F 42'. 3. Check the length and format of the DO with Tag '5F 42'. 4. Check the value of Place of Residence.
Expected Results	1. Tag '5F 42' may be present. 2. The bytes that follow the tag shall contain a valid (ASN.1) length encoding. 3. The Place of Residence field shall be encoded as ADNS on 5 - 113 bytes. 4. The value of Place of Residence shall consist of 6 fields that are separated with a sub-field delimiter (";").

A.3.4 Test Unit SE_LDS_DG3 – Tests for EF.DG3

Test Unit-ID	SE_LDS_DG3 (Standard Encoding – Data Group 3)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Data Group 3.
References	ISO/IEC 18013-2:2008

A.3.4.1 Test Case SE_LDS_DG3_001

Test Case-ID	SE_LDS_DG3_001
Purpose	This test checks the template tag that the encoded EF.DG3 element starts with.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG3
Preconditions	1. EF.DG3 has been retrieved from the IDL.
Test Scenario	1. Check the very first byte of the EF.DG3 element.
Expected Results	1. First byte shall be '6C'.

A.3.4.2 Test Case SE_LDS_DG3_002

Test Case-ID	SE_LDS_DG3_002
Purpose	This test checks the encoding of EF.DG3 element length.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG3
Preconditions	1. EF.DG3 has been retrieved from the IDL.
Test Scenario	1. Analyze the encoding of the bytes that follow the template tag. 2. Verify the length of the EF.DG3 object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.DG3 object.

A.3.4.3 Test Case SE_LDS_DG3_003

Test Case-ID	SE_LDS_DG3_003
Purpose	This test checks the encoding of the Tag List (Tag '5C') in EF.DG3.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG3
Preconditions	1. EF.DG3 has been retrieved from the IDL.
Test Scenario	1. Search for the Tag List (Tag '5C') inside EF.DG3. 2. Analyze the encoding of the bytes that follow the template tag. 3. Verify the length of the DO with Tag '5C'. 4. Analyse the value of the data object with Tag '5C'.
Expected Results	1. Tag '5C' shall be present. 2. The bytes that follow the Tag '5C' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the DO with the Tag '5C'. 4. The encoded value shall only contain tags specified in Table C.8 of ISO/IEC 18013-2:2008.

A.3.4.4 Test Case SE_LDS_DG3_004

Test Case-ID	SE_LDS_DG3_004
Purpose	This test checks the consistency of the Tag List with the actual data tags present.

Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG3
Preconditions	1. EF.DG3 has been retrieved from the IDL. 2. Tag List has been retrieved from the EF.DG3.
Test Scenario	1. Check that all data elements that are indicated by the Tag List in EF.DG3 are present.
Expected Results	1. All data elements that are indicated by the Tag List in EF.DG3 shall be present.

A.3.4.5 Test Case SE_LDS_DG3_005

Test Case-ID	SE_LDS_DG3_005
Purpose	This test checks the consistency of the Tag List with the actual data tags present.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG3
Preconditions	1. EF.DG3 has been retrieved from the IDL. 2. Tag List has been retrieved from the EF.DG3.
Test Scenario	1. Check that only data elements that are indicated by the Tag List in EF.DG3 are present.
Expected Results	1. All data elements that are present shall be indicated in the Tag List in EF.DG3.

A.3.4.6 Test Case SE_LDS_DG3_006

Test Case-ID	SE_LDS_DG3_006
Purpose	This test checks the encoding of the Administrative Number (Tag '5F68') in EF.DG3.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG3 Tag '5F68' is present in EF.DG3.
Preconditions	1. EF.DG3 has been retrieved from the IDL.
Test Scenario	1. Search for the Administrative Number (Tag '5F 68') inside EF.DG3. 2. Check the length of the DO with Tag '5F 68'. 3. Check the encoding of Administrative Number.
Expected Results	1. Tag '5F 68' may be present. 2. The bytes that follow the Tag '5F 68' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The Administrative Number shall be as coded as ANS and shall not be longer than 25 bytes.

A.3.4.7 Test Case SE_LDS_DG3_007

Test Case-ID	SE_LDS_DG3_007
Purpose	This test checks the encoding of the Document Discriminator (Tag '5F69') in EF.DG3.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG3 Tag '5F69' is present in EF.DG3
Preconditions	1. EF.DG3 has been retrieved from the IDL.
Test Scenario	1. Search for the Document Discriminator (Tag '5F 69') inside EF.DG3. 2. Check the length of the DO with Tag '5F 69'. 3. Check the encoding of Document Discriminator.
Expected Results	1. Tag '5F 69' may be present.

	2. The length of the DO with Tag '5F 69' shall be 1 byte. 3. The Document Discriminator shall be as coded as BCD.

A.3.4.8 Test Case SE_LDS_DG3_008

Test Case-ID	SE_LDS_DG3_008
Purpose	This test checks the encoding of the Data Discriminator (Tag '5F6D') in EF.DG3.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG3 Tag '5F6D' is present in EF.DG3
Preconditions	1. EF.DG3 has been retrieved from the IDL.
Test Scenario	1. Search for the Data Discriminator (Tag '5F 6D') inside EF.DG3. 2. Check the length of the DO with Tag '5F 6D'. 3. Check the encoding of Data Discriminator.
Expected Results	1. Tag '5F 6D' may be present. 2. The length of the DO with Tag '5F 6D' shall be 1 byte. 3. The Data Discriminator shall be as coded as BCD.

A.3.4.9 Test Case SE_LDS_DG3_009

Test Case-ID	SE_LDS_DG3_009
Purpose	This test checks the encoding of the ISO Issuer ID Number (Tag '5F6A') in EF.DG3.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG3 Tag '5F6A' is present in EF.DG3
Preconditions	1. EF.DG3 has been retrieved from the IDL.
Test Scenario	1. Search for the ISO Issuer ID Number (Tag '5F 6A') inside EF.DG3. 2. Check the length of the DO with Tag '5F 6A'. 3. Check the encoding of ISO Issuer ID Number.
Expected Results	1. Tag '5F 6A' may be present. 2. The length of the DO with Tag '5F 6A' shall be 3 bytes. 3. The ISO Issuer ID Number shall be as coded as BCD.

A.3.5 Test Unit SE_LDS_DG4 – Tests for EF.DG4

Test Unit-ID	SE_LDS_DG4 (Standard Encoding – Data Group 4)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Data Group 4.
References	ISO/IEC 18013-2:2008

A.3.5.1 Test Case SE_LDS_DG4_001

Test Case-ID	SE_LDS_DG4_001
Purpose	This test checks the template tag, the encoded EF.DG4 element starts with.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG4
Preconditions	1. EF.DG4 has been retrieved from the IDL.
Test Scenario	1. Check the very first byte of the EF.DG4 element.
Expected Results	1. First byte shall be '65'.

A.3.5.2 Test Case SE_LDS_DG4_002

Test Case-ID	SE_LDS_DG4_002
Purpose	This test checks the encoding of EF.DG4 element length.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG4
Preconditions	1. EF.DG4 has been retrieved from the IDL.
Test Scenario	1. Analyze the encoding of the bytes that follow the template tag. 2. Verify the length of the EF.DG4 object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.DG4 object.

A.3.5.3 Test Case SE_LDS_DG4_003

Test Case-ID	SE_LDS_DG4_003
Purpose	This test checks the Number of Portraits (Tag '02') present in EF.DG4.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG4
Preconditions	1. EF.DG4 has been retrieved from the IDL

Test Scenario	1. Search for the Number of Portraits (Tag '02') inside EF.DG4. 2. Check the length of the Number of Portraits data element. 3. Check the value of the Number of Portraits data element.
Expected Results	1. Tag '02' shall be present. 2. The length of the Number of Portraits data element shall be 1 byte. 3. The Number of Portraits (01) shall match the number of occurrences of tag 'A2' in EF.DG4.

A.3.5.4 Test Case SE_LDS_DG4_004

Test Case-ID	SE_LDS_DG4_004
Purpose	This test checks the encoding of all Portrait Templates (Tag 'A2') in EF.DG4.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG4
Preconditions	1. EF.DG4 has been retrieved from the IDL.
Test Scenario	1. Check the Portrait Template tag. 2. Analyze the encoding of the bytes that follow the template tag. 3. Verify the length of the DO with Tag 'A2'.
Expected Results	1. The Portrait Template tag shall be 'A2'. 2. The bytes that follow the Tag 'A2' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the DO with the Tag 'A2'.

A.3.5.5 Test Case SE_LDS_DG4_005

Test Case-ID	SE_LDS_DG4_005
Purpose	This test checks the encoding of the Image Time Stamp (Tag '88') in each Portrait Template in EF.DG4.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG4
Preconditions	1. EF.DG4 has been retrieved from the IDL.
Test Scenario	1. Search for the Image Time Stamp (Tag '88') inside the Portrait Template. 2. Check the length of the Image Time Stamp data element. 3. Check the encoding of the Image Time Stamp data element. 4. Check the value of the Image Time Stamp data element.
Expected Results	1. Tag '88' shall be present. 2. The length of the Image Time Stamp data element shall be 7 bytes. 3. The Image Time Stamp data element shall be BCD encoded. 4. The Image Time Stamp data element shall represent a valid date/time coded as YYYYMMDDhhmmss.

A.3.5.6 Test Case SE_LDS_DG4_006

Test Case-ID	SE_LDS_DG4_006
Purpose	This test checks the encoding of the Type of Image (Tag '89') in each Portrait Template in EF.DG4.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG4
Preconditions	1. EF.DG4 has been retrieved from the IDL.
Test Scenario	1. Search for the Type of Image (Tag '89') inside the Portrait Template. 2. Check the length of the Type of Image data element. 3. Check the value of the Type of Image data element.
Expected Results	1. Tag '89' shall be present. 2. The length of the Type of Image data element shall be 1 byte.

	3. The Type of Image data element shall be one of the values indicated in ISO/IEC 18013-2:2008, 8.4 (i.e. '02', '03', or '04').

A.3.5.7 Test Case SE_LDS_DG4_007

Test Case-ID	SE_LDS_DG4_007
Purpose	This test checks the encoding of the Image (Tag '5F 40') in each Portrait Template in EF.DG4.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C, Annex E
Profile	DG4
Preconditions	1. EF.DG4 has been retrieved from the IDL
Test Scenario	1. Search for the Image (Tag '5F 40') inside the Portrait Template. 2. Check the encoded length of the Image data element. 3. Verify the length of the Image data element. 4. Verify the type of Image. 5. Verify consistency of Image type with encoded element.
Expected Results	1. Tag '5F 40' shall be present. 2. The bytes that follow the Tag '5F 40' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the data element with the Tag '5F 40'. 4. The type of Image shall match one of the values in Table E.1 in ISO/IEC 18013-2:2008 5. The encoded Image format shall match the image type stated in the Type of image field.

A.3.6 Test Unit SE_LDS_DG5 – Tests for EF.DG5

Test Unit-ID	SE_LDS_DG5 (Standard Encoding – Data Group 5)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Data Group 5.
References	ISO/IEC 18013-2:2008

A.3.6.1 Test Case SE_LDS_DG5_001

Test Case-ID	SE_LDS_DG5_001
Purpose	This test checks the template tag that the encoded EF.DG5 element starts with.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG5
Preconditions	1. EF.DG5 has been retrieved from the IDL.
Test Scenario	1. Check the very first byte of the EF.DG5 element.
Expected Results	1. First byte shall be '67'.

A.3.6.2 Test Case SE_LDS_DG5_002

Test Case-ID	SE_LDS_DG5_002
Purpose	This test checks the encoding of EF.DG5 element length.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG5 has been retrieved from the IDL.
Test Scenario	1. Analyze the encoding of the bytes that follow the template tag.johann1e 2. Verify the length of the EF.DG5 object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.DG5 object.

A.3.6.3 Test Case SE_LDS_DG5_003

Test Case-ID	SE_LDS_DG5_003
Purpose	This test checks the Type of Image (Tag '89') present in EF.DG5.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG5 has been retrieved from the IDL.
Test Scenario	1. Search for the Type of Image (Tag '89') inside EF.DG5. 2. Check the length of the Type of Image data element. 3. Check the value of the Type of Image data element.
Expected Results	1. Tag '89' shall be present. 2. The length of the Type of Image data element shall be 1 byte. 3. The Type of Image data element shall be one of the values indicated in ISO/IEC 18013-2:2008, 8.5 (i.e. '02', '03', or '04').

A.3.6.4 Test Case SE_LDS_DG5_004

Test Case-ID	SE_LDS_DG5_004
Purpose	This test checks the Image of Signature or Mark (Tag '5F 43') present in EF.DG5.
Version	1.0

References	ISO/IEC 18013-2:2008, Annex C, Annex E
Profile	DG7
Preconditions	1. EF.DG5 has been retrieved from the IDL.
Test Scenario	1. Search for the Image of Signature or Mark (Tag '5F 43') inside EF.DG5. 2. Check the encoded length of the Image of Signature or Mark data element. 3. Check the length of the Image of Signature or Mark data element. 4. Verify the type of Image. 5. Verify consistency of Image type with encoded element.
Expected Results	1. Tag '5F 43' shall be present. 2. The bytes that follow the Tag '5F 43' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the Image of Signature or Mark data element. 4. The type of Image shall match one of the values in Table E.1 in ISO/IEC 18013-2:2008. 5. The encoded Image format shall match the image type stated in the Type of image field.

A.3.7 Test Unit SE_LDS_DG6 – Tests for EF.DG6

Test Unit-ID	SE_LDS_DG6 (Standard Encoding – Data Group 6)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Data Group 6.
References	ISO/IEC 18013-2:2008

A.3.7.1 Test Case SE_LDS_DG6_001

Test Case-ID	SE_LDS_DG6_001
Purpose	This test checks the template tag that the encoded EF.DG6 element starts with.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL.
Test Scenario	1. Check the very first byte of the EF.DG6 element.
Expected Results	1. First byte shall be '75'.

A.3.7.2 Test Case SE_LDS_DG6_002

Test Case-ID	SE_LDS_DG6_002
Purpose	This test checks the encoding of EF.DG6 element length.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL.
Test Scenario	1. Analyze the encoding of the bytes that follow the template tag. 2. Verify the length of the EF.DG6 object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.DG6 object.

A.3.7.3 Test Case SE_LDS_DG6_003

Test Case-ID	SE_LDS_DG6_003
Purpose	This test checks the encoding of the Biometric Group Template (Tag '7F

	61') present in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL.
Test Scenario	1. Search for the Biometric Group Template (Tag '7F 61') inside EF.DG6. 2. Check the encoded length of the Biometric Group Template data element. 3. Check the length of the Biometric Group Template data element.
Expected Results	1. Tag '7F 61' shall be present. 2. The bytes that follow the Tag '7F 61' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the Biometric Group Template data element.

A.3.7.4 Test Case SE_LDS_DG6_004

Test Case-ID	SE_LDS_DG6_004
Purpose	This test checks the "Number of Biometric Templates" DO in the "Biometric Group Template" DO (Tag '7F61') in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	1. Search for the Number of Biometric Templates (Tag '02') inside the Biometric Group Template. 2. Analyze the encoding of the length of the Number of Biometric Templates DO coded with tag '02'. 3. Check the value encoded in the Number of Biometric Templates DO.
Expected Results	1. Tag '02' shall be present. 2. The length encoded in the Number of Biometric Templates DO shall be '01'h. 3. The value encoded in the Number of Biometric Templates DO matches the number of occurences of a DO with tag '7F 60' in the Biometric Group Template.

A.3.7.5 Test Case SE_LDS_DG6_005

Test Case-ID	SE_LDS_DG6_005
Purpose	This test checks the encoding of each "Biometric Template" DO in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Analyze the tag of the Biometric Template. 2. Analyze the encoding of the bytes that follow the tag '7F 60'. 3. Verify the length of the DO with Tag '7F 60'.
Expected Results	1. The tag shall be '7F 60'. 2. The bytes that follow the Tag '7F 60' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the DO with the Tag '7F 60'.

A.3.7.6 Test Case SE_LDS_DG6_006

Test Case-ID	SE_LDS_DG6_006
Purpose	This test checks the encoding of the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Biometric Header Template (Tag 'A1') inside the Biometric Template. 2. Analyze the encoding of the bytes that follow the tag 'A1'. 3. Check the length of the Biometric Header Template.
Expected Results	1. Tag 'A1' shall be present. 2. The bytes that follow the Tag 'A1' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the Biometric Header Template.

A.3.7.7 Test Case SE_LDS_DG6_008

Test Case-ID	SE_LDS_DG6_008
Purpose	This test checks the encoding of the Patron Header Version (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Patron Header Version data element with tag '80' is present inside the Biometric Header Template: 1. Search for the Patron Header Version (Tag '80') inside the Biometric Header Template. 2. Check the length encoded for the Patron Header Version data element. 3. Check the value of the Patron Header Version data element.
Expected Results	1. Tag '80' may be present and shall not occur more than once. 2. The encoded length shall be '02'. 3. The Patron Header Version shall have the value '01 01'.

A.3.7.8 Test Case SE_LDS_DG6_009

Test Case-ID	SE_LDS_DG6_009
Purpose	This test checks the encoding of the Biometric Type (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Biometric Type data element with tag '81' is present inside the Biometric Header Template: 1. Search for the Biometric Type (Tag '81') inside the Biometric Header Template.

	2. Check the length encoded for the Biometric Type data element. 3. Check the value of the Biometric Type data element.
Expected Results	1. Tag '81' may be present and shall not occur more than once. 2. The encoded length shall be '01'. 3. The Biometric Type shall have the value '02' (Facial).

A.3.7.9 Test Case SE_LDS_DG6_010

Test Case-ID	SE_LDS_DG6_010
Purpose	This test checks the encoding of the Biometric Subtype (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Biometric Subtype data element with tag '82' is present inside the Biometric Header Template: 1. Search for the Biometric Subtype (Tag '82') inside the Biometric Header Template. 2. Check the length encoded for the Biometric Subtype data element. 3. Check the value of the Biometric Subtype data element.
Expected Results	1. Tag '82' may be present and shall not occur more than once. 2. The encoded length shall be '01'. 3. The Biometric Subtype shall have the value '00' (No information given).

A.3.7.10 Test Case SE_LDS_DG6_011

Test Case-ID	SE_LDS_DG6_011
Purpose	This test checks the encoding of the Biometric data creation date and time (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6. 3. The Number of Biometric Templates has been retrieved from the Biometric Group Template.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Biometric data creation date and time data element with tag '83' is present inside the Biometric Header Template or if more than one Biometric Template is present inside the Biometric Group Template: 1. Search for the Biometric data creation date and time (Tag '83') inside the Biometric Header Template. 2. Check the length encoded for the Biometric data creation date and time data element. 3. Check the format of the Biometric data creation date and time. 4. Check the value of the Biometric data creation date and time data element.
Expected Results	1. Tag '83' may be present and shall not occur more than once. 2. The encoded length shall be '07'. 3. Date of Issue shall be BCD encoded. 4. The Biometric data creation date and time data element shall represent a valid date/time coded as YYYYMMDDhhmmss.

A.3.7.11 Test Case SE_LDS_DG6_012

Test Case-ID	SE_LDS_DG6_012
Purpose	This test checks the encoding of the BIR Creator (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BIR Creator data element with tag '84' is present inside the Biometric Header Template: 1. Search for the BIR Creator (Tag '84') inside the Biometric Header Template. 2. Check the length encoded for the BIR Creator data element. 3. Verify the length of the BIR Creator data element. 4. Check the format of the BIR Creator data element.
Expected Results	1. Tag '84' may be present and shall not occur more than once. 2. The bytes that follow the Tag '84' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the BIR Creator data element. 4. The BIR Creator shall be encoded as ANS characters.

A.3.7.12 Test Case SE_LDS_DG6_013

Test Case-ID	SE_LDS_DG6_013
Purpose	This test checks the encoding of the BDB Validity Period (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BDB Validity Period data element with tag '85' is present inside the Biometric Header Template: 1. Search for the BDB Validity Period (Tag '85') inside the Biometric Header Template. 2. Check the length encoded for the BDB Validity Period data element. 3. Check the format of the BDB Validity Period. 4. Check the value of the BDB Validity Period data element. 5. Check the consistency of the value of the BDB Validity Period data element.
Expected Results	1. Tag '85' may be present and shall not occur more than once. 2. The encoded length shall be '08'. 3. The BDB Validity Period shall be BCD encoded. 4. The BDB Validity Period shall represent a valid effective date and a valid expiry date coded as YYYYMMDDYYYYMMDD. 5. The BDB Validity Period effective date shall represent an effective date BEFORE the expiry date.

A.3.7.13 Test Case SE_LDS_DG6_014

Test Case-ID	SE_LDS_DG6_014
Purpose	This test checks the encoding of the BDB Product Owner, Product Type (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.

Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 19785-1:2006
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BDB Product Owner, Product Type data element with tag '86' is present inside the Biometric Header Template: 1. Search for the BDB Product Owner, Product Type (Tag '86') inside the Biometric Header Template. 2. Check the length encoded for the BDB Product Owner, Product Type data element. 3. Check the value of the BDB Product Owner, Product Type data element. 4. Check the consistency of the BDB Product Owner, Product Type data element.
Expected Results	1. Tag '86' may be present and shall not occur more than once. 2. The encoded length shall be '04'. 3. The BDB Product Owner, Product Type shall be a concatenation of two 16-bit POSITIVE integers. 4. The BDB Product Owner, Product Type shall have be a valid combination of product owner and product type as defined in ISO/IEC 19785-1:2006, 6.5.12 and 6.5.13.

A.3.7.14 Test Case SE_LDS_DG6_015

Test Case-ID	SE_LDS_DG6_015
Purpose	This test checks the encoding of the BDB Format Owner in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 19785-1:2006
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BDB Format Owner (Tag '87') inside the Biometric Header Template. 2. Check the length encoded for the BDB Format Owner data element. 3. Check the value of the BDB Format Owner data element. 4. Check the validity of the BDB Format Owner data element.
Expected Results	1. Tag '87' shall be present. 2. The encoded length shall be '02'. 3. The BDB Format Owner shall be a 16-bit POSITIVE integer. 4. The BDB Format Owner shall have be a valid format owner as defined in ISO/IEC 19785-1:2006, 6.5.1.

A.3.7.15 Test Case SE_LDS_DG6_016

Test Case-ID	SE_LDS_DG6_016
Purpose	This test checks the encoding of the BDB format type in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 19785-1:2006
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BDB format type (Tag '88') inside the Biometric Header Template. 2. Check the length encoded for the BDB format type data element. 3. Check the value of the BDB format type data element. 4. Check the validity of the BDB format type data element. 5. Check the consistency of the BDB format type data element with the BDB format owner data element.
Expected Results	1. Tag '88' shall be present. 2. The encoded length shall be '02'. 3. The BDB format type shall be a 16-bit POSITIVE integer. 4. The BDB format type shall have be a valid format type as defined in ISO/IEC 19785-1:2006, 6.5.2. 5. The BDB format type shall be valid in combination with the format owner data element.

A.3.7.16 Test Case SE_LDS_DG6_017

Test Case-ID	SE_LDS_DG6_017
Purpose	This test checks the encoding of the BIR index (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BIR index data element with tag '90' is present inside the Biometric Header Template: 1. Search for the BIR index (Tag '90') inside the Biometric Header Template. 2. Check the length encoded for the BIR index data element. 3. Verify the length of the BIR index data element.
Expected Results	1. Tag '90' may be present and shall not occur more than once. 2. The bytes that follow the Tag '90' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the BIR index data element.

A.3.7.17 Test Case SE_LDS_DG6_018

Test Case-ID	SE_LDS_DG6_018
Purpose	This test checks the presence and encoding of the Biometric Data Block (Tag '5F 2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Biometric Data Block (Tag '5F 2E') inside the Biometric Template. 2. If Tag '5F 2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3. If Tag '5F 2E' is present, verify the length of the Biometric Data Block DO. 4. If Tag '5F 2E' is present, verify that the tag for the Enciphered Biometric Data Block (Tag '7F 2E') is absent. 5. If Tag '5F 2E' is absent, verify that the tag for the Enciphered Biometric Data Block (Tag '7F 2E') is present.
Expected Results	1. Tag '5F 2E' may be present and shall not occur more than once. 2. If Tag '5F 2E' is present, the bytes that follow the Biometric Data Block Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '5F 2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4. If Tag '5F 2E' is present, Tag '7F 2E' shall be absent. 5. If Tag '5F 2E' is absent, Tag '7F 2E' shall be present.

A.3.7.18 Test Case SE_LDS_DG6_019

Test Case-ID	SE_LDS_DG6_019
Purpose	This test checks the presence and encoding of the Enciphered Biometric Data Block (Tag '7F 2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Biometric Data Block (Tag '7F 2E') inside the Biometric Template. 2. If Tag '7F 2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3. If Tag '7F 2E' is present, verify the length of the Enciphered Biometric Data Block DO. 4. If Tag '7F 2E' is present, verify that the tag for the Biometric Data Block (Tag '5F 2E') is absent. 5. If Tag '7F 2E' is absent, verify that the tag for the Biometric Data Block (Tag '5F 2E') is present.
Expected Results	1. Tag '7F 2E' may be present and shall not occur more than once. 2. If Tag '7F 2E' is present, the bytes that follow the Biometric Data Block Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '7F 2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4. If Tag '7F 2E' is present, Tag '5F 2E' shall be absent.

	5. If Tag '7F 2E' is absent, Tag '5F 2E' shall be present.

A.3.7.19 Test Case SE_LDS_DG6_020

Test Case-ID	SE_LDS_DG6_020
Purpose	This test checks the encoding of the BIR payload (Tag '53') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BIR payload (Tag '53') inside the Biometric Template. 2. If Tag '53' is present, analyze the encoding of the bytes that follow the BIR payload tag. 3. If Tag '53' is present, verify the length of the BIR payload DO. 4. If Tag '53' is present, verify that the tag '73' is absent.
Expected Results	1. Tag '53' may be present and shall not occur more than once. 2. If Tag '53' is present, the bytes that follow the BIR payload Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '53' is present, the encoded length shall match the size of the BIR payload DO. 4. If Tag '53' is present, Tag '73' shall be absent.

A.3.7.20 Test Case SE_LDS_DG6_021

Test Case-ID	SE_LDS_DG6_021
Purpose	This test checks the encoding of the BIR payload (Tag '73') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BIR payload (Tag '73') inside the Biometric Template. 2. If Tag '73' is present, analyze the encoding of the bytes that follow the BIR payload tag. 3. If Tag '73' is present, verify the length of the BIR payload DO. 4. If Tag '73' is present, verify that the tag '53' is absent.
Expected Results	1. Tag '73' may be present and shall not occur more than once. 2. If Tag '73' is present, the bytes that follow the BIR payload Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '73' is present, the encoded length shall match the size of the BIR payload DO. 4. If Tag '73' is present, Tag '53' shall be absent.

A.3.7.21 Test Case SE_LDS_DG6_022

Test Case-ID	SE_LDS_DG6_022
Purpose	This test checks the encoding of the Security Block (Tag '5F 3D') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG6
Preconditions	1. EF.DG6 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG6.

Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Security Block (Tag '5F 3D') inside the Biometric Template. 2. If Tag '5F 3D' is present, analyze the encoding of the bytes that follow the Security Block tag. 3. If Tag '5F 3D' is present, verify the length of the Security Block DO.
Expected Results	1. Tag '5F 3D' may be present and shall not occur more than once. 2. If Tag '5F 3D' is present, the bytes that follow the Security Block Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '5F 3D' is present, the encoded length shall match the size of the Security Block DO.

A.3.8 Test Unit SE_LDS_DG7 – Tests for EF.DG7

Test Unit-ID	SE_LDS_DG7 (Standard Encoding – Data Group 7)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Data Group 7.
References	ISO/IEC 18013-2:2008

A.3.8.1 Test Case SE_LDS_DG7_001

Test Case-ID	SE_LDS_DG7_001
Purpose	This test checks the template tag; the encoded EF.DG7 element starts with.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL.
Test Scenario	1. Check the very first byte of the EF.DG7 element.
Expected Results	1. First byte shall be '63'.

A.3.8.2 Test Case SE_LDS_DG7_002

Test Case-ID	SE_LDS_DG7_002
Purpose	This test checks the encoding of EF.DG7 element length.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL.
Test Scenario	1. Analyze the encoding of the bytes that follow the template tag. 2. Verify the length of the EF.DG7 object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.DG7 object.

A.3.8.3 Test Case SE_LDS_DG7_003

Test Case-ID	SE_LDS_DG7_003
Purpose	This test checks the encoding of the Biometric Group Template (Tag '7F 61') present in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL.
Test Scenario	1. Search for the Biometric Group Template (Tag '7F 61') inside EF.DG7. 2. Check the encoded length of the Biometric Group Template data

	element. 3. Check the length of the Biometric Group Template data element.
Expected Results	1. Tag '7F 61' shall be present. 2. The bytes that follow the Tag '7F 61' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the Biometric Group Template data element.

A.3.8.4 Test Case SE_LDS_DG7_004

Test Case-ID	SE_LDS_DG7_004
Purpose	This test checks the "Number of Biometric Templates" DO in the "Biometric Group Template" DO (Tag '7F61') in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	1. Search for the Number of Biometric Templates (Tag '02') inside the Biometric Group Template. 2. Analyze the encoding of the length of the Number of Biometric Templates DO coded with tag '02'. 3. Check the value encoded in the Number of Biometric Templates DO.
Expected Results	1. Tag '02' shall be present. 2. The length encoded in the Number of Biometric Templates DO shall be '01'h. 3. The value encoded in the Number of Biometric Templates DO matches the number of occurences of a DO with tag '7F 60' in the Biometric Group Template.

A.3.8.5 Test Case SE_LDS_DG7_005

Test Case-ID	SE_LDS_DG7_005
Purpose	This test checks the encoding of each "Biometric Template" DO in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Analyze the tag of the Biometric Template. 2. Analyze the encoding of the bytes that follow the tag '7F 60'. 3. Verify the length of the DO with Tag '7F 60'.
Expected Results	1. The tag shall be '7F 60'. 2. The bytes that follow the Tag '7F 60' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the DO with the Tag '7F 60'.

A.3.8.6 Test Case SE_LDS_DG7_006

Test Case-ID	SE_LDS_DG7_006
Purpose	This test checks the encoding of the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL.

	2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Biometric Header Template (Tag 'A1') inside the Biometric Template. 2. Analyze the encoding of the bytes that follow the tag 'A1'. 3. Check the length of the Biometric Header Template.
Expected Results	1. Tag 'A1' shall be present. 2. The bytes that follow the Tag 'A1' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the Biometric Header Template.

A.3.8.7 Test Case SE_LDS_DG7_008

Test Case-ID	SE_LDS_DG7_008
Purpose	This test checks the encoding of the Patron Header Version (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Patron Header Version data element with tag '80' is present inside the Biometric Header Template: 1. Search for the Patron Header Version (Tag '80') inside the Biometric Header Template. 2. Check the length encoded for the Patron Header Version data element. 3. Check the value of the Patron Header Version data element.
Expected Results	1. Tag '80' may be present and shall not occur more than once. 2. The encoded length shall be '02'. 3. The Patron Header Version shall have the value '01 01'.

A.3.8.8 Test Case SE_LDS_DG7_009

Test Case-ID	SE_LDS_DG7_009
Purpose	This test checks the encoding of the Biometric Type (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Biometric Type data element with tag '81' is present inside the Biometric Header Template: 1. Search for the Biometric Type (Tag '81') inside the Biometric Header Template. 2. Check the length encoded for the Biometric Type data element. 3. Check the value of the Biometric Type data element.
Expected Results	1. Tag '81' may be present and shall not occur more than once. 2. The encoded length shall be '01'. 3. The Biometric Type shall have the value '08' (Finger).

A.3.8.9 Test Case SE_LDS_DG7_010

Test Case-ID	SE_LDS_DG7_010

Purpose	This test checks the encoding of the Biometric Subtype (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Biometric Subtype data element with tag '82' is present inside the Biometric Header Template: 1. Search for the Biometric Subtype (Tag '82') inside the Biometric Header Template. 2. Check the length encoded for the Biometric Subtype data element. 3. Check the value of the Biometric Subtype data element.
Expected Results	1. Tag '82' shall be present. 2. The encoded length shall be '01'. 3. The Biometric Subtype shall have a non-zero value.

A.3.8.10 Test Case SE_LDS_DG7_011

Test Case-ID	SE_LDS_DG7_011
Purpose	This test checks the encoding of the Biometric data creation date and time (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7. 3. The Number of Biometric Templates has been retrieved from the Biometric Group Template.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Biometric data creation date and time data element with tag '83' is present inside the Biometric Header Template or if more than one Biometric Template is present inside the Biometric Group Template: 1. Search for the Biometric data creation date and time (Tag '83') inside the Biometric Header Template. 2. Check the length encoded for the Biometric data creation date and time data element. 3. Check the format of the Biometric data creation date and time. 4. Check the value of the Biometric data creation date and time data element.
Expected Results	1. Tag '83' may be present and shall not occur more than once. 2. The encoded length shall be '07'. 3. Date of Issue shall be BCD encoded. 4. The Biometric data creation date and time data element shall represent a valid date/time coded as YYYYMMDDhhmmss.

A.3.8.11 Test Case SE_LDS_DG7_012

Test Case-ID	SE_LDS_DG7_012
Purpose	This test checks the encoding of the BIR Creator (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL.

	2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BIR Creator data element with tag '84' is present inside the Biometric Header Template: 1. Search for the BIR Creator (Tag '84') inside the Biometric Header Template. 2. Check the length encoded for the BIR Creator data element. 3. Verify the length of the BIR Creator data element. 4. Check the format of the BIR Creator data element.
Expected Results	1. Tag '84' may be present and shall not occur more than once. 2. The bytes that follow the Tag '84' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the BIR Creator data element. 4. The BIR Creator shall be encoded as ANS characters.

A.3.8.12 Test Case SE_LDS_DG7_013

Test Case-ID	SE_LDS_DG7_013
Purpose	This test checks the encoding of the BDB Validity Period (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BDB Validity Period data element with tag '85' is present inside the Biometric Header Template: 1. Search for the BDB Validity Period (Tag '85') inside the Biometric Header Template. 2. Check the length encoded for the BDB Validity Period data element. 3. Check the format of the BDB Validity Period. 4. Check the value of the BDB Validity Period data element. 5. Check the consistency of the value of the BDB Validity Period data element.
Expected Results	1. Tag '85' may be present and shall not occur more than once. 2. The encoded length shall be '08'. 3. The BDB Validity Period shall be BCD encoded. 4. The BDB Validity Period shall represent a valid effective date and a valid expiry date coded as YYYYMMDDYYYYMMDD. 5. The BDB Validity Period effective date shall represent an effective date BEFORE the expiry date.

A.3.8.13 Test Case SE_LDS_DG7_014

Test Case-ID	SE_LDS_DG7_014
Purpose	This test checks the encoding of the BDB Product Owner, Product Type (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 19785-1:2006
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BDB Product Owner, Product Type data element with tag '86'

	is present inside the Biometric Header Template: 1. Search for the BDB Product Owner, Product Type (Tag '86') inside the Biometric Header Template. 2. Check the length encoded for the BDB Product Owner, Product Type data element. 3. Check the value of the BDB Product Owner, Product Type data element. 4. Check the consistency of the BDB Product Owner, Product Type data element.
Expected Results	1. Tag '86' may be present and shall not occur more than once. 2. The encoded length shall be '04'. 3. The BDB Product Owner, Product Type shall be a concatenation of two 16-bit POSITIVE integers. 4. The BDB Product Owner, Product Type shall have be a valid combination of product owner and product type as defined in ISO/IEC 19785-1:2006, 6.5.12 and 6.5.13.

A.3.8.14 Test Case SE_LDS_DG7_015

Test Case-ID	SE_LDS_DG7_015
Purpose	This test checks the encoding of the BDB Format Owner in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 19785-1:2006
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BDB Format Owner (Tag '87') inside the Biometric Header Template. 2. Check the length encoded for the BDB Format Owner data element. 3. Check the value of the BDB Format Owner data element. 4. Check the validity of the BDB Format Owner data element.
Expected Results	1. Tag '87' shall be present. 2. The encoded length shall be '02'. 3. The BDB Format Owner shall be a 16-bit POSITIVE integer. 4. The BDB Format Owner shall have be a valid format owner as defined in ISO/IEC 19785-1:2006, 6.5.1

A.3.8.15 Test Case SE_LDS_DG7_016

Test Case-ID	SE_LDS_DG7_016
Purpose	This test checks the encoding of the BDB Format Type in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 19785-1:2006
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BDB Format Type (Tag '88') inside the Biometric Header Template. 2. Check the length encoded for the BDB Format Type data element. 3. Check the value of the BDB Format Type data element. 4. Check the validity of the BDB Format Type data element. 5. Check the consistency of the BDB Format Type data element with the BDB format owner data element.
Expected Results	1. Tag '88' shall be present. 2. The encoded length shall be '02'. 3. The BDB Format Type shall be a 16-bit POSITIVE integer. 4. The BDB Format Type shall have be a valid format type as defined in ISO/IEC 19785-1:2006, 6.5.2. 5. The BDB Format Type shall be valid in combination with the format owner data element.

A.3.8.16 Test Case SE_LDS_DG7_017

Test Case-ID	SE_LDS_DG7_017
Purpose	This test checks the encoding of the BIR index (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BIR index data element with tag '90' is present inside the Biometric Header Template: 1. Search for the BIR index (Tag '90') inside the Biometric Header Template. 2. Check the length encoded for the BIR index data element. 3. Verify the length of the BIR index data element.
Expected Results	1. Tag '90' may be present and shall not occur more than once. 2. The bytes that follow the Tag '90' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the BIR index data element.

A.3.8.17 Test Case SE_LDS_DG7_018

Test Case-ID	SE_LDS_DG7_018
Purpose	This test checks the presence and encoding of the Biometric Data Block (Tag '5F 2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Biometric Data Block (Tag '5F 2E') inside the Biometric Template. 2. If Tag '5F 2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3. If Tag '5F 2E' is present, verify the length of the Biometric Data Block DO. 4. If Tag '5F 2E' is present, verify that the tag for the Enciphered Biometric Data Block (Tag '7F 2E') is absent. 5. If Tag '5F 2E' is absent, verify that the tag for the Enciphered Biometric Data Block (Tag '7F 2E') is present.
Expected Results	1. Tag '5F 2E' may be present and shall not occur more than once. 2. If Tag '5F 2E' is present, the bytes that follow the Biometric Data Block Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '5F 2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4. If Tag '5F 2E' is present, Tag '7F 2E' shall be absent. 5. If Tag '5F 2E' is absent, Tag '7F 2E' shall be present.

A.3.8.18 Test Case SE_LDS_DG7_019

Test Case-ID	SE_LDS_DG7_019
Purpose	This test checks the presence and encoding of the Enciphered Biometric Data Block (Tag '7F 2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Biometric Data Block (Tag '7F 2E') inside the Biometric Template. 2. If Tag '7F 2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3. If Tag '7F 2E' is present, verify the length of the Enciphered Biometric Data Block DO. 4. If Tag '7F 2E' is present, verify that the tag for the Biometric Data Block (Tag '5F 2E') is absent. 5. If Tag '7F 2E' is absent, verify that the tag for the Biometric Data Block (Tag '5F 2E') is present.
Expected Results	1. Tag '7F 2E' may be present and shall not occur more than once. 2. If Tag '7F 2E' is present, the bytes that follow the Biometric Data Block Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '7F 2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4. If Tag '7F 2E' is present, Tag '5F 2E' shall be absent. 5. If Tag '7F 2E' is absent, Tag '5F 2E' shall be present.

A.3.8.19 Test Case SE_LDS_DG7_020

Test Case-ID	SE_LDS_DG7_020
Purpose	This test checks the encoding of the BIR payload (Tag '53') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BIR payload (Tag '53') inside the Biometric Template. 2. If Tag '53' is present, analyze the encoding of the bytes that follow the BIR payload tag. 3. If Tag '53' is present, verify the length of the BIR payload DO. 4. If Tag '53' is present, verify that the tag '73' is absent.
Expected Results	1. Tag '53' may be present and shall not occur more than once. 2. If Tag '53' is present, the bytes that follow the BIR payload Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '53' is present, the encoded length shall match the size of the BIR payload DO. 4. If Tag '53' is present, Tag '73' shall be absent.

A.3.8.20 Test Case SE_LDS_DG7_021

Test Case-ID	SE_LDS_DG7_021
Purpose	This test checks the encoding of the BIR payload (Tag '73') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C

Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BIR payload (Tag '73') inside the Biometric Template. 2. If Tag '73' is present, analyze the encoding of the bytes that follow the BIR payload tag. 3. If Tag '73' is present, verify the length of the BIR payload DO. 4. If Tag '73' is present, verify that the tag '53' is absent.
Expected Results	1. Tag '73' may be present and shall not occur more than once. 2. If Tag '73' is present, the bytes that follow the BIR payload Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '73' is present, the encoded length shall match the size of the BIR payload DO. 4. If Tag '73' is present, Tag '53' shall be absent.

A.3.8.21 Test Case SE_LDS_DG7_022

Test Case-ID	SE_LDS_DG7_022
Purpose	This test checks the encoding of the Security Block (Tag '5F 3D') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG7
Preconditions	1. EF.DG7 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG7.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Security Block (Tag '5F 3D') inside the Biometric Template. 2. If Tag '5F 3D' is present, analyze the encoding of the bytes that follow the Security Block tag. 3. If Tag '5F 3D' is present, verify the length of the Security Block DO.
Expected Results	1. Tag '5F 3D' may be present and shall not occur more than once. 2. If Tag '5F 3D' is present, the bytes that follow the Security Block Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '5F 3D' is present, the encoded length shall match the size of the Security Block DO.

A.3.9 Test Unit SE_LDS_DG8 – Tests for EF.DG8

Test Unit-ID	SE_LDS_DG8 (Standard Encoding – Data Group 8)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Data Group 8.
References	ISO/IEC 18013-2:2008

A.3.9.1 Test Case SE_LDS_DG8_001

Test Case-ID	SE_LDS_DG8_001
Purpose	This test checks the template tag that the encoded EF.DG8 element starts with.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL.
Test Scenario	1. Check the very first byte of the EF.DG8 element.

Expected Results	1. First byte shall be '76'.

A.3.9.2 Test Case SE_LDS_DG8_002

Test Case-ID	SE_LDS_DG8_002
Purpose	This test checks the encoding of EF.DG8 element length.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL.
Test Scenario	1. Analyze the encoding of the bytes that follow the template tag. 2. Verify the length of the EF.DG8 object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.DG8 object.

A.3.9.3 Test Case SE_LDS_DG8_003

Test Case-ID	SE_LDS_DG8_003
Purpose	This test checks the encoding of the Biometric Group Template (Tag '7F 61') present in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL.
Test Scenario	1. Search for the Biometric Group Template (Tag '7F 61') inside EF.DG8. 2. Check the encoded length of the Biometric Group Template data element. 3. Check the length of the Biometric Group Template data element.
Expected Results	1. Tag '7F 61' shall be present. 2. The bytes that follow the Tag '7F 61' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the Biometric Group Template data element.

A.3.9.4 Test Case SE_LDS_DG8_004

Test Case-ID	SE_LDS_DG8_004
Purpose	This test checks the "Number of Biometric Templates" DO in the "Biometric Group Template" DO (Tag '7F61') in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	1. Search for the Number of Biometric Templates (Tag '02') inside the Biometric Group Template. 2. Analyze the encoding of the length of the Number of Biometric Templates DO coded with tag '02'. 3. Check the value encoded in the Number of Biometric Templates DO.
Expected Results	1. Tag '02' shall be present. 2. The length encoded in the Number of Biometric Templates DO shall be '01'h. 3. The value encoded in the Number of Biometric Templates DO matches the number of occurences of a DO with tag '7F 60' in the Biometric Group Template.

A.3.9.5 Test Case SE_LDS_DG8_005

Test Case-ID	SE_LDS_DG8_005
Purpose	This test checks the encoding of each "Biometric Template" DO in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Analyze the tag of the Biometric Template. 2. Analyze the encoding of the bytes that follow the tag '7F 60'. 3. Verify the length of the DO with Tag '7F 60'.
Expected Results	1. The tag shall be '7F 60'. 2. The bytes that follow the Tag '7F 60' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the DO with the Tag '7F 60'.

A.3.9.6 Test Case SE_LDS_DG8_006

Test Case-ID	SE_LDS_DG8_006
Purpose	This test checks the encoding of the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Biometric Header Template (Tag 'A1') inside the Biometric Template. 2. Analyze the encoding of the bytes that follow the tag 'A1'. 3. Check the length of the Biometric Header Template.
Expected Results	1. Tag 'A1' shall be present. 2. The bytes that follow the Tag 'A1' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the Biometric Header Template.

A.3.9.7 Test Case SE_LDS_DG8_008

Test Case-ID	SE_LDS_DG8_008
Purpose	This test checks the encoding of the Patron Header Version (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Patron Header Version data element with tag '80' is present inside the Biometric Header Template: 1. Search for the Patron Header Version (Tag '80') inside the Biometric Header Template. 2. Check the length encoded for the Patron Header Version data element. 3. Check the value of the Patron Header Version data element.

Expected Results	1. Tag '80' may be present and shall not occur more than once. 2. The encoded length shall be '02'. 3. The Patron Header Version shall have the value '01 01'.

A.3.9.8 Test Case SE_LDS_DG8_009

Test Case-ID	SE_LDS_DG8_009
Purpose	This test checks the encoding of the Biometric Type (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Biometric Type data element with tag '81' is present inside the Biometric Header Template: 1. Search for the Biometric Type (Tag '81') inside the Biometric Header Template. 2. Check the length encoded for the Biometric Type data element. 3. Check the value of the Biometric Type data element.
Expected Results	1. Tag '81' may be present and shall not occur more than once. 2. The encoded length shall be '01'. 3. The Biometric Type shall have the value '10' (Iris).

A.3.9.9 Test Case SE_LDS_DG8_010

Test Case-ID	SE_LDS_DG8_010
Purpose	This test checks the encoding of the Biometric Subtype (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Biometric Subtype data element with tag '82' is present inside the Biometric Header Template: 1. Search for the Biometric Subtype (Tag '82') inside the Biometric Header Template. 2. Check the length encoded for the Biometric Subtype data element. 3. Check the value of the Biometric Subtype data element.
Expected Results	1. Tag '82' may be present and shall not occur more than once. 2. The encoded length shall be '01'. 3. The Biometric Subtype shall have a non-zero value.

A.3.9.10 Test Case SE_LDS_DG8_011

Test Case-ID	SE_LDS_DG8_011
Purpose	This test checks the encoding of the Biometric data creation date and time (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8. 3. The Number of Biometric Templates has been retrieved from the

	Biometric Group Template.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Biometric data creation date and time data element with tag '83' is present inside the Biometric Header Template or if more than one Biometric Template is present inside the Biometric Group Template: 1. Search for the Biometric data creation date and time (Tag '83') inside the Biometric Header Template. 2. Check the length encoded for the Biometric data creation date and time data element. 3. Check the format of the Biometric data creation date and time. 4. Check the value of the Biometric data creation date and time data element.
Expected Results	1. Tag '83' may be present and shall not occur more than once. 2. The encoded length shall be '07'. 3. Date of Issue shall be BCD encoded. 4. The Biometric data creation date and time data element shall represent a valid date/time coded as YYYYMMDDhhmmss.

A.3.9.11 Test Case SE_LDS_DG8_012

Test Case-ID	SE_LDS_DG8_012
Purpose	This test checks the encoding of the BIR Creator (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BIR Creator data element with tag '84' is present inside the Biometric Header Template: 1. Search for the BIR Creator (Tag '84') inside the Biometric Header Template. 2. Check the length encoded for the BIR Creator data element. 3. Verify the length of the BIR Creator data element. 4. Check the format of the BIR Creator data element.
Expected Results	1. Tag '84' may be present and shall not occur more than once. 2. The bytes that follow the Tag '84' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the BIR Creator data element. 4. The BIR Creator shall be encoded as ANS characters.

A.3.9.12 Test Case SE_LDS_DG8_013

Test Case-ID	SE_LDS_DG8_013
Purpose	This test checks the encoding of the BDB Validity Period (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BDB Validity Period data element with tag '85' is present inside the Biometric Header Template: 1. Search for the BDB Validity Period (Tag '85') inside the Biometric Header Template. 2. Check the length encoded for the BDB Validity Period data element. 3. Check the format of the BDB Validity Period. 4. Check the value of the BDB Validity Period data element. 5. Check the consistency of the value of the BDB Validity Period data element.
Expected Results	1. Tag '85' may be present and shall not occur more than once. 2. The encoded length shall be '08'. 3. The BDB Validity Period shall be BCD encoded. 4. The BDB Validity Period shall represent a valid effective date and a valid expiry date coded as YYYYMMDDYYYYMMDD. 5. The BDB Validity Period effective date shall represent an effective date BEFORE the expiry date.

A.3.9.13 Test Case SE_LDS_DG8_014

Test Case-ID	SE_LDS_DG8_014
Purpose	This test checks the encoding of the BDB Product Owner, Product Type

	(if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 19785-1:2006
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BDB Product Owner, Product Type data element with tag '86' is present inside the Biometric Header Template: 1. Search for the BDB Product Owner, Product Type (Tag '86') inside the Biometric Header Template. 2. Check the length encoded for the BDB Product Owner, Product Type data element. 3. Check the value of the BDB Product Owner, Product Type data element. 4. Check the consistency of the BDB Product Owner, Product Type data element.
Expected Results	1. Tag '86' may be present and shall not occur more than once. 2. The encoded length shall be '04'. 3. The BDB Product Owner, Product Type shall be a concatenation of two 16-bit POSITIVE integers. 4. The BDB Product Owner, Product Type shall have be a valid combination of product owner and product type as defined in ISO/IEC 19785-1:2006, 6.5.12 and 6.5.13.

A.3.9.14 Test Case SE_LDS_DG8_015

Test Case-ID	SE_LDS_DG8_015
Purpose	This test checks the encoding of the BDB Format Owner in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 19785-1:2006
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BDB Format Owner (Tag '87') inside the Biometric Header Template. 2. Check the length encoded for the BDB Format Owner data element. 3. Check the value of the BDB Format Owner data element. 4. Check the validity of the BDB Format Owner data element.
Expected Results	1. Tag '87' shall be present. 2. The encoded length shall be '02'. 3. The BDB Format Owner shall be a 16-bit POSITIVE integer. 4. The BDB Format Owner shall have be a valid format owner as defined in ISO/IEC 19785-1:2006, 6.5.1.

A.3.9.15 Test Case SE_LDS_DG8_016

Test Case-ID	SE_LDS_DG8_016
Purpose	This test checks the encoding of the BDB Format Type in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C

	ISO/IEC 19785-1:2006
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BDB Format Type (Tag '88') inside the Biometric Header Template. 2. Check the length encoded for the BDB Format Type data element. 3. Check the value of the BDB Format Type data element. 4. Check the validity of the BDB Format Type data element. 5. Check the consistency of the BDB Format Type data element with the BDB format owner data element.
Expected Results	1. Tag '88' shall be present. 2. The encoded length shall be '02'. 3. The BDB Format Type shall be a 16-bit POSITIVE integer. 4. The BDB Format Type shall have be a valid format type as defined in ISO/IEC 19785-1:2006, 6.5.2. 5. The BDB Format Type shall be valid in combination with the format owner data element.

A.3.9.16 Test Case SE_LDS_DG8_017

Test Case-ID	SE_LDS_DG8_017
Purpose	This test checks the encoding of the BIR index (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BIR index data element with tag '90' is present within the Biometric Header Template: 1. Search for the BIR index (Tag '90') inside the Biometric Header Template. 2. Check the length encoded for the BIR index data element. 3. Verify the length of the BIR index data element.
Expected Results	1. Tag '90' may be present and shall not occur more than once. 2. The bytes that follow the Tag '90' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the BIR index data element.

A.3.9.17 Test Case SE_LDS_DG8_018

Test Case-ID	SE_LDS_DG8_018
Purpose	This test checks the presence and encoding of the Biometric Data Block (Tag '5F 2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Biometric Data Block (Tag '5F 2E') inside the Biometric Template. 2. If Tag '5F 2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3. If Tag '5F 2E' is present, verify the length of the Biometric Data Block DO. 4. If Tag '5F 2E' is present, verify that the tag for the Enciphered Biometric Data Block (Tag '7F 2E') is absent. 5. If Tag '5F 2E' is absent, verify that the tag for the Enciphered Biometric Data Block (Tag '7F 2E') is present.
Expected Results	1. Tag '5F 2E' may be present and shall not occur more than once. 2. If Tag '5F 2E' is present, the bytes that follow the Biometric Data Block Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '5F 2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4. If Tag '5F 2E' is present, Tag '7F 2E' shall be absent. 5. If Tag '5F 2E' is absent, Tag '7F 2E' shall be present.

A.3.9.18 Test Case SE_LDS_DG8_019

Test Case-ID	SE_LDS_DG8_019
Purpose	This test checks the presence and encoding of the Enciphered Biometric Data Block (Tag '7F 2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Biometric Data Block (Tag '7F 2E') inside the Biometric Template. 2. If Tag '7F 2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3. If Tag '7F 2E' is present, verify the length of the Enciphered Biometric Data Block DO. 4. If Tag '7F 2E' is present, verify that the tag for the Biometric Data Block (Tag '5F 2E') is absent. 5. If Tag '7F 2E' is absent, verify that the tag for the Biometric Data Block (Tag '5F 2E') is present.
Expected Results	1. Tag '7F 2E' may be present and shall not occur more than once. 2. If Tag '7F 2E' is present, the bytes that follow the Biometric Data Block Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '7F 2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4. If Tag '7F 2E' is present, Tag '5F 2E' shall be absent.

	5. If Tag '7F 2E' is absent, Tag '5F 2E' shall be present.

A.3.9.19 Test Case SE_LDS_DG8_020

Test Case-ID	SE_LDS_DG8_020
Purpose	This test checks the encoding of the BIR payload (Tag '53') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BIR payload (Tag '53') inside the Biometric Template. 2. If Tag '53' is present, analyze the encoding of the bytes that follow the BIR payload tag. 3. If Tag '53' is present, verify the length of the BIR payload DO. 4. If Tag '53' is present, verify that the tag '73' is absent.
Expected Results	1. Tag '53' may be present and shall not occur more than once. 2. If Tag '53' is present, the bytes that follow the BIR payload Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '53' is present, the encoded length shall match the size of the BIR payload DO. 4. If Tag '53' is present, Tag '73' shall be absent.

A.3.9.20 Test Case SE_LDS_DG8_021

Test Case-ID	SE_LDS_DG8_021
Purpose	This test checks the encoding of the BIR payload (Tag '73') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BIR payload (Tag '73') inside the Biometric Template. 2. If Tag '73' is present, analyze the encoding of the bytes that follow the BIR payload tag. 3. If Tag '73' is present, verify the length of the BIR payload DO. 4. If Tag '73' is present, verify that the tag '53' is absent.
Expected Results	1. Tag '73' may be present and shall not occur more than once. 2. If Tag '73' is present, the bytes that follow the BIR payload Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '73' is present, the encoded length shall match the size of the BIR payload DO. 4. If Tag '73' is present, Tag '53' shall be absent.

A.3.9.21 Test Case SE_LDS_DG8_022

Test Case-ID	SE_LDS_DG8_022
Purpose	This test checks the encoding of the Security Block (Tag '5F 3D') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG8
Preconditions	1. EF.DG8 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG8.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Security Block (Tag '5F 3D') inside the Biometric Template. 2. If Tag '5F 3D' is present, analyze the encoding of the bytes that follow the Security Block tag. 3. If Tag '5F 3D' is present, verify the length of the Security Block DO.
Expected Results	1. Tag '5F 3D' may be present and shall not occur more than once. 2. If Tag '5F 3D' is present, the bytes that follow the Security Block Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '5F 3D' is present, the encoded length shall match the size of the Security Block DO.

A.3.10 Test Unit SE_LDS_DG9 – Tests for EF.DG9

Test Unit-ID	SE_LDS_DG9 (Standard Encoding – Data Group 9)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Data Group 9.
References	ISO/IEC 18013-2:2008

A.3.10.1 Test Case SE_LDS_DG9_001

Test Case-ID	SE_LDS_DG9_001
Purpose	This test checks the template tag that the encoded EF.DG9 element

	starts with.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL.
Test Scenario	1. Check the very first byte of the EF.DG9 element.
Expected Results	1. First byte shall be '70'.

A.3.10.2 Test Case SE_LDS_DG9_002

Test Case-ID	SE_LDS_DG9_002
Purpose	This test checks the encoding of EF.DG9 element length.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL.
Test Scenario	1. Analyze the encoding of the bytes that follow the template tag. 2. Verify the length of the EF.DG9 object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.DG9 object.

A.3.10.3 Test Case SE_LDS_DG9_003

Test Case-ID	SE_LDS_DG9_003
Purpose	This test checks the encoding of the Biometric Group Template (Tag '7F 61') present in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL.
Test Scenario	1. Search for the Biometric Group Template (Tag '7F 61') inside EF.DG9. 2. Check the encoded length of the Biometric Group Template data element. 3. Check the length of the Biometric Group Template data element.
Expected Results	1. Tag '7F 61' shall be present. 2. The bytes that follow the Tag '7F 61' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the Biometric Group Template data element.

A.3.10.4 Test Case SE_LDS_DG9_004

Test Case-ID	SE_LDS_DG9_004
Purpose	This test checks the "Number of Biometric Templates" DO in the "Biometric Group Template" DO (Tag '7F61') in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	1. Search for the Number of Biometric Templates (Tag '02') inside the Biometric Group Template. 2. Analyze the encoding of the length of the Number of Biometric Templates DO coded with tag '02'. 3. Check the value encoded in the Number of Biometric Templates DO.
Expected Results	1. Tag '02' shall be present. 2. The length encoded in the Number of Biometric Templates DO shall

	be '01'h. 3. The value encoded in the Number of Biometric Templates DO matches the number of occurences of a DO with tag '7F 60' in the Biometric Group Template.

A.3.10.5 Test Case SE_LDS_DG9_005

Test Case-ID	SE_LDS_DG9_005
Purpose	This test checks the encoding of each "Biometric Template" DO in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Analyze the tag of the Biometric Template. 2. Analyze the encoding of the bytes that follow the tag '7F 60'. 3. Verify the length of the DO with Tag '7F 60'.
Expected Results	1. The tag shall be '7F 60'. 2. The bytes that follow the Tag '7F 60' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the DO with the Tag '7F 60'.

A.3.10.6 Test Case SE_LDS_DG9_006

Test Case-ID	SE_LDS_DG9_006
Purpose	This test checks the encoding of the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Biometric Header Template (Tag 'A1') inside the Biometric Template. 2. Analyze the encoding of the bytes that follow the tag 'A1'. 3. Check the length of the Biometric Header Template.
Expected Results	1. Tag 'A1' shall be present. 2. The bytes that follow the Tag 'A1' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the Biometric Header Template.

A.3.10.7 Test Case SE_LDS_DG9_008

Test Case-ID	SE_LDS_DG9_008
Purpose	This test checks the encoding of the Patron Header Version (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Patron Header Version data element with tag '80' is present inside the Biometric Header Template:

	1. Search for the Patron Header Version (Tag '80') inside the Biometric Header Template. 2. Check the length encoded for the Patron Header Version data element. 3. Check the value of the Patron Header Version data element.
Expected Results	1. Tag '80' may be present and shall not occur more than once. 2. The encoded length shall be '02'. 3. The Patron Header Version shall have the value '01 01'.

A.3.10.8 Test Case SE_LDS_DG9_009

Test Case-ID	SE_LDS_DG9_009
Purpose	This test checks the encoding of the Biometric Type (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 19785-3:2007
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Biometric Type data element with tag '81' is present inside the Biometric Header Template : 1. Search for the Biometric Type (Tag '81') inside the Biometric Header Template. 2. Check the length encoded for the Biometric Type data element. 3. Check the value of the Biometric Type data element.
Expected Results	1. Tag '81' may be present and shall not occur more than once. 2. The encoded length shall be '01' - '03'. 3. The Biometric Type shall have the valid value according to ISO/IEC 19785-3:2007.

A.3.10.9 Test Case SE_LDS_DG9_010

Test Case-ID	SE_LDS_DG9_010
Purpose	This test checks the encoding of the Biometric Subtype (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Biometric Subtype data element with tag '82' is present inside the Biometric Header Template: 1. Search for the Biometric Subtype (Tag '82') inside the Biometric Header Template. 2. Check the length encoded for the Biometric Subtype data element. 3. Check the value of the Biometric Subtype data element.
Expected Results	1. Tag '82' may be present and shall not occur more than once. 2. The encoded length shall be '01'. 3. The Biometric Subtype shall have a non-zero value.

A.3.10.10 Test Case SE_LDS_DG9_011

Test Case-ID	SE_LDS_DG9_011
Purpose	This test checks the encoding of the Biometric data creation date and time (if present) in the Biometric Header Template (Tag 'A1') in each

	"Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9. 3. The Number of Biometric Templates has been retrieved from the Biometric Group Template.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) Biometric data creation date and time data element with tag '83' is present inside the Biometric Header Template or if more than one Biometric Template is present inside the Biometric Group Template: 1. Search for the Biometric data creation date and time (Tag '83') inside the Biometric Header Template. 2. Check the length encoded for the Biometric data creation date and time data element. 3. Check the format of the Biometric data creation date and time. 4. Check the value of the Biometric data creation date and time data element.
Expected Results	1. Tag '83' may be present and shall not occur more than once. 2. The encoded length shall be '07'. 3. Date of Issue shall be BCD encoded. 4. The Biometric data creation date and time data element shall represent a valid date/time coded as YYYYMMDDhhmmss.

A.3.10.11 Test Case SE_LDS_DG9_012

Test Case-ID	SE_LDS_DG9_012
Purpose	This test checks the encoding of the BIR Creator (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BIR Creator data element with tag '84' is present inside the Biometric Header Template : 1. Search for the BIR Creator (Tag '84') inside the Biometric Header Template. 2. Check the length encoded for the BIR Creator data element. 3. Verify the length of the BIR Creator data element. 4. Check the format of the BIR Creator data element.
Expected Results	1. Tag '84' may be present and shall not occur more than once. 2. The bytes that follow the Tag '84' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the BIR Creator data element. 4. The BIR Creator shall be encoded as ANS characters.

A.3.10.12 Test Case SE_LDS_DG9_013

Test Case-ID	SE_LDS_DG9_013
Purpose	This test checks the encoding of the BDB Validity Period (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BDB Validity Period data element with tag '85' is present inside the Biometric Header Template: 1. Search for the BDB Validity Period (Tag '85') inside the Biometric Header Template. 2. Check the length encoded for the BDB Validity Period data element. 3. Check the format of the BDB Validity Period. 4. Check the value of the BDB Validity Period data element. 5. Check the consistency of the value of the BDB Validity Period data element.
Expected Results	1. Tag '85' may be present and shall not occur more than once. 2. The encoded length shall be '08'. 3. The BDB Validity Period shall be BCD encoded. 4. The BDB Validity Period shall represent a valid effective date and a valid expiry date coded as YYYYMMDDYYYYMMDD. 5. The BDB Validity Period effective date shall represent an effective date BEFORE the expiry date.

A.3.10.13 Test Case SE_LDS_DG9_014

Test Case-ID	SE_LDS_DG9_014
Purpose	This test checks the encoding of the BDB Product Owner, Product Type (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 19785-1:2006
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BDB Product Owner, Product Type data element with tag '86' is present inside the Biometric Header Template: 1. Search for the BDB Product Owner, Product Type (Tag '86') inside the Biometric Header Template. 2. Check the length encoded for the BDB Product Owner, Product Type data element. 3. Check the value of the BDB Product Owner, Product Type data element. 4. Check the consistency of the BDB Product Owner, Product Type data element.
Expected Results	1. Tag '86' may be present and shall not occur more than once. 2. The encoded length shall be '04'. 3. The BDB Product Owner, Product Type shall be a concatenation of two 16-bit POSITIVE integers. 4. The BDB Product Owner, Product Type shall have be a valid combination of product owner and product type as defined in ISO/IEC 19785-1:2006, 6.5.12 and 6.5.13.

A.3.10.14 Test Case SE_LDS_DG9_015

Test Case-ID	SE_LDS_DG9_015
Purpose	This test checks the encoding of the BDB Format Owner in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 19785-1:2006
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BDB Format Owner (Tag '87') inside the Biometric Header Template. 2. Check the length encoded for the BDB Format Owner data element. 3. Check the value of the BDB Format Owner data element. 4. Check the validity of the BDB Format Owner data element.
Expected Results	1. Tag '87' shall be present. 2. The encoded length shall be '02'. 3. The BDB Format Owner shall be a 16-bit POSITIVE integer. 4. The BDB Format Owner shall have be a valid format owner as defined in ISO/IEC 19785-1:2006, 6.5.1.

A.3.10.15 Test Case SE_LDS_DG9_016

Test Case-ID	SE_LDS_DG9_016
Purpose	This test checks the encoding of the BDB Format Type in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 19785-1:2006
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BDB Format Type (Tag '88') inside the Biometric Header Template. 2. Check the length encoded for the BDB Format Type data element. 3. Check the value of the BDB Format Type data element. 4. Check the validity of the BDB Format Type data element. 5. Check the consistency of the BDB Format Type data element with the BDB format owner data element.
Expected Results	1. Tag '88' shall be present. 2. The encoded length shall be '02'. 3. The BDB Format Type shall be a 16-bit POSITIVE integer. 4. The BDB Format Type shall have be a valid format type as defined in ISO/IEC 19785-1:2006, 6.5.2. 5. The BDB Format Type shall be valid in combination with the format owner data element.

A.3.10.16 Test Case SE_LDS_DG9_017

Test Case-ID	SE_LDS_DG9_017
Purpose	This test checks the encoding of the BIR index (if present) in the Biometric Header Template (Tag 'A1') in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0

References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	For each "Biometric Template", perform the following checks if the (optional) BIR index data element with tag '90' is present inside the Biometric Header Template : 1. Search for the BIR index (Tag '90') inside the Biometric Header Template. 2. Check the length encoded for the BIR index data element. 3. Verify the length of the BIR index data element.
Expected Results	1. Tag '90' may be present and shall not occur more than once. 2. The bytes that follow the Tag '90' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the BIR index data element.

A.3.10.17 Test Case SE_LDS_DG9_018

Test Case-ID	SE_LDS_DG9_018
Purpose	This test checks the presence and encoding of the Biometric Data Block (Tag '5F 2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Biometric Data Block (Tag '5F 2E') inside the Biometric Template. 2. If Tag '5F 2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3. If Tag '5F 2E' is present, verify the length of the Biometric Data Block DO. 4. If Tag '5F 2E' is present, verify that the tag for the Enciphered Biometric Data Block (Tag '7F 2E') is absent. 5. If Tag '5F 2E' is absent, verify that the tag for the Enciphered Biometric Data Block (Tag '7F 2E') is present.
Expected Results	1. Tag '5F 2E' may be present and shall not occur more than once. 2. If Tag '5F 2E' is present, the bytes that follow the Biometric Data Block Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '5F 2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4. If Tag '5F 2E' is present, Tag '7F 2E' shall be absent. 5. If Tag '5F 2E' is absent, Tag '7F 2E' shall be present.

A.3.10.18 Test Case SE_LDS_DG9_019

Test Case-ID	SE_LDS_DG9_019
Purpose	This test checks the presence and encoding of the Enciphered Biometric Data Block (Tag '7F 2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the Biometric Data Block (Tag '7F 2E') inside the Biometric Template. 2. If Tag '7F 2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3. If Tag '7F 2E' is present, verify the length of the Enciphered Biometric Data Block DO. 4. If Tag '7F 2E' is present, verify that the tag for the Biometric Data Block (Tag '5F 2E') is absent. 5. If Tag '7F 2E' is absent, verify that the tag for the Biometric Data Block (Tag '5F 2E') is present.
Expected Results	1. Tag '7F 2E' may be present and shall not occur more than once. 2. If Tag '7F 2E' is present, the bytes that follow the Biometric Data Block Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '7F 2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4. If Tag '7F 2E' is present, Tag '5F 2E' shall be absent.

	5. If Tag '7F 2E' is absent, Tag '5F 2E' shall be present.

A.3.10.19 Test Case SE_LDS_DG9_020

Test Case-ID	SE_LDS_DG9_020
Purpose	This test checks the encoding of the BIR payload (Tag '53') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BIR payload (Tag '53') inside the Biometric Template. 2. If Tag '53' is present, analyze the encoding of the bytes that follow the BIR payload tag. 3. If Tag '53' is present, verify the length of the BIR payload DO. 4. If Tag '53' is present, verify that the tag '73' is absent.
Expected Results	1. Tag '53' may be present and shall not occur more than once. 2. If Tag '53' is present, the bytes that follow the BIR payload Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '53' is present, the encoded length shall match the size of the BIR payload DO. 4. If Tag '53' is present, Tag '73' shall be absent.

A.3.10.20 Test Case SE_LDS_DG9_021

Test Case-ID	SE_LDS_DG9_021
Purpose	This test checks the encoding of the BIR payload (Tag '73') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	Perform the following checks for each "Biometric Template": 1. Search for the BIR payload (Tag '73') inside the Biometric Template. 2. If Tag '73' is present, analyze the encoding of the bytes that follow the BIR payload tag. 3. If Tag '73' is present, verify the length of the BIR payload DO. 4. If Tag '73' is present, verify that the tag '53' is absent.
Expected Results	1. Tag '73' may be present and shall not occur more than once. 2. If Tag '73' is present, the bytes that follow the BIR payload Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '73' is present, the encoded length shall match the size of the BIR payload DO. 4. If Tag '73' is present, Tag '53' shall be absent.

A.3.10.21 Test Case SE_LDS_DG9_022

Test Case-ID	SE_LDS_DG9_022
Purpose	This test checks the encoding of the Security Block (Tag '5F 3D') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG9
Preconditions	1. EF.DG9 has been retrieved from the IDL. 2. The Biometric Group Template has been retrieved from EF.DG9.
Test Scenario	Perform the following checks for each "Biometric Template":

	1. Search for the Security Block (Tag '5F 3D') inside the Biometric Template. 2. If Tag '5F 3D' is present, analyze the encoding of the bytes that follow the Security Block tag. 3. If Tag '5F 3D' is present, verify the length of the Security Block DO.
Expected Results	1. Tag '5F 3D' may be present and shall not occur more than once. 2. If Tag '5F 3D' is present, the bytes that follow the Security Block Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3. If Tag '5F 3D' is present, the encoded length shall match the size of the Security Block DO.

A.3.11 Test Unit SE_LDS_SOD – Tests for EF.SOD

Test Unit-ID	SE_LDS_SOD (Standard Encoding – Document Security Object)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Security Object.
References	ISO/IEC 18013-2:2008 ISO/IEC 18013-3:2009

A.3.11.1 Test Case SE_LDS_SOD_001

Test Case-ID	SE_LDS_SOD_001
Purpose	This test checks the template tag; the encoded EF.SOD element starts with.
Version	1.0
References	ISO/IEC 18013-3:2009
Profile	PA
Preconditions	1. EF.SOD has been retrieved from the IDL.
Test Scenario	1. Check the very first byte of the EF.SOD element.
Expected Results	1. First byte shall be '77'.

A.3.11.2 Test Case SE_LDS_SOD_002

Test Case-ID	SE_LDS_SOD_002
Purpose	This test checks the encoding of EF.SOD element length.
Version	1.0
References	ISO/IEC 18013-3:2009
Profile	PA
Preconditions	1. EF.SOD has been retrieved from the IDL.
Test Scenario	1. Analyze the encoding of the bytes that follow the template tag. 2. Verify the length of the EF.SOD object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.SOD object.

A.3.11.3 Test Case SE_LDS_SOD_003

Test Case-ID	SE_LDS_SOD_003
Purpose	This test checks the ASN#1 encoding of the PCKS#7 signedData object.
Version	1.0
References	ISO/IEC 18013-3:2009 RFC-3369
Profile	PA
Preconditions	1. EF.SOD has been retrieved from the IDL.
Test Scenario	1. Analyze the ASN.1 encoding of the content of EF.SOD. 2. Analyze the value of the EF.SOD template.
Expected Results	1. The signedData object shall be DER encoded. 2. The value of the the EF.SOD template shall be a ContentInfo data element of the SignedData Type as specified in RFC 3369.

A.3.11.4 Test Case SE_LDS_SOD_004

Test Case-ID	SE_LDS_SOD_004
Purpose	This test checks the value encoded in the signedData element.
Version	1.0
References	ISO/IEC 18013-3:2009 RFC-3369
Profile	PA
Preconditions	1. EF.SOD has been retrieved from the IDL. 2. The SignedData field has been retrieved from the ContentInfo DO in EF.SOD.
Test Scenario	1. Check the SignedData version value (Tag '02'). 2. Check the digestAlgorithms list (Tag '31'). 3. Check the eContentType (Tag '06'). 4. Check the certificates list (Tag 'A0'). 5. Check the Certificate Revocation Lists (Tag 'A1').
Expected Results	1. The version shall be 3. 2. The digestAlgorithms list may contain all used digestAlgorithms in the signedData. The digestAlgorithms list shall not contain other digest algorithms than those specified in ISO/IEC 18013-3:2009 8.1.4. 3. The eContentType shall have OID as specified in ISO/IEC 18013-3:2009. 4. Tag 'A0' may be present and shall occur only once. 5. Tag 'A1' shall be absent.

A.3.11.5 Test Case SE_LDS_SOD_005

Test Case-ID	SE_LDS_SOD_005
Purpose	This test checks the SignerInfo element of the signedData structure.
Version	1.0
References	ISO/IEC 18013-3:2009 RFC-3369
Profile	PA
Preconditions	1. EF.SOD has been retrieved from the IDL. 2. The SignedData field has been retrieved from the ContentInfo DO in EF.SOD.
Test Scenario	Perform the following checks for each entry of the "signerInfos" field in the signedData structure: 1. Check the signer info version (Tag '02'). 2. Check the choice in the sid field (first instance of Tag '30'). 3. Check the certificate identified in the sid field. 4. Check the digestAlgorithm field (second instance of Tag '30'). 5. Check the presence of the Digest Algorithm Identifier in the digestAlgorithmlist of the signedData element. 6. Check the signedAttrs element (Tag 'A0').

	7. Check the value of the signedAttrs element. 8. Check the value of the signedAttrs element. 9. Check the message-digest Attribute. 10. Check the content-type Attribute. 11. Check the SigningTime attribute if present. 12. Check the signatureAlgorithm element. 13. Check the signature element.
Expected Results	1. The version shall be 1 or 3. 2. The sid field shall match the signer info version value. (version 1 if issuerandSerialNumber is used and 3 if subjectKeyIdentifier is used). 3. The certificate identified in the sid field shall be included in the signed data certificates list or shall be available in the PKD. 4. The digestAlgorithms list shall be one of the algorithms specified in ISO/IEC 18013-3:2009 8.1.4 (i.e. only the following algorithms are allowed: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512). 5. The digestAlgorithm should be included in the digestAlgorithmlist of the signedData element. 6. Tag 'A0' shall be present and shall occur only once. 7. The signed attributes list shall contain the message-digest attribute. 8. The signed attributes list shall contain the content-type attribute. 9. The value of the message-digest attribute shall match the hash value of the eContent element (using the digestAlgorithm specified above). 10. The content-type attribute value shall match the encapContentInfo eContentType value in the signed-data. 11. The signing time shall be within the validity period of the signing certificate. 12. The signature algorithm shall refer to an algorithm specified in ISO/IEC 18013-3:2009 (i.e. the algorithm shall be using RSASSA-PSS, RSASSA-PKCS1-v1.5, or ECDSA). 13. The signature shall be valid.

A.3.11.6 Test Case SE_LDS_SOD_006

Test Case-ID	SE_LDS_SOD_006
Purpose	This test checks the LDS Security Object stored as eContent in the signedData Object.
Version	1.0
References	ISO/IEC 18013-3:2009 RFC 3369
Profile	PA
Preconditions	1. EF.SOD has been retrieved from the IDL. 2. The SignedData field has been retrieved from the ContentInfo DO in EF.SOD.
Test Scenario	1. Check the ASN.1 encoding of the LDS Security Object. 2. Check the encoding of the LDS Security Object. 3. Check the LDS Security Object version (Tag '02'). 4. Check the digestAlgorithm identifier. 5. Check the DataGroupHash Sequence. 6. Check the dataGroup numbers in the DataGroup Hash Sequence. 7. Check the dataGroup numbers in the DataGroup Hash Sequence. 8. Check the dataGroup hash values in the Hash Sequence.
Expected Results	1. The LDS Security Object shall be DER encoded. 2. The encoding of the LDS Security Object shall follow the ASN1.1 encoding specified in ISO/IEC 18013-3:2009. 3. The version shall be 0. 4. The digestAlgorithms list shall be one of the digest algorithms specified in ISO/IEC 18013-3:2009 8.1.4 (i.e. SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512). 5. The Hash Sequence shall contains at least the entries for DG 1.

	6. The Hash Sequence shall contain a hash value for all present data groups. The Hash Sequence shall not conatin additional hash value for non-existing data groups. 7. The referred data groups shall match the Data Group list in the EF.COM. 8. All hash values shall be valid.

A.3.11.7 Test Case SE_LDS_SOD_007

Test Case-ID	SE_LDS_SOD_007
Purpose	This test checks the signing certificate used to verify the EF.SOD object.
Version	1.0
References	ISO/IEC 18013-3:2009 RFC-3280
Profile	PA
Preconditions	1. EF.SOD has been retrieved from the IDL. 2. The SignedData field has been retrieved from the ContentInfo DO in EF.SOD. 3. The Signing Certificate has been retrieved (from the SignedData structure or from the PKD). 4. The Issuing Authority Certificate has been retrieved.
Test Scenario	1. Check the ASN.1 encoding of the signing certificate. 2. Check the ASN.1 structure of the signing certificate. 3. Check the signing certificate version. 4. Check the signature field of the certificate. 5. Check the certificates validity period. 6. Check the certificates issuer element. 7. Check the subjectPublicKeyInfo element. 8. Check the AKID extension in the signing certificate. 9. Check that the the SubjectKeyIdentifier extension of the country signing certificate. 10. Check the keyUsage extension of the signing certificate. 11. Check the signatureAlgorithm element. 12. Verify the signatureValue of the signing certificate with the public key of the Issuing Authority certificate.
Expected Results	1. The signing certificate shall be DER encoded. 2. The signing certificate shall be encoded as specified in RFC 3280. 3. The version shall be 2. 4. The algorithm indicated in the signature element shall match the OID in the signatureAlgorithm field. 5. The validity period shall use UTC time for dates until 2049 and shall use GeneralisedTime for dates after 2049 inclusive. (NOTE: It is not necessary that the certificate is still valid; it shall only have been valid at signing time). 6. The issuer shall match the subject of the provided country signing certificate. 7. The algorithm identifier in the subjectPublicKeyInfo shall refer to a algorithm specified in ISO/IEC 18013-3:2009 (i.e. the algorithm shall be using RSASSA-PSS, RSASSA-PKCS1-v1.5, or ECDSA). 8. The AKID extension shall be present and shall contain a keyIdentifier value. 9. The SubjectKeyIdentifier extension shall match the AKID of the signing certificate. 10. The keyUsage extension shall be matked critical and only the digitalSignature bit shall be set. 11. The signatureAlgorithm shall indicate one of the algorithms specified in ISO/IEC 18013-3:2009 (i.e. the algorithm shall be using RSASSA-PSS, RSASSA-PKCS1-v1.5, or ECDSA). 12. Verification shall be successful.

A.3.12 Test Unit SE_LDS_DG12 – Tests for EF.DG12

Test Unit-ID	SE_LDS_DG12 (Standard Encoding – Data Group 12)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Data Group 12.
References	ISO/IEC 18013-2:2008 ISO/IEC 18013-3:2009

A.3.12.1 Test Case SE_LDS_DG12_001

Test Case-ID	SE_LDS_DG12_001
Purpose	This test checks the template tag that the encoded EF.DG12 element starts with.
Version	1.0
References	ISO/IEC 18013-3:2009
Profile	NMA
Preconditions	1. EF.DG12 has been retrieved from the IDL.
Test Scenario	1. Check the very first byte of the EF.DG12 element.
Expected Results	1. First byte shall be '71'.

A.3.12.2 Test Case SE_LDS_DG12_002

Test Case-ID	SE_LDS_DG12_002
Purpose	This test checks the encoding of EF.DG12 element length.
Version	1.0
References	ISO/IEC 18013-3:2009
Profile	NMA
Preconditions	1. EF.DG12 has been retrieved from the IDL.
Test Scenario	1. Analyze the encoding of the bytes that follow the template tag. 2. Verify the length of the EF.DG12 object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.DG12 object.

A.3.12.3 Test Case SE_LDS_DG12_003

Test Case-ID	SE_LDS_DG12_003
Purpose	This test checks the encoding of the SAI Reference String (Tag '82') present in EF.DG12.
Version	1.0
References	ISO/IEC 18013-3:2009 ISO/IEC 8859-1
Profile	NMA
Preconditions	1. EF.DG12 has been retrieved from the IDL.
Test Scenario	1. Search for the SAI Reference String (Tag '82') inside EF.DG12. 2. Check the encoded length of the SAI Reference String data element. 3. Check the length of the SAI Reference String data element. 4. Check the value of the SAI Reference String. 5. If the SAI Reference String starts with '00', check the value of the subsequent bytes of the SAI Reference String. 6. If the SAI Reference String starts with '01', check the value of the subsequent bytes of the SAI Reference String. 7. If the SAI Reference String starts with '01', check the value of the subsequent bytes of the SAI Reference String. 8. If the SAI Reference String starts with '01', check the value of the subsequent bytes of the SAI Reference String.
Expected Results	1. Tag '82' shall be present. 2. The bytes that follow the Tag '82' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the SAI Reference String data element. 4. The first byte of the SAI Reference String shall be '00' or '01'. 5. The subsequent bytes of the SAI Reference String shall be encoded in accordance with ISO/IEC 8859-1. 6. The subsequent bytes of the SAI Reference String shall be 2 BCD encoded bytes. 7. The second byte of the SAI Reference String shall refer to an existing Data Group in the IDL. 8. The third byte of the SAI Reference String shall refer to a field in an existing Data Group in the IDL that is available outside the ICC (i.e. DG1 Field 1..9, DG2 Field 1..7), or DG3 Field 1..4).

A.3.12.4 Test Case SE_LDS_DG12_004

Test Case-ID	SE_LDS_DG12_004
Purpose	This test checks the encoding of the SAI Input Method (Tag '81') present in EF.DG12.
Version	1.0
References	ISO/IEC 18013-3:2009
Profile	NMA
Preconditions	1. EF.DG12 has been retrieved from the IDL.
Test Scenario	1. Search for the SAI Input Method (Tag '81') inside EF.DG12. 2. Check the encoded length of the SAI Input Method data element, if present. 3. Check the length of the SAI Input Method data element. 4. Check the value of the SAI Input Method. 5. Check the value of the SAI Input Method. 6. If the SAI Input Method starts with '02', check the presence of byte 2 of the SAI Input Method. 7. Check the value of byte 2 of the SAI Input Method. 8. Check the value of byte 3 of the SAI Input Method, if present. 9. Check the value of the bytes 4 - 7 of the SAI Input Method, if present. 10. Check the consistency of the bytes 4 and 6 of the SAI Input Method, if present. 11. Check the consistency of the bytes 5 and 7 of the SAI Input Method,

	if present.
Expected Results	1. Tag '81' may be present and shall not occur more than once. 2. The encoded length shall be '01', '02', or '07'. 3. The encoded length shall match the size of the SAI Input Method data element. 4. The first nibble of byte 1 of the SAI Input Method shall be '0', '1' or '2'. 5. The second nibble of byte 1 of the SAI Input Method shall be '0', '1' or '2'. 6. Byte 2 of the SAI Input Method shall be present. 7. Byte 2 of the SAI Input Method shall have one of the following values : '00', '01', '02', '03', 'FE', or 'FF'. 8. Byte 3 of the SAI Input Method shall have the value '00' or '01'. 9. Byte 4 - 7 of the SAI Input Method shall be BCD encoded. 10. Byte 4 of the SAI Input Method shall be smaller than byte 6 of the SAI Input Method. 11. Byte 7 of the SAI Input Method shall be smaller than byte 5 of the SAI Input Method.

A.3.13 Test Unit SE_LDS_DG13 – Tests for EF.DG13

Test Unit-ID	SE_LDS_DG13 (Standard Encoding – Data Group 13)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Data Group 13.
References	ISO/IEC 18013-2:2008 ISO/IEC 18013-3:2009

A.3.13.1 Test Case SE_LDS_DG13_001

Test Case-ID	SE_LDS_DG13_001
Purpose	This test checks the template tag that the encoded EF.DG13 element starts with.
Version	1.0
References	ISO/IEC 18013-3:2009
Profile	AA
Preconditions	1. EF.DG13 has been retrieved from the IDL.
Test Scenario	1. Check the very first byte of the EF.DG13 element.
Expected Results	1. First byte shall be '6F'.

A.3.13.2 Test Case SE_LDS_DG13_002

Test Case-ID	SE_LDS_DG13_002
Purpose	This test checks the encoding of EF.DG13 element length.
Version	1.0
References	ISO/IEC 18013-3:2009
Profile	AA
Preconditions	1. EF.DG13 has been retrieved from the IDL.
Test Scenario	1. Analyze the encoding of the bytes that follow the template tag. 2. Verify the length of the EF.DG13 object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.DG13 object.

A.3.13.3 Test Case SE_LDS_DG13_003

Test Case-ID	SE_LDS_DG13_003
Purpose	This test checks the DER-TLV encoding of the "Subject Public Key Info" present in EF.DG13.

Version	1.0
References	ISO/IEC 18013-3:2009 RFC-3280
Profile	AA
Preconditions	1. EF.DG13 has been retrieved from the IDL.
Test Scenario	1. Search for the AA Public Key Info (Tag '30') inside EF.DG13. 2. Check the DER-TLV encoding of the AA Public Key Info. 3. Check the value of the encoded AA Public Key Info.
Expected Results	1. Tag '30' shall be present. 2. The AA Public Key Info shall be DER encoded. 3. The AA Public Key Info shall be follow the encoding of the Subject Public Key Info specified in RFC-3280.

A.3.13.4 Test Case SE_LDS_DG13_004

Test Case-ID	SE_LDS_DG13_004
Purpose	This test checks that the algorithm indicated for the Public Key in EF.DG13 is one of the algorithms specified in ISO/IEC18013-3.
Version	1.0
References	ISO/IEC 18013-3:2009 RFC-3279
Profile	AA
Preconditions	1. EF.DG13 has been retrieved from the IDL.
Test Scenario	1. Search for the Algorithm Identifier (Tag '30') inside the AA Public Key Info. 2. Check the DER-TLV encoding of the Algorithm Identifier. 3. Check the value of the Algorithm Identifier. 4. Check the value of the algorithm indicated in the Algorithm Identifier.
Expected Results	1. Tag '30' shall be present and shall occur only once. 2. The Algorithm Identifier shall be DER encoded. 3. The Algorithm Identifier shall be follow the ASN.1 encoding specified in RFC-3280. 4. The Public Key Algorithm indicated in the Algorithm Identifier shall be one of the algorithms indicated in ISO/IEC 18013-3:2009 (i.e. the OID of the algorithm shall be rsaEncryption or id-ecPublicKey).

A.3.13.5 Test Case SE_LDS_DG13_005

Test Case-ID	SE_LDS_DG13_005
Purpose	This test the encoding of the Subject Public Key in the AA Public Key Info in EF.DG13.
Version	1.0
References	ISO/IEC 18013-3:2009 RFC-3280 RFC-3279
Profile	AA
Preconditions	1. EF.DG13 has been retrieved from the IDL.
Test Scenario	1. Search for the Subject Public Key (Tag '03') inside the AA Public Key Info. 2. Check the DER-TLV encoding of the Subject Public Key. 3. Check the data bits from the bit string code a valid Public Key for the algorithm indicated in the Subject Public Key Info data element. 4. Checks that the length of the encoded Public Key meets the minimum size recommendations.

Expected Results	1. Tag '03' shall be present and shall occur only once. 2. The Subject Public Key shall be encoded as a bit-string. 3. The data bits from the bit string shall code a valid Public Key for the algorithm indicated in the Subject Public Key Info data element. 4. An RSA Public Keys shall have a length of at least 1024 bits, an EC Public shall have a length of at least 160 bits.

A.3.13.6 Test Case SE_LDS_DG13_006

Test Case-ID	SE_LDS_DG13_006
Purpose	This test checks the signature that has been generated by the IDL during AA.
Version	1.0
References	ISO/IEC 18013-3:2009 ISO/IEC 9796-2 RFC-3280 RFC-3279
Profile	AA, AA-RSA
Preconditions	1. EF.DG13 has been retrieved from the IDL. 2. EF.DG13 contains a valid RSA public key. 3. The RND.IFD and the signature that has been generated by the IDL are available.
Test Scenario	1. Obtain the plaintext signature from the Internal Authenticate Response. 2. Decipher the AA signature using the Public Key from EF.DG13. 3. "Signature Opening" - Check the leftmost 2 bits of the Recoverable String. 4. "Signature Opening" - Check the last byte of the Recoverable String. 5. "Intermediate String Recovery" - Retrieve the number of padding bits from the beginning of the Recoverable String. 6. "Trailer Recovery" - Check the last byte of the Recoverable String. 7. "Hash Code Checking" - Retrieve the hash code from the Recoverable String.
Expected Results	1. The length of the signature shall be in accordance with the length of the public key from EF.DG13. 2. The length of the deciphered signature shall be in accordance with the length of the public key from EF.DG13. 3. The leftmost 2 bits of the Recoverable String shall be equal to '01'b. 4. The rightmost 4 bits of the Recoverable String shall be equal to '1100'b. 5. The number of padding bits equal to '0'b following the 3rd bit of the Recoverable String shall be less than 8. 6. The Trailer of the Recoverable String shall be 'BC' for trailer option 1 or 'CC' for trailer option 2 (ISO/IEC 9796-2 digital Signature Scheme 1, with has HASH according to hash-function identifier). 7. The hash code shall match the hash calculated over M1||M2 (M1 is the nonce that has been generated by the IDL; M2 is RDN.IFD).

A.3.13.7 Test Case SE_LDS_DG13_007

Test Case-ID	SE_LDS_DG13_007
Purpose	This test checks the signature that has been generated by the IDL during AA.
Version	1.0
References	ISO/IEC 18013-3:2009 RFC-3280 RFC-3279
Profile	AA, AA-ECDSA
Preconditions	1. EF.DG13 has been retrieved from the IDL.

	2. EF.DG13 contains a valid EC public key.
Test Scenario	1. Obtain the plaintext signature from the Internal Authenticate Response. 2. Verify the signature using ECDSA SHA-1.
Expected Results	1. The length of the signature shall be in accordance with the length of the public key from EF.DG13. 2. Signature verification shall be successful.

A.3.14 Test Unit SE_LDS_DG14 – Tests for EF.DG14

Test Unit-ID	SE_LDS_DG14 (Standard Encoding – Data Group 14)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Data Group 14.
References	ISO/IEC 18013-2:2008 ISO/IEC 18013-3:2009

A.3.14.1 Test Case SE_LDS_DG14_001

Test Case-ID	SE_LDS_DG14_001
Purpose	This test checks the template tag; the encoded EF.DG14 element starts with.
Version	1.0
References	ISO/IEC 18013-3:2009
Profile	EAP
Preconditions	1. EF.DG14 has been retrieved from the IDL.
Test Scenario	1. Check the very first byte of the EF.DG14 element.
Expected Results	1. First byte shall be '6E'.

A.3.14.2 Test Case SE_LDS_DG14_002

Test Case-ID	SE_LDS_DG14_002
Purpose	This test checks the encoding of EF.DG14 element length
Version	1.0
References	ISO/IEC 18013-3:2009
Profile	EAP
Preconditions	1. EF.DG14 has been retrieved from the IDL.
Test Scenario	1. Analyze the encoding of the bytes that follow the template tag. 2. Verify the length of the EF.DG14 object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.DG14 object.

A.3.14.3 Test Case SE_LDS_DG14_003

Test Case-ID	SE_LDS_DG14_003
Purpose	This test checks the DER-TLV encoding of the "SecurityInfos" in EF.DG14"
Version	1.0
References	ISO/IEC 18013-3:2009
Profile	EAP
Preconditions	1. EF.DG14 has been retrieved from the IDL.
Test Scenario	1. Search for the Security Infos (Tag '31') data element inside EF.DG14. 2. Check the absence of other data in EF.DG14. 3. Check the DER-TLV encoding of the Security Infos data element.
Expected Results	1. Tag '31' shall be present; tag '31' shall occur only once. 2. Tags not equal to '31' shall be absent. 3. The Security Infos data element shall contain a valid DER-TLV structure (according to ASN.1 encoding rules).

A.3.14.4 Test Case SE_LDS_DG14_004

Test Case-ID	SE_LDS_DG14_004
Purpose	This test checks the presence of Security Info for CA in the Security Infos data element in EF.DG14.
Version	1.0
References	ISO/IEC 18013-3:2009
Profile	EAP
Preconditions	1. EF.DG14 has been retrieved from the IDL. 2. The Security Infos data element has been retrieved from EF.DG14.
Test Scenario	1. Check the presence of the Security Info that defines the CA public key in the Security Infos Set.
Expected Results	1. The Security Infos data element shall contain at least one element that has the protocol OID id-ICAuth.

A.3.14.5 Test Case SE_LDS_DG14_005

Test Case-ID	SE_LDS_DG14_005
Purpose	This test checks the content of each Security Info for CA in the Security Infos data element in EF.DG14.
Version	1.0
References	ISO/IEC 18013-3:2009
Profile	EAP
Preconditions	1. EF.DG14 has been retrieved from the IDL. 2. The Security Infos data element has been retrieved from EF.DG14. 3. At least one Security Info element in the Security Infos data element has the protocol OID id-ICAuth.
Test Scenario	Perform the following checks for each Security Info that defines the CA public key in the Security Infos Set: 1. Check the presence of the requiredData field in the Security Info structure. 2. Check the content of the requiredData field in the Security Info structure. 3. Check the encodeing of the icAuthPublicKey field of the IC Auth PublicKey Info. 4. Search for the Algorithm Identifier (Tag '30') inside the icAuthPublicKey field of the IC Auth PublicKey Info. 5. Check the value of the Algorithm Identifier. 6. Check the value of the algorithm indicated in the Algorithm Identifier. 7. If the algorithm indicated in the Algorithm Identifier is KAEG, verify the domain parameters. 8. Search for the Subject Public Key (Tag '03') inside the icAuthPublicKey field of the IC Auth PublicKey Info. 9. Check the DER-TLV encoding of the Subject Public Key. 10. Check the data bits from the bit string code a valid Public Key for the algorithm indicated in the Subject Public Key Info data element. 11. Check the presence of the keyIdentifier field (Tag '02') in the IC Auth PublicKey Info. 12. Check the presence of the optionalData field in the Security Info structure.
Expected Results	1. The requiredData field shall be present in the Security Info structure. 2. The requiredData field shall be of the type ICAuthPublicKeyInfo. 3. The icAuthPublicKey field shall be follow the encoding of the Subject Public Key Info specified in RFC-3280. 4. Tag '30' shall be present and shall occur only once. 5. The Algorithm Identifier shall be follow the ASN.1 encoding specified in RFC-3280. 6. The Public Key Algorithm indicated in the Algorithm Identifier shall be one of the key agreement protocols given in ISO/IEC 18013-3:2009 (i.e. it shall be dhpublicnumber or id-ecPublicKey).

	7. All domain parameters shall be explicitly included. 8. Tag '03' shall be present and shall occur only once. 9. The Subject Public Key shall be encoded as a bit-string. 10. The data bits from the bit string shall code a valid Public Key for the algorithm indicated in the Subject Public Key Info data element. 11. If a single public key is specified, the keyIdentifier field (Tag '02') may be present and shall occur only once; if more than 1 public key is specified, the keyIdentifier field (Tag '02') shall be present and shall occur only once. 12. The optionalData field shall be absent from the Security Info structure.

A.3.14.6 Test Case SE_LDS_DG14_006

Test Case-ID	SE_LDS_DG14_006
Purpose	If the algorithm used is Diffie Hellman, test the value of the parameters of the icAuthPublicKey field of the IC Auth PublicKey Info for each Security Info that defines the CA public key in the Security Infos Set.
Version	1.0
References	ISO/IEC 18013-3:2009
Profile	EAP, EAP-DH
Preconditions	1. EF.DG14 has been retrieved from the IDL. 2. The Security Infos data element has been retrieved from EF.DG14. 3. At least one Security Info element in the Security Infos data element has the protocol OID id-ICAuth.
Test Scenario	Perform the following checks for each Security Info that defines the CA public key in the Security Infos Set: 1. Check the DH parameters of the algorithm. 2. Check the encoding of the base g. 3. Check the encoding of the prime p. 4. Check the consistency of g and p. 5. If private value length l is present, check the encoding of l. 6. If private value length l is present, check the value of l. 7. If private value length l is present, check the value of l. 8. Check the encoding of the DH Public Key. 9. Check the consistency of the DH Public Key value and prime p.
Expected Results	1. The parameters shall be ASN.1 encoded and follow PKCS #3 (DH), i.e. the DH parameters shall specify a prime (integer), a base (integer), and optionally a privateValueLength (integer). 2. g shall be a positive integer. 3. p shall be a positive integer. 4. g shall be less than p (0 < g < p). 5. length l shall be a positive integer. 6. length l shall be non-zero (l > 0). 7. length l shall be such that 2l-1 < p. 8. The DH Public Key shall be a positive integer. 9. The DH Public Key shall be smaller than p (0 < PublicKey < p).

A.3.14.7 Test Case SE_LDS_DG14_007

Test Case-ID	SE_LDS_DG14_007
Purpose	If the algorithm used is ECDH, test the value of the parameters of the icAuthPublicKey field of the IC Auth PublicKey Info for each Security Info that defines the CA public key in the Security Infos Set.
Version	1.0
References	ISO/IEC 18013-3:2009 RFC-3279
Profile	EAP, EAP-ECDH

Preconditions	1. EF.DG14 has been retrieved from the IDL. 2. The Security Infos data element has been retrieved from EF.DG14. 3. At least one Security Info element in the Security Infos data element has the protocol OID id-ICAuth.
Test Scenario	Perform the following checks for each Security Info that defines the CA public key in the Security Infos Set: 1. Check the Elliptic Curve parameters. 2. Check the encoding of the prime p. 3. Check the value of the prime p. 4. Check the value of the curve parameter a. 5. Check the consistency of the curve parameter a and prime p. 6. Check the value of the curve parameter b. 7. Check the consistency of the curve parameter b and prime p. 8. Check the consistency of the curve parameters a and b. 9. Check the value of the base point G. 10. Check the encoding of the Cofactor f. 11. Check the value of the Cofactor f. 12. Check the encoding of the order r of base point. 13. Check the value of the order r of base point. 14. Check the consistency of the order r and prime p. 15. Check the consistency of the order r, prime p, and co-factor f. 16. Check value of the EC public key (base point Y).
Expected Results	1. The parameters shall follow ASN.1 structure specified in RFC 3279. 2. p shall be a positive integer. 3. p shall be larger than 2 (p>2). 4. a shall be larger than or equal to zero (a>=0). 5. a shall be smaller than p (a<p). 6. b shall be larger than or equal to zero (b>=0). 7. b shall be smaller than p (b<p). 8. The values of a and b shall be such that 4a3 + 27b2 <> 0. 9. The base point G shall be on the curve, with both coordinates in range 0 .. (p - 1). 10. f shall be a positive integer. 11. f shall be larger than zero (f>0). 12. r shall be a positive integer. 13. r shall be larger than zero (r>0). 14. r shall not be equal to p (r <> p). 15. r, p, and f shall be such that r * f <= 2p. 16. The public base point Y is on the curve, with both coordinates in range 0 .. (p - 1).

Annex B
(normative)

Test case specification: Commands for SE on SIC

B.1 Introduction

This annex specifies the test cases for commands implemented for SE on SIC.

B.2 General test requirements

B.2.1 Preconditions for testing

The tests in this annex require a fully personalized IDL. This means that all mandatory data groups shall be present. This annex tests all mandatory ISO/IEC 7816 commands of the SIC. There are additional test units for testing of optional features such as BAP, EAP and NMA.

All tests are mandatory unless marked as optional or conditional.

B.2.2 Test setup

For setting up these tests, any reader for communicating with SIC compliant with ISO/IEC 7816 or ISO/IEC 14443 can be used. The reader shall support extended length APDUs and command chaining.

A three level certificate hierarchy is applicable for EAP in all test cases except where explicitly specified otherwise.

NOTE For SIC supporting EAP, this test case specification contains certain test cases which verify the IDLs behavior with expired certificates. During these tests, the effective date stored inside the chip is changed. For these tests, a set of certificates can be used only once with a single IDL sample. After these tests have been performed, another sample or a new set of certificates is needed to repeat the tests. Therefore it is recommended to perform these tests as the last one in a test sequence.

B.2.3 Implementation conformance statement

In order to set up the tests properly, Tables B.1 and B.2 shall be completed.

ISO/IEC 18013-2 defines several optional elements that may be supported by an IDL. This includes security mechanisms like BAP, EAP and AA as well as additional data groups (DG2 to DG14).

Since these elements are optional, it is not possible to define the corresponding tests as mandatory for each IDL. Therefore, this part of ISO/IEC 18013 specifies a set of profiles. Each profile covers a specific optional element. A tested IDL shall be assigned to the supported profiles in the ICS, and a test shall only be performed if the IDL supports this profile.

NOTE No profile ID's are explicitly defined for DG12 to DG14 because the EAP, AA and NMA profiles cover these data groups implicitly.

Table B.1 — Implementation conformance statement

Profile	Information for test setup	Applicable (YES or NO)	Protection level (Plain, BAP or EAP)
Plain	Non-BAP protected		
OddIns	Read Binary with odd instruction byte supported		
SMI	Security Mechanism Indicator		
DG2	IDL contains elementary file with LDS Data Group 2		
DG3	IDL contains elementary file with LDS Data Group 3		
DG4	IDL contains elementary file with LDS Data Group 4		
DG5	IDL contains elementary file with LDS Data Group 5		
DG6	IDL contains elementary file with LDS Data Group 6		
DG7	IDL contains elementary file with LDS Data Group 7		
DG8	IDL contains elementary file with LDS Data Group 8		
DG9	IDL contains elementary file with LDS Data Group 9		
DG11	IDL contains elementary file with LDS Data Group 11		
PA	Passive Authentication		
AA	Active Authentication		
AA-ECDSA	AA ECDSA algorithm		
AA-RSA	AA RSA algorithm		
NMA	Non-Match Alert		
BAP	Basic Access Protection		
EAP	Extended Access Protection		
CA-DH	CA Diffie-Hellman		
CA-ECDH	CA Elliptic Curve Diffie-Hellman		
TA-ECDSA	TA ECDSA algorithm		
TA-RSA	TA RSA algorithm		
TA-MIG	TA Migration of the crypto system		
TA-PKI3+	PKI hierarchy of more than 3 levels for Terminal Authentication		

Table B.2 — Configuration information

Supported Profile	Configuration information
PA	Provide the country signing certificate name:
BAP	Provide the reference string provided with the samples:
EAP	Provide the name of the trust point certificate under card verifiable format:
	Provide the name of the private key in PKCS 8 format:
TA-MIG	Provide the list of the supported algorithms:
DG11	Provide the template tag:

B.2.4 Verification of ISO/IEC 7816-4 status bytes

For most of the test cases defined in this part of ISO/IEC 18013, the status bytes returned by the IDL are not exactly defined in ISO/IEC 18013-2 and ISO/IEC 18013-3. In these cases the result analysis uses the scheme defined in the ISO/IEC 7816-4 in order to specify the expected result.

It is only checked that the response belongs to the specified category. In cases where the expected result is unambiguously defined in ISO/IEC 18013-2 and ISO/IEC 18013-3, the exact value is specified in the test case. Proprietary status bytes outside the range of defined ISO status bytes will be treated as failures in the test cases.

The status bytes are defined in 5.1.3 of ISO/IEC 7816-4.

B.2.5 Key pair definition

The certificate sets defined in B.2.6 are based on several asymmetric key pairs. In preparation to the tests, these key pairs have to be generated. The parameter used for these keys are depending on the initial trust root private key, which should be provided with the IDL.

For the key set 09 (CERT_LF_KEY_09a, CERT_L1_KEY_09b, CERT_L0_KEY_09c) the algorithm for the cryptosystem migration shall be used as defined in the ICS.

All key pairs shall be generated independently; it is not permitted to use the same key pair for all sets.

Table B.3 — Key pair definition

Key pair	Description
TRUSTPOINT_KEY_00	The key pair TRUSTPOINT_KEY_00 is the public/private key for the initial Trust point root.
CERT_L1_KEY_01	Key pair of the Certificate CERT_L1_01
CERT_L0_KEY_01	Key pair of the Certificate CERT_L0_01
CERT_L1_KEY_02	Key pair of the Certificate CERT_L1_02
CERT_L0_KEY_02	Key pair of the Certificate CERT_L0_02
CERT_L0_KEY_03	Key pair of the Certificate CERT_L0_03
CERT_L0_KEY_04	Key pair of the Certificate CERT_L0_04
CERT_LF_KEY_05	Key pair of the Certificate CERT_LF_05
CERT_L1_KEY_05	Key pair of the Certificate CERT_L1_05
CERT_L0_KEY_05	Key pair of the Certificate CERT_L0_05
CERT_LF_KEY_06	Key pair of the Certificate CERT_LF_06
CERT_L0_KEY_06	Key pair of the Certificate CERT_L0_06
CERT_LF_KEY_07	Key pair of the Certificate CERT_LF_07
CERT_LF_KEY_07k	Key pair of the Certificate CERT_LF_07k
CERT_L1_KEY_07	Key pair of the Certificate CERT_L1_07
CERT_LF_KEY_08a	Key pair of the Certificate CERT_LF_08a
CERT_LF_KEY_08b	Key pair of the Certificate CERT_LF_08b
CERT_L1_KEY_08c	Key pair of the Certificate CERT_L1_08c
CERT_LF_KEY_09a	Key pair of the Certificate CERT_LF_09a
CERT_L1_KEY_09b	Key pair of the Certificate CERT_L1_09b
CERT_L0_KEY_09c	Key pair of the Certificate CERT_L0_09c

B.2.6 Certificate specification

The certificate chain hierarchy is incorporated in the certificate set definition.

The definition of a certificate set uses the notation ‘CERT_La_bbc’,

where

'La' can assume any of the following values:

- L1 : Certificates of which the path length constraint is set to ‘1h’
- L0 : Certificates of which the path length constraint is set to ‘0h’
- LF : Certificates of which the path length constraint is set to ‘Fh’

'bb' is the certificate set number, and

'c' is an invalid encoding of ‘CERT_La_bb’ or a specific regular certificate and can assume any value from a to z.

EXAMPLE All certificates defined in Certificate set 1 will have 'bb' equal to '01'.

B.2.6.1 Certificate set 1

The certificate set consists of a regular certificate chain (Trust Point -> CERT_L1 -> CERT_L0) which is used for the positive tests regarding the certificate verification. Furthermore, it contains variants of the original CERT_L1 certificate to simulate a variety of certificate coding issues (such as missing elements, badly encoded dates …).

B.2.6.1.1 CERT_L1_01

Cert ID	CERT_L1_01	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 31 30 30 31 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 11 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate , hh is the placeholder for the BCD encoded expiration date of the certificate , ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1001
	Relative authorization	Authoritative time source Path length constraint set to 1 Grant read access to all DGs
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_L1_KEY_01
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.1.2 CERT_L1_01a

Cert ID	CERT_L1_01a	
Purpose	This certificate is similar to CERT_L1_01, but does not contain a Certificate Holder Authorization.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 31 30 30 31 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate , hh is the placeholder for the BCD encoded expiration date of the certificate , ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1001
	Relative authorization	absent
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_L1_KEY_01
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.1.3 CERT_L1_01b

Cert ID	CERT_L1_01b	
Purpose	This certificate is similar to CERT_L1_01, but does not contain a Certificate Effective Date.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 31 30 30 31 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 11 FF FF FF 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), hh is the placeholder for the BCD encoded expiration date of the certificate , ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1001
	Relative authorization	Authoritative time source Path length constraint set to 1 Grant read access to all DGs
	Certificate effective date	absent
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_L1_KEY_01
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.1.4 CERT_L1_01c

Cert ID	CERT_L1_01c	
Purpose	This certificate is similar to CERT_L1_01, but does not contain a Certificate Expiration Date.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 31 30 30 31 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 11 FF FF FF 5F 25 06 gg 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1001
	Relative authorization	Authoritative time source Path length constraint set to 1 Grant read access to all DGs
	Certificate effective date	Trust Pointeff
	Certificate expiration date	absent
	Public Key reference	Public key of key pair CERT_L1_KEY_01
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.1.5 CERT_L1_01d

Cert ID	CERT_L1_01d	
Purpose	This certificate is similar to CERT_L1_01, but contains a badly encoded Certificate Effective Date (invalid BCD encoding).	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 31 30 30 31 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 11 FF FF FF 5F 25 06 0A 0B 0C 0D 0E 0F 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1001
	Relative authorization	Authoritative time source Path length constraint set to 1 Grant read access to all DGs
	Certificate effective date	0A 0B 0C 0D 0E 0F (invalid BCD encoding)
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_L1_KEY_01
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.1.6 CERT_L1_01e

Cert ID	CERT_L1_01e	
Purpose	This certificate is similar to CERT_L1_01, but contains a badly encoded Certificate Expiration Date (invalid BCD encoding).	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 31 30 30 31 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 11 FF FF FF 5F 25 06 gg 5F 24 06 0A 0B 0C 0D 0E 0F 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1001
	Relative authorization	Authoritative time source Path length constraint set to 1 Grant read access to all DGs
	Certificate effective date	Trust Pointeff
	Certificate expiration date	0A 0B 0C 0D 0E 0F (invalid BCD encoding)
	Public Key reference	Public key of key pair CERT_L1_KEY_01
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.1.7 CERT_L1_01f

Cert ID	CERT_L1_01f	
Purpose	This certificate is similar to CERT_L1_01, but contains a badly encoded Certificate Effective Date (invalid Gregorian date).	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 31 30 30 31 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 11 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1001
	Relative authorization	Authoritative time source Path length constraint set to 1 Grant read access to all DGs
	Certificate effective date	The month and the year used as defined by the TrustPointeff and the day is always set to the 32nd so that it becomes an invalid Gregorian date.
	Certificate expiration date	TrustPointeff+ 1 month
	Public Key reference	Public key of key pair CERT_L1_KEY_01
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.1.8 CERT_L1_01g

Cert ID	CERT_L1_01g	
Purpose	This certificate is similar to CERT_L1_01, but contains a badly encoded Certificate Expiration Date (invalid Gregorian date).	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 31 30 30 31 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 11 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1001
	Relative authorization	Authoritative time source Path length constraint set to 1 Grant read access to all DGs
	Certificate effective date	TrustPointeff
	Certificate expiration date	The month and the year used as defined by the TrustPointeff+ 1 month and the day is always set to the 32nd so that it becomes an invalid Gregorian date.
	Public Key reference	Public key of key pair CERT_L1_KEY_01
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.1.9 CERT_L1_01h

Cert ID	CERT_L1_01h	
Purpose	This certificate is similar to CERT_L1_01, but contains a Certificate Expiration Date BEFORE the Certificate Effective Date.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 31 30 30 31 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 11 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1001
	Relative authorization	Authoritative time source Path length constraint set to 1 Grant read access to all DGs
	Certificate effective date	TrustPointeff+ 1 day
	Certificate expiration date	TrustPointeff
	Public Key reference	Public key of key pair CERT_L1_KEY_01
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.1.10 CERT_L1_01i

Cert ID	CERT_L1_01i	
Purpose	This certificate is similar to CERT_L1_01, but contains an invalid Certificate Holder Authorization.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 31 30 30 31 7F 4C 0F 06 07 28 81 8C 5D 03 03 02 53 04 11 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1001
	Relative authorization	Authoritative time source Path length constraint set to 1 Grant read access to all DGs
	Certificate effective date	TrustPointeff
	Certificate expiration date	TrustPointeff+ 1 month
	Public Key reference	Public key of key pair CERT_L1_KEY_01
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.1.11 CERT_L1_01j

Cert ID	CERT_L1_01j	
Purpose	This certificate is similar to CERT_L1_01, but contains a Public Key with an invalid OID.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 31 30 30 31 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 11 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1001
	Certificate Public Key	Bad OID not contained in 18013-3 Table C.20 — Supported algorithms for example : 1.0.18013.3.1.10
	Relative authorization	Authoritative time source Path length constraint set to 1 Grant read access to all DGs
	Certificate effective date	TrustPointeff
	Certificate expiration date	TrustPointeff+ 1 month
	Public Key reference	Public key of key pair CERT_L1_KEY_01
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.1.12 CERT_L0_01

Cert ID	CERT_L0_01	
Purpose	This certificate is a regular CERT_L0 certificate, which is issued by CERT_L1.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 0D 54 45 53 54 43 45 52 54 4C 31 30 30 31 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 31 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTL1001
	Subject Key Identifier	TESTCERTL0001
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_L0_KEY_01
	Signing Key reference	Signed with the private key of key pair CERT_L1_KEY_01

B.2.6.2 Certificate set 2

The certificate set consists of a regular certificate chain (Trust Point -> CERT_L1 -> CERT_L0) which is used to verify the behaviour of IDL with respect to authoritative time source value.

B.2.6.2.1 CERT_L1_02

Cert ID	CERT_L1_02	
Purpose	This certificate is a regular certificate without authoritative time source, which validity period starts at the effective date of the Trust point and expires after one month.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 31 30 30 32 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 01 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1002
	Relative authorization	Path length constraint set to 1 Grant read access to all DGs
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_L1_KEY_02
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.2.2 CERT_L0_02a

Cert ID	CERT_L0_02a	
Purpose	This certificate is a regular CERT_L0 certificate, which is issued by CERT_L1. It has an advanced effective date (beyond the current date of the IDL).	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 0D 54 45 53 54 43 45 52 54 4C 31 30 30 32 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 32 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTL1002
	Subject Key Identifier	TESTCERTL0002
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 14 days
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_L0_KEY_02
	Signing Key reference	Signed with the private key of key pair CERT_L1_KEY_02

B.2.6.2.3 CERT_L0_02b

Cert ID	CERT_L0_02b	
Purpose	This certificate is a regular CERT_L0 certificate, which is issued by CERT_L1. It has an expiry date BEFORE the effective date of CERT_L0_02a.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 0D 54 45 53 54 43 45 52 54 4C 31 30 30 32 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 32 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTL0002
	Subject Key Identifier	TESTCERTL0002
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 13 days
	Public Key reference	Public key of key pair CERT_L0_KEY_02
	Signing Key reference	Signed with the private key of key pair CERT_L1_KEY_02

B.2.6.3 Certificate set 3

This certificate set consists of a certificate chain (Trust Point -> CERT_L0) which is used for the certificate structure tests.

B.2.6.3.1 CERT_L0_03a

Cert ID	CERT_L0_03a	
Purpose	This certificate contains a bad AKID.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	AKID Trust point plus 1
	Subject Key Identifier	TESTCERTL0003
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.2 CERT_L0_03b

Cert ID	CERT_L0_03b	
Purpose	This certificate contains a bad certificate body tag.	
Version	1.0	
Content definition	7F 21 aa 7F 4F bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.3 CERT_L0_03c

Cert ID	CERT_L0_03c	
Purpose	This certificate contains a bad certificate signature tag.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 38 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.4 CERT_L0_03d

Cert ID	CERT_L0_03d	
Purpose	Certificate with an inconsistent “certificate body” DO (wrong length).	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object decreased by one, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.5 CERT_L0_03e

Cert ID	CERT_L0_03e	
Purpose	Certificate with an inconsistent “certificate signature” DO (wrong length).	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object decreased by one, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.6 CERT_L0_03f

Cert ID	CERT_L0_03f	
Purpose	Certificate with a wrong signature.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes) last byte is increased by one (mod 256).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.7 CERT_L0_03g

Cert ID	CERT_L0_03g	
Purpose	Certificate with a wrong signature.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes) - last byte is dropped and the TLV encoding is updated to reflect the new length.	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.8 CERT_L0_03i

Cert ID	CERT_L0_03i	
Purpose	For RSA profile only: Certificate with a wrong signature.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes) – the signature is greater than the modulus of the issuing key TRUSTPOINT_KEY_00, the length of signature matches the length of the modulus.	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.9 CERT_L0_03j

Cert ID	CERT_L0_03j	
Purpose	For ECDSA profile only: The certificate signature is wrong. It is obtained by filling the 'r' part of the signature with '00'. The length of 'r' still matches the size of the prime.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes) – with r = 0.	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.10 CERT_L0_03k

Cert ID	CERT_L0_03k	
Purpose	For ECDSA profile only: The certificate signature is wrong. It is obtained by filling the 's' part of the signature with '00'. The length of 's' still matches the size of the prime.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes) - with s = 0.	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.11 CERT_L0_03I

Cert ID	CERT_L0_03I	
Purpose	Modification in the certificate public key: wrong OID.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Certificate Public Key	Bad OID not contained in 18013-3 Table C.20 — Supported algorithms for example : 1.0.18013.3.1.10
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.12 CERT_L0_03m

Cert ID	CERT_L0_03m	
Purpose	Modification in the certificate public key: OID is missing.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Certificate Public Key	It does not contain any OID DO
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.13 CERT_L0_03n

Cert ID	CERT_L0_03n	
Purpose	For ECDSA profile only: Modification in the certificate public key: the elliptic curve public point is missing.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Certificate Public Key	The elliptic curve public point is missing
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.14 CERT_L0_03o

Cert ID	CERT_L0_03o	
Purpose	For RSA profile only: Modification in the certificate public key: the RSA modulus is missing.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate,, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Certificate Public Key	The RSA modulus is missing
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.15 CERT_L0_03p

Cert ID	CERT_L0_03p	
Purpose	For RSA profile only: Modification in the certificate public key: the RSA public exponent is missing.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Certificate Public Key	The RSA public exponent is missing
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.16 CERT_L0_03q

Cert ID	CERT_L0_03q	
Purpose	Modification in the certificate public key. For ECDSA profile: an unknown DO is present within the EC parameters (tag '77'). For RSA profile: an unknown DO is present within the RSA parameters ('77 01 00').	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0003
	Certificate Public Key	An unknown DO '77' is present
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.17 CERT_L0_03r

Cert ID	CERT_L0_03r	
Purpose	The AKID value is more than 16 bytes length.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 33 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID – more than 16 bytes, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point and right padded with 20h to have 17 bytes length
	Subject Key Identifier	TESTCERTL0003
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.3.18 CERT_L0_03s

Cert ID	CERT_L0_03s	
Purpose	The SKID value is more than 16 bytes length.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 11 54 45 53 54 43 45 52 54 4C 30 30 30 33 20 20 20 20 20 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	"TESTCERTL0003" and right padded with '20'h to have 17 bytes length
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_03
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.4 Certificate set 4

The certificate set consists of a certificate chain (Trust Point -> CERT_L0) which follows a certification scheme where the certificate contains public key information from a generated key, the length of which is shorter than the Trust Point key length.

B.2.6.4.1 CERT_L0_04

Cert ID	CERT_L0_04	
Purpose	Certificate with a wrong (short) public key. For RSA profile, same Algorithm Identifier but the modulus length of the certificate PK is shorter than the Trust point's key modulus length. For ECDSA profile, same Algorithm Identifier but the domain parameters of the certificate are different and have a shorter prime length than the Trust Point's key. The hash algorithm should be adapted (by selecting a shorter hash length) if the length of the initial hash is larger than the key size.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 34 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL0004
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff+ 1 month + 20 days
	Certificate expiration date	Trust Pointeff + 1 month + 25 days
	Public Key reference	Public key of key pair CERT_L0_KEY_04
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.5 Certificate set 5

This certificate set consists of a 4 level hierarchy certificate chain which follows a certification scheme where the path length is set to different value to verify the transition.

B.2.6.5.1 CERT_LF_05a

Cert ID	CERT_LF_05a	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to 'Fh'.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 35 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF005
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_LF_KEY_05
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.5.2 CERT_LF_05b

Cert ID	CERT_LF_05b	
Purpose	This certificate is an irregular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to 'Fh'.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 0D 54 45 53 54 43 45 52 54 4C 30 30 30 35 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 35 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTL0005
	Subject Key Identifier	TESTCERTLF005
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_LF_KEY_05
	Signing Key reference	Signed with the private key of key pair CERT_L0_KEY_05

B.2.6.5.3 CERT_LF_05c

Cert ID	CERT_LF_05c	
Purpose	This certificate is an irregular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to 'Fh'.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 0D 54 45 53 54 43 45 52 54 4C 31 30 30 35 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 35 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTL1005
	Subject Key Identifier	TESTCERTLF005
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_LF_KEY_05
	Signing Key reference	Signed with the private key of key pair CERT_L1_KEY_05

B.2.6.5.4 CERT_L1_05a

Cert ID	CERT_L1_05a	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to '1h'.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 0D 54 45 53 54 43 45 52 54 4C 46 30 30 35 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 31 30 30 35 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 11 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTLF005
	Subject Key Identifier	TESTCERTL1005
	Relative authorization	Authoritative time source Path length constraint set to 1 Grant read access to all DGs
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_L1_KEY_05
	Signing Key reference	Signed with the private key of key pair CERT_LF_KEY_05

B.2.6.5.5 CERT_L1_05b

Cert ID	CERT_L1_05b	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to '1h'.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 31 30 30 35 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 11 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1005
	Relative authorization	Authoritative time source Path length constraint set to 1 Grant read access to all DGs
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_L1_KEY_05
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.5.6 CERT_L0_05a

Cert ID	CERT_L0_05a	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to '0h'.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 0D 54 45 53 54 43 45 52 54 4C 31 30 30 35 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 35 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTL1005
	Subject Key Identifier	TESTCERTL0005
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_L0_KEY_05
	Signing Key reference	Signed with the private key of key pair CERT_L1_KEY_05

B.2.6.5.7 CERT_L0_05b

Cert ID	CERT_L0_05b	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to '0h'.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 0D 54 45 53 54 43 45 52 54 4C 46 30 30 35 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 30 30 30 35 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTLF005
	Subject Key Identifier	TESTCERTL0005
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all DGs
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_L0_KEY_05
	Signing Key reference	Signed with the private key of key pair CERT_LF_KEY_05

B.2.6.6 Certificate set 6

This certificate set is used for the effective access condition tests in case the EAP is supported. For each DG present on the IDL, a set of these certificates shall be built.

B.2.6.6.1 CERT_LF_06a_DGx

Cert ID	CERT_LF_06a_DGx	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to 'Fh'. This certificate gives access to DG_x only.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 36 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F kk 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes). kk is the placeholder for the authorisation access rights bytes	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF006
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to DGx
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_LF_KEY_06
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.6.2 CERT_LF_06b_DGx

Cert ID	CERT_LF_06b_DGx	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to 'Fh'. This certificate gives access to all DGs present on the IDL except DG_x.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 36 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F kk 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes). kk is the placeholder for the authorisation access rights bytes	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF006
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to all the DGs except the DGx
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_LF_KEY_06
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.6.3 CERT_LF_06c_DGx

Cert ID	CERT_LF_06c_DGx	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to 'Fh'. This certificate gives access to all DGs present on the IDL.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 36 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF006
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to all the DGs present on the IDL
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_LF_KEY_06
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.6.4 CERT_LF_06d_DGx

Cert ID	CERT_LF_06d_DGx	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to 'Fh'. This certificate does not give access to any DG present on the IDL.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 36 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F 00 00 00 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF006
	Relative authorization	Authoritative time source Path length constraint set to F Does not give any access to any DGs
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_LF_KEY_06
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.6.5 CERT_L0_06a_DGx

Cert ID	CERT_L0_06a_DGx	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to '0h'. This certificate gives access to DG_x only.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 36 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F kk 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes). kk is the placeholder for the authorisation access rights bytes	
Parameter	Authority Key Identifier	TESTCERTLF006
	Subject Key Identifier	TESTCERTL0006
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to DGx
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_L0_KEY_06
	Signing Key reference	Signed with the private key of key pair CERT_LF_KEY_06

B.2.6.6.6 CERT_L0_06b_DGx

Cert ID	CERT_L0_06b_DGx	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to '0h'. This certificate gives access to all DGs present on the IDL except DG_x.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 36 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F kk 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes). kk is the placeholder for the authorisation access rights bytes	
Parameter	Authority Key Identifier	TESTCERTLF006
	Subject Key Identifier	TESTCERTL0006
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all the DGs except the DGx
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_L0_KEY_06
	Signing Key reference	Signed with the private key of key pair CERT_LF_KEY_06

B.2.6.6.7 CERT_L0_06c_DGx

Cert ID	CERT_L0_06c_DGx	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to '0h'. This certificate gives access to all DGs present on the IDL.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 36 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTLF006
	Subject Key Identifier	TESTCERTL0006
	Relative authorization	Authoritative time source Path length constraint set to 0 Grant read access to all the DGs present on the IDL
	Certificate effective date	Trust Pointeff
	Certificate expiration date	Trust Pointeff + 1 month
	Public Key reference	Public key of key pair CERT_L0_KEY_06
	Signing Key reference	Signed with the private key of key pair CERT_LF_KEY_06

B.2.6.6.8 CERT_L0_06d_DGx

Cert ID	CERT_L0_06d_DGx	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after one month. Path length constraint is set to '0h'. This certificate does not give access to any DG present on the IDL.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 36 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F 00 00 00 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTLF006
	Subject Key Identifier	TESTCERTL0006
	Relative authorization	Authoritative time source Path length constraint set to 0 Does not give any access to any DGs
	Certificate effective date	Trust Point$_{eff}$
	Certificate expiration date	Trust Point$_{eff}$ + 1 month
	Public Key reference	Public key of key pair CERT_L0_KEY_06
	Signing Key reference	Signed with the private key of key pair CERT_LF_KEY_06

B.2.6.7 Certificate set 7

This certificate set is used for the update mechanism tests in case the EAP is supported. Read access may be granted to all DGs.

B.2.6.7.1 CERT_LF_07a

Cert ID	CERT_LF_07a	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date plus one month of the Trust root and expires after two months. Path length constraint is set to 'Fh. This certificate is a certificate of an authoritative time source.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 37 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF007
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	Trust Point$_{eff}$ + 1 month
	Certificate expiration date	Trust Point$_{eff}$ + 2 months
	Public Key reference	Public key of key pair CERT_LF_KEY_07
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.7.2 CERT_LF_07b

Cert ID	CERT_LF_07b	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after 26 days. Path length constraint is set to 'Fh'. This certificate is a certificate of an authoritative time source.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 37 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF007
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	$\text{Trust Point}_{\text{eff}}$
	Certificate expiration date	$\text{Trust Point}_{\text{eff}}$ + 26 days
	Public Key reference	Public key of key pair CERT_LF_KEY_07
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.7.3 CERT_LF_07c

Cert ID	CERT_LF_07c	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date plus one month of the Trust root and expires after two months. Path length constraint is set to 'Fh'. This certificate is not a certificate of an authoritative time source.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 37 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 0F FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF007
	Relative authorization	Non authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	Trust $\text{Point}_{\text{eff}}$ + 1 month
	Certificate expiration date	Trust $\text{Point}_{\text{eff}}$ + 2 months
	Public Key reference	Public key of key pair CERT_LF_KEY_07
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.7.4 CERT_LF_07d

Cert ID	CERT_LF_07d	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after 20 days. Path length constraint is set to 'Fh'. This certificate is not a certificate of an authoritative time source.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 37 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 0F FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF007
	Relative authorization	Non authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	$\text{Trust Point}_{\text{eff}}$
	Certificate expiration date	$\text{Trust Point}_{\text{eff}}$ + 20 days
	Public Key reference	Public key of key pair CERT_LF_KEY_07
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.7.5 CERT_L1_07e

Cert ID	CERT_L1_07e	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date plus 25 days of the Trust root and expires after two months. Path length constraint is set to '1h'. This certificate is a certificate of an authoritative time source.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 37 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate , ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1007
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	$\text{Trust Point}_{\text{eff}}$ + 25 days
	Certificate expiration date	$\text{Trust Point}_{\text{eff}}$ + 2 months
	Public Key reference	Public key of key pair CERT_L1_KEY_07
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.7.6 CERT_L1_07f

Cert ID	CERT_L1_07f	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date of the Trust root and expires after 20 days. Path length constraint is set to '1h'. This certificate is a certificate of an authoritative time source.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 42 cc dd 7F 49 ee ff 5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 37 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1007
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	$\text{Trust Point}_{\text{eff}}$
	Certificate expiration date	$\text{Trust Point}_{\text{eff}}$ + 20 days
	Public Key reference	Public key of key pair CERT_L1_KEY_07
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.7.7 CERT_L1_07g

Cert ID	CERT_L1_07g	
Purpose	This certificate is a regular certificate, of which the validity period starts at the effective date plus one month of the Trust root and expires after two months. Path length constraint is set to '1h'. This certificate is not a certificate of an authoritative time source.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 42 cc dd 7F 49 ee ff **5F 20** 0D 54 45 53 54 43 45 52 54 4C 46 30 30 37 **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 01 FF FF FF **5F 25** 06 gg **5F 24** 06 hh **5F 37** ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTL1007
	Relative authorization	Non authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	Trust $\text{Point}_{\text{eff}}$ + 1 month
	Certificate expiration date	Trust $\text{Point}_{\text{eff}}$ + 2 months
	Public Key reference	Public key of key pair CERT_L1_KEY_07
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.7.8 CERT_LF_07i

Cert ID	CERT_LF_07i	
Purpose	This certificate is a regular Trust point certificate, which validity period starts one day before the original Trust point certificate expires. Path length constraint is set to 'Fh'. This certificate is an authoritative time source certificate.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 **42** cc dd **7F 49** ee ff **5F 20** 0D 54 45 53 54 43 45 52 54 4C 46 30 30 37 **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 3F FF FF FF **5F 25** 06 gg **5F 24** 06 hh **5F 37** ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF007
	Relative authorization	Trust point Authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	Trust Point$_{exp}$ - 1 day
	Certificate expiration date	Trust Point$_{exp}$ + 2 months
	Public Key reference	Public key of key pair CERT_LF_KEY_07
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.7.9 CERT_LF_07j

Cert ID	CERT_LF_07j	
Purpose	This certificate is a regular certificate, which the validity period matches with validity period of the initial Trust root. Path length constraint is set to 'Fh'. This certificate is an authoritative time source certificate.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 **42** cc dd **7F 49** ee ff **5F 20** 0D 54 45 53 54 43 45 52 54 4C 46 30 30 37 **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F FF FF FF **5F 25** 06 gg **5F 24** 06 hh **5F 37** ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF007
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	$\text{Trust Point}_{\text{eff}}$
	Certificate expiration date	$\text{Trust Point}_{\text{exp}}$
	Public Key reference	Public key of key pair CERT_LF_KEY_07
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

B.2.6.7.10 CERT_LF_07k

Cert ID	CERT_LF_07k	
Purpose	This certificate is a regular certificate, which validity period starts one day after the original Trust point certificate expires. Path length constraint is set to 'Fh'. This certificate is an authoritative time source certificate.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 **42** cc dd **7F 49** ee ff **5F 20** 0E 54 45 53 54 43 45 52 54 4C 46 30 30 37 6B **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 1F FF FF FF **5F 25** 06 gg **5F 24** 06 hh **5F 37** ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTLF007
	Subject Key Identifier	TESTCERTLF007k
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	Trust Point$_{exp}$+ 1 day
	Certificate expiration date	Trust Point$_{exp}$+ 1 month
	Public Key reference	Public key of key pair CERT_LF_KEY_07k
	Signing Key reference	Signed with the private key of key pair CERT_LF_KEY_07

B.2.6.8 Certificate set 8

As certificate set 7, this certificate set is used for the update mechanism tests in case the EAP is supported. Read access may be granted to all DGs.

B.2.6.8.1 CERT_LF_08a

Cert ID	CERT_LF_08a	
Purpose	This certificate is a regular Trust point certificate, of which the validity period starts at the expiration date plus one month of the Trust root and expires three months later. Path length constraint is set to 'Fh. This certificate is an authoritative time source certificate.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 **42** cc dd **7F 49** ee ff **5F 20** 0D 54 45 53 54 43 45 52 54 4C 46 30 30 38 **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 3F FF FF FF **5F 25** 06 gg **5F 24** 06 hh **5F 37** ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTLF007
	Subject Key Identifier	TESTCERTLF008
	Relative authorization	Trust point Authoritative time source Path length constraint set to F
	Certificate effective date	Trust Point$_{exp}$ + 1 month
	Certificate expiration date	Trust Point$_{exp}$ + 4 months
	Public Key reference	Public key of key pair CERT_LF_KEY_08a
	Signing Key reference	Signed with the private key of key pair CERT_LF_KEY_07

B.2.6.8.2 CERT_LF_08b

Cert ID	CERT_LF_08b	
Purpose	This certificate is a regular Trust point certificate, of which the validity period starts at the expiration date plus three months of the Trust root and expires three months later. Path length constraint is set to 'Fh. This certificate is an authoritative time source certificate.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 **42** cc dd **7F 49** ee ff **5F 20** 0E 54 45 53 54 43 45 52 54 4C 46 30 30 38 62 **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 3F FF FF FF **5F 25** 06 gg **5F 24** 06 hh **5F 37** ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTLF008
	Subject Key Identifier	TESTCERTLF008b
	Relative authorization	Trust point Authoritative time source Path length constraint set to F
	Certificate effective date	Trust Point$_{exp}$ + 3 months
	Certificate expiration date	Trust Point$_{exp}$ + 6 months
	Public Key reference	Public key of key pair CERT_LF_KEY_08b
	Signing Key reference	Signed with the private key of key pair CERT_LF_KEY_08a

B.2.6.8.3 CERT_L1_08c

Cert ID	CERT_L1_08c	
Purpose	This certificate is a regular certificate, of which the validity period starts at the expiration date plus three months of the Trust root and expires one month later. Path length constraint is set to '1h. This certificate is an authoritative time source certificate.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 **42** cc dd **7F 49** ee ff **5F 20** 0E 54 45 53 54 43 45 52 54 4C 46 30 30 38 63 **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 11 FF FF FF **5F 25** 06 gg **5F 24** 06 hh **5F 37** ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, cc is the encoded length of the AKID, dd is the placeholder for the AKID (cc bytes), ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTLF008b
	Subject Key Identifier	TESTCERTL1008c
	Relative authorization	Authoritative time source Path length constraint set to 1
	Certificate effective date	Trust Point$_{exp}$ + 3 months
	Certificate expiration date	Trust Point$_{exp}$ + 4 months
	Public Key reference	Public key of key pair CERT_L1_KEY_08c
	Signing Key reference	Signed with the private key of key pair CERT_LF_KEY_08b

B.2.6.9 Certificate set 9

This certificate set defines a link certificate used to update the chip signature mechanism according to the migration policy as defined by the manufacturer. The cryptographic elements of these certificates shall use the new mechanisms (except for the signature of the CERT_LF_09, which is done with the original signature mechanism). This certificate set is only needed if the "TA-MIG" profile is supported. Read access may be granted to all DGs.

B.2.6.9.1 CERT_LF_09a

Note for ECDSA profile: Since the crypto mechanism is changed by this certificate, the domain parameters shall be included in this certificate.

<table>
<tr><td>Cert ID</td><td colspan="2">CERT_LF_09a</td></tr>
<tr><td>Purpose</td><td colspan="2">For TA-MIG profile only:
This certificate is a link certificate, which defines a new crypto mechanism to be used by the chip.
Path length constraint is set to ‘Fh.
This certificate is an authoritative time source certificate.</td></tr>
<tr><td>Version</td><td colspan="2">1.0</td></tr>
<tr><td>Content definition</td><td colspan="2">7F 21 aa
7F 4E bb
5F 29 01 00
42 0E 54 45 53 54 43 45 52 54 4C 46 30 30 38 62
7F 49 ee ff
5F 20 0E 54 45 53 54 43 45 52 54 4C 46 30 30 39 61
7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 3F FF FF FF
5F 25 06 gg
5F 24 06 hh
5F 37 ii jj
aa is the encoded combined length of certificate body and signature objects,
bb is the encoded length the certificate body object,
ee is the encoded length of the certificate's public key,
ff is the placeholder for the certificate's public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate,
hh is the placeholder for the BCD encoded expiration date of the certificate,
ii is the encoded length of the certificate's signature object,
jj is the placeholder for the certificate's signature (ii bytes).</td></tr>
<tr><td rowspan="7">Parameter</td><td>Authority Key Identifier</td><td>TESTCERTLF008b</td></tr>
<tr><td>Subject Key Identifier</td><td>TESTCERTLF009a</td></tr>
<tr><td>Relative authorization</td><td>Trust point
Authoritative time source
Path length constraint set to F</td></tr>
<tr><td>Certificate effective date</td><td>Trust Point$_{exp}$ + 5 months</td></tr>
<tr><td>Certificate expiration date</td><td>Trust Point$_{exp}$ + 8 months</td></tr>
<tr><td>Public Key reference</td><td>Public key of key pair CERT_LF_KEY_09a</td></tr>
<tr><td>Signing Key reference</td><td>Signed with the private key of key pair CERT_LF_KEY_08b</td></tr>
</table>

B.2.6.9.2 CERT_L1_09b

Cert ID	CERT_L1_09b	
Purpose	For TA-MIG profile only: This certificate is a regular certificate, issued by CERT_LF_09a, of which the validity period starts at the expiry date plus five months of the Trust root and expires one month later. Path length constraint is set to ‘1h. This certificate is an authoritative time source certificate.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 **42** 0E 54 45 53 54 43 45 52 54 4C 46 30 30 39 61 **7F 49** ee ff **5F 20** 0E 54 45 53 54 43 45 52 54 4C 31 30 30 39 62 **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 11 FF FF FF **5F 25** 06 gg **5F 24** 06 hh **5F 37** ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTLF009a
	Subject Key Identifier	TESTCERTL1009b
	Relative authorization	Authoritative time source Path length constraint set to 1
	Certificate effective date	Trust Point$_{exp}$ + 5 months
	Certificate expiration date	Trust Point$_{exp}$ + 6 months
	Public Key reference	Public key of key pair CERT_L1_KEY_09b
	Signing Key reference	Signed with the private key of key pair CERT_LF_KEY_09a

B.2.6.9.3 CERT_L0_09c

Cert ID	CERT_L0_09c	
Purpose	For TA-MIG profile only: This certificate is a regular certificate, issued by CERT_L1_09b the new Trust point, of which the validity period starts at the expiry date plus five months of the Trust root and expires one month later. Path length constraint is set to '0h'. This certificate is an authoritative time source certificate.	
Version	1.0	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 **42** 0E 54 45 53 54 43 45 52 54 4C 31 30 30 39 62 7F 49 ee ff 5F 20 0E 54 45 53 54 43 45 52 54 4C 30 30 30 39 63 7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 10 FF FF FF 5F 25 06 gg **5F 24** 06 hh **5F 37** ii jj aa is the encoded combined length of certificate body and signature objects, bb is the encoded length the certificate body object, ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), gg is the placeholder for the BCD encoded effective date of the certificate, hh is the placeholder for the BCD encoded expiration date of the certificate, ii is the encoded length of the certificate's signature object, jj is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTL1009b
	Subject Key Identifier	TESTCERTL0009c
	Relative authorization	Authoritative time source Path length constraint set to 0
	Certificate effective date	Trust $Point_{exp}$ + 5 months
	Certificate expiration date	Trust $Point_{exp}$ + 6 months
	Public Key reference	Public key of key pair CERT_L0_KEY_09c
	Signing Key reference	Signed with the private key of key pair CERT_L1_KEY_09b

B.3 Test Layer SE_ISO7816 - Security and Command Tests

SE_ISO7816_SelDF – SELECT DF Command

SE_ISO7816_SecBAP – Security conditions of BAP protected IDL

SE_ISO7816_BAP – Basic Access Protection

SE_ISO7816_SelEFSM – Protected SELECT EF Command

SE_ISO7816_ReadEFSM – Protected READ BINARY Command

SE_ISO7816_SelEF – Unprotected SELECT EF Command

SE_ISO7816_ReadEF – Unprotected READ BINARY Command

SE_ISO7816_AA – Active Authentication

SE_ISO7816_SecEAP – Security Conditions for EAP protected IDL

SE_ISO7816_CA – Chip Authentication

SE_ISO7816_CertVer – Certificate verification

SE_ISO7816_TA – Terminal Authentication

SE_ISO7816_AccCond – Effective Access Conditions

SE_ISO7816_Update – Update mechanism

SE_ISO7816_Migration – Migration Policies

NOTE The objective is not to perform the full spectrum of robustness tests, since it is a function of the chip manufacturer. However, selective robustness tests that may commonly occur have been included.

B.3.1 Test Unit SE_ISO7816_SelDF – SELECT DF Command

This test unit covers all tests about the SELECT DF command. The LDS specification requires the selection of the LDS application by its AID. Since the AID is unique, selecting the application should be possible regardless of the previously selected DF or EF. Selecting the LDS Application should also reset the cards security state but this scenario is tested in the access control unit test.

B.3.1.1 Test case SE_ISO7816_SelDF_1

Test – ID	SE_ISO7816_SelDF_1
Purpose	Selecting the LDS application using the AID (positive test).
Version	1.0
Profile	
Preconditions	1. LDS application shall not be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 04 0C 07 A0 00 00 02 48 02 00'
Expected results	1. P2 denotes "return no file information", and there is no Le present. Therefore, the response data field shall be empty. The IDL return status bytes '90 00'.

B.3.1.2 Test case SE_ISO7816_SelDF_2

Test – ID	SE_ISO7816_SelDF_2
Purpose	Selecting the LDS application using the AID with a wrong CLA byte.
Version	1.0
Profile	
Preconditions	1. LDS application shall not be selected.
Test scenario	1. Send the given SELECT APDU to the IDL (wrong CLA). '80 A4 04 0C 07 A0 00 00 02 48 02 00'
Expected results	1. The IDL shall return an ISO Checking Error.

B.3.1.3 Test case SE_ISO7816_SelDF_3

Test – ID	SE_ISO7816_SelDF_3
Purpose	Selecting the LDS application using wrong AID.
Version	1.0
Profile	
Preconditions	1. LDS application shall not be selected.
Test scenario	1. Send the given SELECT APDU to the IDL (wrong AID). '00 A4 04 0C 07 A0 00 00 02 48 02 01'
Expected results	1. The IDL shall return an ISO Checking Error.

B.3.1.4 Test case SE_ISO7816_SelDF_4

Test – ID	SE_ISO7816_SelDF_4
Purpose	Selecting the LDS application using wrong P1 byte.
Version	1.0
Profile	
Preconditions	1. LDS application shall not be selected.
Test scenario	1. Send the given SELECT APDU to the IDL (wrong P1). '00 A4 84 0C 07 A0 00 00 02 48 02 00'
Expected results	1. The IDL shall return an ISO Checking Error.

B.3.1.5 Test case SE_ISO7816_SelDF_5

Test – ID	SE_ISO7816_SelDF_5
Purpose	Selecting the LDS application using wrong P2 byte.
Version	1.0
Profile	
Preconditions	1. LDS application shall not be selected.
Test scenario	1. Send the given SELECT APDU to the IDL (wrong P2). '00 A4 04 8C 07 A0 00 00 02 48 02 00'
Expected results	1. The IDL shall return an ISO Checking Error.

B.3.1.6 Test case SE_ISO7816_SelDF_6

Test – ID	SE_ISO7816_SelDF_6
Purpose	Selecting the LDS application using wrong Lc byte.
Version	1.0
Profile	
Preconditions	1. LDS application shall not be selected.
Test scenario	1. The tester shall ensure that the command with an incorrect Lc byte can be transmitted from the reader to the IDL under test. 2. Send the given SELECT APDU to the IDL (wrong Lc). '00 A4 04 0C 08 A0 00 00 02 48 02 00'
Expected results	1. The reader should be able to transmit the command with an incorrect Lc byte. If not, the test result shall be recorded as inconclusive. 2. The IDL shall return an ISO Checking Error.

B.3.1.7 Test case SE_ISO7816_SelDF_7

Test – ID	SE_ISO7816_SelDF_7
Purpose	Selecting twice the LDS application.
Version	1.0
Profile	
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 04 0C 07 A0 00 00 02 48 02 00'
Expected results	1. The IDL shall return'90 00' with an empty data field.

B.3.2 Test Unit SE_ISO7816_SecBAP– Security conditions of BAP protected IDL

This unit tests the security conditions of a BAP protected IDL. It shall not be possible read the content of any present file. The tests of this unit try to access the files with an explicit SELECT EF command, a READ BINARY command with implicit file selection via the short EF ID and unsecured READ BINARY while access is granted.

NOTE If the IDL is EAP protected some of the tests of this unit should be adapted (from ISO7816_SecBAP_35 to ISO7816_SecBAP_48), because each certificate of the the certificates chain contains authorization access rights bytes that describes data group access rights. In these specific cases, the EAP process shall be done just next to the BAP process.

B.3.2.1 Test case SE_ISO7816_SecBAP_1

Test – ID	SE_ISO7816_SecBAP_1
Purpose	Selecting EF.COM
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 1E'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.2 Test case SE_ISO7816_SecBAP_2

Test – ID	SE_ISO7816_SecBAP_2
Purpose	Selecting EF.SOD file.
Version	1.0
Profile	BAP, PA
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 1D'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.3 Test case SE_ISO7816_SecBAP_3

Test – ID	SE_ISO7816_SecBAP_3
Purpose	Selecting EF.DG1
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 01'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.4 Test case SE_ISO7816_SecBAP_4

Test – ID	SE_ISO7816_SecBAP_4
Purpose	Selecting EF.DG2
Version	1.0
Profile	BAP, DG2
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 02'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.5 Test case SE_ISO7816_SecBAP_5

Test – ID	SE_ISO7816_SecBAP_5
Purpose	Selecting EF.DG3
Version	1.0
Profile	BAP, DG3
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 03'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.6 Test case SE_ISO7816_SecBAP_6

Test – ID	SE_ISO7816_SecBAP_6
Purpose	Selecting EF.DG4
Version	1.0
Profile	BAP, DG4
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 04'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.7 Test case SE_ISO7816_SecBAP_7

Test – ID	SE_ISO7816_SecBAP_7
Purpose	Selecting EF.DG5
Version	1.0
Profile	BAP, DG5
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 05'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.8 Test case SE_ISO7816_SecBAP_8

Test – ID	SE_ISO7816_SecBAP_8
Purpose	Selecting EF.DG6
Version	1.0
Profile	BAP, DG6
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 06'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.9 Test case SE_ISO7816_SecBAP_9

Test – ID	SE_ISO7816_SecBAP_9
Purpose	Selecting EF.DG7
Version	1.0
Profile	BAP, DG7
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 07'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.10 Test case SE_ISO7816_SecBAP_10

Test – ID	SE_ISO7816_SecBAP_10
Purpose	Selecting EF.DG8
Version	1.0
Profile	BAP, DG8
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 08'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.11 Test case SE_ISO7816_SecBAP_11

Test – ID	SE_ISO7816_SecBAP_11
Purpose	Selecting EF.DG9
Version	1.0
Profile	BAP, DG9
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 09'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.12 Test case SE_ISO7816_SecBAP_12

Test – ID	SE_ISO7816_SecBAP_12
Purpose	Selecting EF.DG10
Version	1.0
Profile	BAP, DG10
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 0A'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.13 Test case SE_ISO7816_SecBAP_13

Test – ID	SE_ISO7816_SecBAP_13
Purpose	Selecting EF.DG11
Version	1.0
Profile	BAP, DG11
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 0B'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.14 Test case SE_ISO7816_SecBAP_14

Test – ID	SE_ISO7816_SecBAP_14
Purpose	Selecting EF.DG12
Version	1.0
Profile	BAP, NMA
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 0C'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.15 Test case SE_ISO7816_SecBAP_15

Test – ID	SE_ISO7816_SecBAP_15
Purpose	Selecting EF.DG13
Version	1.0
Profile	BAP, AA
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 0D'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.16 Test case SE_ISO7816_SecBAP_16

Test – ID	SE_ISO7816_SecBAP_16
Purpose	Selecting EF.DG14
Version	1.0
Profile	BAP, EAP
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 0E'
Expected results	1. The IDL shall return status bytes '69 82'.

B.3.2.17 Test case SE_ISO7816_SecBAP_17

Test – ID	SE_ISO7816_SecBAP_17
Purpose	Accesing the EF.COM by READ BINARY with Short EF Identifier.
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 9E 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.18 Test case SE_ISO7816_SecBAP_18

Test – ID	SE_ISO7816_SecBAP_18
Purpose	Accessing the EF.SOD (READ BINARY with short EF ID).
Version	1.0
Profile	BAP, PA
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 9D 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.19 Test case SE_ISO7816_SecBAP_19

Test – ID	SE_ISO7816_SecBAP_19
Purpose	Accessing the EF.DG1 (READ BINARY with short EF ID).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 81 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.20 Test case SE_ISO7816_SecBAP_20

Test – ID	SE_ISO7816_SecBAP_20
Purpose	Accessing the EF.DG2 (READ BINARY with short EF ID).
Version	1.0
Profile	BAP, DG2
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 82 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.21 Test case SE_ISO7816_SecBAP_21

Test – ID	SE_ISO7816_SecBAP_21
Purpose	Accessing the EF.DG3 (READ BINARY with short EF ID).
Version	1.0
Profile	BAP, DG3
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 83 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.22 Test case SE_ISO7816_SecBAP_22

Test – ID	SE_ISO7816_SecBAP_22
Purpose	Accessing the EF.DG4 (READ BINARY with short EF ID).
Version	1.0
Profile	BAP, DG4
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 84 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.23 Test case SE_ISO7816_SecBAP_23

Test – ID	SE_ISO7816_SecBAP_23
Purpose	Accessing the EF.DG5 (READ BINARY with short EF ID).
Version	1.0
Profile	BAP, DG5
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 85 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.24 Test case SE_ISO7816_SecBAP_24

Test – ID	SE_ISO7816_SecBAP_24
Purpose	Accessing the EF.DG6 (READ BINARY with short EF ID).
Version	1.0
Profile	BAP, DG6
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 86 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.25 Test case SE_ISO7816_SecBAP_25

Test – ID	SE_ISO7816_SecBAP_25
Purpose	Accessing the EF.DG7 (READ BINARY with short EF ID).
Version	1.0
Profile	BAP, DG7
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 87 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.26 Test case SE_ISO7816_SecBAP_26

Test – ID	SE_ISO7816_SecBAP_26
Purpose	Accessing the EF.DG8 (READ BINARY with short EF ID).
Version	1.0
Profile	BAP, DG8
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 88 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.27 Test case SE_ISO7816_SecBAP_27

Test – ID	SE_ISO7816_SecBAP_27
Purpose	Accessing the EF.DG9 (READ BINARY with short EF ID).
Version	1.0
Profile	BAP, DG9
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 89 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.28 Test case SE_ISO7816_SecBAP_28

Test – ID	SE_ISO7816_SecBAP_28
Purpose	Accessing the EF.DG10 (READ BINARY with short EF ID).
Version	1.0
Profile	BAP, DG10
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 8A 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.29 Test case SE_ISO7816_SecBAP_29

Test – ID	SE_ISO7816_SecBAP_29
Purpose	Accessing the EF.DG11 (READ BINARY with short EF ID).
Version	1.0
Profile	BAP, DG11
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 8B 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.30 Test case SE_ISO7816_SecBAP_30

Test – ID	SE_ISO7816_SecBAP_30
Purpose	Accessing the EF.DG12 (READ BINARY with short EF ID).
Version	1.0
Profile	BAP, NMA
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 8C 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.31 Test case SE_ISO7816_SecBAP_31

Test – ID	SE_ISO7816_SecBAP_31
Purpose	Accessing the EF.DG13 (READ BINARY with short EF ID).
Version	1.0
Profile	BAP, AA
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 8D 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.32 Test case SE_ISO7816_SecBAP_32

Test – ID	SE_ISO7816_SecBAP_32
Purpose	Reading the EF.DG14 (READ BINARY with short EF ID).
Version	1.0
Profile	BAP, EAP
Preconditions	1. LDS application shall be selected.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '00 B0 8E 00 00'
Expected results	1. Since read access is prohibited without BAP, the response field shall be empty. The IDL shall return status bytes '69 82'.

B.3.2.33 Test case SE_ISO7816_SecBAP_33

Test – ID	SE_ISO7816_SecBAP_33
Purpose	Accessing the EF.COM file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY (short EF ID) APDU for EF.COM to the IDL. '0C B0 9E 00 0D 97 01 06 8E 08 <Checksum> 00' 2. Send the given READ BINARY APDU as a plain unprotected APDU to the IDL. '00 B0 00 00 00'
Expected results	1. The IDL shall return 6 bytes of response data and status bytes '90 00' within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.34 Test case SE_ISO7816_SecBAP_34

Test – ID	SE_ISO7816_SecBAP_34
Purpose	Accessing the EF.SOD file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP, PA
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the READ BINARY (short EF ID) APDU for EF.SOD to the IDL. '0C B0 9D 00 0D 97 01 06 8E 08 <Checksum> 00' 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. '00 B0 00 00 00'
Expected results	1. The IDL shall return 6 bytes of content data and status bytes '90 00' within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.35 Test case SE_ISO7816_SecBAP_35

Test – ID	SE_ISO7816_SecBAP_35
Purpose	Accessing the EF.DG1 file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY (short EF ID) APDU for EF.DG1 to the IDL. '0C B0 81 00 0D 97 01 06 8E 08 <Checksum> 00' 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. '00 B0 00 00 00'
Expected results	1. The IDL shall return 6 bytes of content data and status bytes '90 00' within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.36 Test case SE_ISO7816_SecBAP_36

Test – ID	SE_ISO7816_SecBAP_36
Purpose	Accessing the EF.DG2 file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP, DG2

Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY (short EF ID) APDU for EF.DG2 to the IDL. '0C B0 82 00 0D 97 01 06 8E 08 <Checksum> 00' 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. '00 B0 00 00 00'
Expected results	1. The IDL shall return 6 bytes of content data and status bytes '90 00' within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.37 Test case SE_ISO7816_SecBAP_37

Test – ID	SE_ISO7816_SecBAP_37
Purpose	Accessing the EF.DG3 file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP, DG3
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY (short EF ID) APDU for EF.DG3 to the IDL. '0C B0 83 00 0D 97 01 06 8E 08 <Checksum> 00' 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. '00 B0 00 00 00'
Expected results	1. The IDL shall return 6 bytes of content data and status bytes '90 00' within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.38 Test case SE_ISO7816_SecBAP_38

Test – ID	SE_ISO7816_SecBAP_37
Purpose	Accessing the EF.DG4 file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP, DG4
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the READ BINARY (short EF ID) APDU for EF.DG4 to the IDL. '0C B0 84 00 0D 97 01 06 8E 08 <Checksum> 00' 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. '00 B0 00 00 00'
Expected results	1. The IDL shall return 6 bytes of content data and status bytes '90 00' within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.39 Test case SE_ISO7816_SecBAP_39

Test – ID	SE_ISO7816_SecBAP_39
Purpose	Accessing the EF.DG5 file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP, DG5
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY (short EF ID) APDU for EF.DG5 to the IDL. '0C B0 85 00 0D 97 01 06 8E 08 <Checksum> 00' 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. '00 B0 00 00 00'
Expected results	1. The IDL shall return 6 bytes of content data and status bytes '90 00' within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.40 Test case SE_ISO7816_SecBAP_40

Test – ID	SE_ISO7816_SecBAP_40
Purpose	Accessing the EF.DG6 file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP, DG6
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY (short EF ID) APDU for EF.DG6 to the IDL. '0C B0 86 00 0D 97 01 06 8E 08 <Checksum> 00' 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. '00 B0 00 00 00'
Expected results	1. The IDL shall return 6 bytes of content data and status bytes '90 00' within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.41 Test case SE_ISO7816_SecBAP_41

Test – ID	SE_ISO7816_SecBAP_41
Purpose	Accessing the EF.DG7 file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP, DG7

Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY (short EF ID) APDU for EF.DG7 to the IDL. ’0C B0 87 00 0D 97 01 06 8E 08 <Checksum> 00’ 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. ’00 B0 00 00 00’
Expected results	1. The IDL shall return 6 bytes of content data and status bytes ’90 00’ within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.42 Test case SE_ISO7816_SecBAP_42

Test – ID	SE_ISO7816_SecBAP_42
Purpose	Accessing the EF.DG8 file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP, DG8
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY (short EF ID) APDU for EF.DG8 to the IDL. ’0C B0 88 00 0D 97 01 06 8E 08 <Checksum> 00’ 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. ’00 B0 00 00 00’
Expected results	1. The IDL shall return 6 bytes of content data and status bytes ’90 00’ within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.43 Test case SE_ISO7816_SecBAP_43

Test – ID	SE_ISO7816_SecBAP_43
Purpose	Accessing the EF.DG9 file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP, DG9
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY (short EF ID) APDU for EF.DG9 to the IDL. ’0C B0 89 00 0D 97 01 06 8E 08 <Checksum> 00’ 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. ’00 B0 00 00 00’
Expected results	1. The IDL shall return 6 bytes of content data and status bytes ’90 00’ within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.44 Test case SE_ISO7816_SecBAP_44

Test – ID	SE_ISO7816_SecBAP_44
Purpose	Accessing the EF.DG10 file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP, DG10
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY (short EF ID) APDU for EF.DG10 to the IDL. '0C B0 8A 00 0D 97 01 06 8E 08 <Checksum> 00' 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. '00 B0 00 00 00'
Expected results	1. The IDL shall return 6 bytes of content data and status bytes '90 00' within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.45 Test case SE_ISO7816_SecBAP_45

Test – ID	SE_ISO7816_SecBAP_45
Purpose	Accessing the EF.DG11 file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP, DG11
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY (short EF ID) APDU for EF.DG11 to the IDL. '0C B0 8B 00 0D 97 01 06 8E 08 <Checksum> 00' 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. '00 B0 00 00 00'
Expected results	1. The IDL shall return 6 bytes of content data and status bytes '90 00' within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.46 Test case SE_ISO7816_SecBAP_46

Test – ID	SE_ISO7816_SecBAP_46
Purpose	Accessing the EF.DG12 file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP, NMA

Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY (short EF ID) APDU for EF.DG12 to the IDL. '0C B0 8C 00 0D 97 01 06 8E 08 <Checksum> 00' 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. '00 B0 00 00 00'
Expected results	1. The IDL shall return 6 bytes of content data and status bytes '90 00' within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.47 Test case SE_ISO7816_SecBAP_47

Test – ID	SE_ISO7816_SecBAP_47
Purpose	Accessing the EF.DG13 file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP, AA
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY (short EF ID) APDU for EF.DG13 to the IDL. '0C B0 8D 00 0D 97 01 06 8E 08 <Checksum> 00' 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. '00 B0 00 00 00'
Expected results	1. The IDL shall return 6 bytes of content data and status bytes '90 00' within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.2.48 Test case SE_ISO7816_SecBAP_48

Test – ID	SE_ISO7816_SecBAP_48
Purpose	Accessing the EF.DG14 file with READ BINARY. The test verifies the enforcement of Secure Messaging while basic access is granted.
Version	1.0
Profile	BAP, EAP
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY (short EF ID) APDU for EF.DG14 to the IDL. '0C B0 8E 00 0D 97 01 06 8E 08 <Checksum> 00' 2. Send the given READ BINARY APDU as a plain unprotected APDU to the Drivring licence. '00 B0 00 00 00'
Expected results	1. The IDL shall return 6 bytes of content data and status bytes '90 00' within a valid Secure Messaging encoding. 2. The IDL shall return ISO checking error without Secure Messaging encoding.

B.3.3 Test Unit SE_ISO7816_BAP – Basic Access Protection

This unit checks the BAP implementation of the IDL. The complete BAP access mechanism is tested, including robustness tests with invalid input data.

This unit only applies to BAP protected IDLs.

B.3.3.1 Test case SE_ISO7816_BAP_1

Test – ID	SE_ISO7816_BAP_1
Purpose	Verification of the GET CHALLENGE command (positive test).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall not have been performed.
Test scenario	1. Send the given GET CHALLENGE APDU to the IDL. '00 84 00 00 08' 2. Send the same GET CHALLENGE APDU to the IDL. '00 84 00 00 08'
Expected results	1. The IDL shall return 8 random bytes of content data and status bytes '90 00'. 2. The IDL shall return 8 different random bytes of content data and status bytes '90 00'.

B.3.3.2 Test case SE_ISO7816_BAP_2

Test – ID	SE_ISO7816_BAP_2
Purpose	Checking the response to the MUTUAL AUTHENTICATE command (positive test).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall not have been performed.
Test scenario	1. Send the given GET CHALLENGE APDU to the IDL. '00 84 00 00 08' 2. Send the given MUTUAL AUTHENTICATE APDU to the IDL. The field <Data> shall be computed with the challenge returned in step 1 and the reference string for the IDL under test. The <Lc> and <Le> fields can be 0x28 or 0x38 depending of the BAP configuration. '00 82 00 00 <Lc> <Data> <Le>'
Expected results	1. The IDL shall return 8 random bytes of content data and status bytes '90 00'. 2. The response from the IDL shall be verified as specified in ISO/IEC 18013-3. The returned status bytes shall be '90 00.

B.3.3.3 Test case SE_ISO7816_BAP_3

Test – ID	SE_ISO7816_BAP_3
Purpose	Checking the authentication failure response to the MUTUAL AUTHENTICATE command.
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall not have been performed.
Test scenario	1. Send the given GET CHALLENGE APDU to the IDL. '00 84 00 00 08' 2. Send the same MUTUAL AUTHENTICATE APDU as int test case SE_ISO7816_BAP_2 to the IDL. But the field <Data> shall be computed with a different reference. The <Lc> and <Le> fields can be 0x28 or 0x38 depending of the BAP configuration. '00 82 00 00 <Lc> <Data> <Le>'
Expected results	1. The IDL shall return 8 random bytes of content data and status bytes '90 00'. 2. The IDL shall return an ISO warning or ISO checking error.

B.3.3.4 Test case SE_ISO7816_BAP_4

Test – ID	SE_ISO7816_BAP_4
Purpose	Checking the authentication failure response to the MUTUAL AUTHENTICATE command.
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall not have been performed. The GET CHALLENGE command shall not have been executed.
Test scenario	1. Send the same MUTUAL AUTHENTICATE APDU as in test case SE_ISO7816_BAP_2 to the IDL. But the field <Data> shall be computed with the challenge '00 00 00 00 00 00 00 00'. The <Lc> and <Le> fields can be 0x28 or 0x38 depending of the BAP configuration. '00 82 00 00 <Lc> <Data> <Le>' 2. Send the given GET CHALLENGE APDU to the IDL. '00 84 00 00 08' 3. Send the given GET CHALLENGE APDU to the IDL. '00 84 00 00 08' 4. Send the same MUTUAL AUTHENTICATE APDU as int test case SE_ISO7816_BAP_2 to the IDL. But the field <Data> shall be computed with the challenge returned in step 2. The <Lc> and <Le> fields can be 0x28 or 0x38 depending of the BAP configuration. '00 82 00 00 <Lc> <Data> <Le>'

Expected results	1. The IDL shall return an ISO warning or ISO checking error. 2. The IDL shall return 8 random bytes of content data and status bytes '90 00'. 3. The IDL shall return 8 random bytes of content data and status bytes '90 00'. 4. The IDL shall return an ISO warning or ISO checking error.

B.3.3.5 Test case SE_ISO7816_BAP_5

Test – ID	SE_ISO7816_BAP_5
Purpose	Checking of the MUTUAL AUTHENTICATE command (robustness test).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall not have been performed.
Test scenario	1. Send the given GET CHALLENGE APDU to the IDL. '00 84 00 00 08' 2. Send the given MUTUAL AUTHENTICATE APDU to the IDL. The field <Data> shall be computed with the challenge returned in step 1 and the reference string for the IDL under test. The CLA byte is set to a wrong value. The <Lc> and <Le> fields can be 0x28 or 0x38 depending of the BAP configuration. '80 82 00 00 <Lc> <Data> <Le>' 3. Send the given GET CHALLENGE APDU to the IDL. '00 84 00 00 08' 4. Send the given MUTUAL AUTHENTICATE APDU to the IDL. The field <Data> shall be computed with the challenge returned in step 3 and the reference string for the IDL under test. The P1 byte is set to a wrong value. The <Lc> and <Le> fields can be 0x28 or 0x38 depending of the BAP configuration. '00 82 60 00 <Lc> <Data> <Le>' 5. Send the given GET CHALLENGE APDU to the IDL. '00 84 00 00 08' 6. Send the given MUTUAL AUTHENTICATE APDU to the IDL. The field <Data> shall be computed with the challenge returned in step 5 and the reference string for the IDL under test. The P2 byte is set to a wrong value. The <Lc> and <Le> fields can be 0x28 or 0x38 depending of the BAP configuration. '00 82 00 60 <Lc> <Data> <Le>' 7. Send the given GET CHALLENGE APDU to the IDL. '00 84 00 00 08' 8. Send the given MUTUAL AUTHENTICATE APDU to the IDL. The field <Data> shall be computed with the challenge returned in step 7 and the reference string for the IDL under test. The <Lc> field is set to a wrong value (advice: use Lc = Lc+1). The <Le> field can be 0x28 or 0x38 depending of the BAP configuration. '00 82 00 00 <Lc> <Data> <Le>'
Expected results	1. The IDL shall return 8 random bytes of content data and status bytes '90 00'. 2. The IDL shall return an ISO warning or ISO checking error.

	3. The IDL shall return 8 random bytes of content data and status bytes ’90 00’. 4. The IDL shall return an ISO warning or ISO checking error. 5. The IDL shall return 8 random bytes of content data and status bytes ’90 00’. 6. The IDL shall return an ISO warning or ISO checking error. 7. The IDL shall return 8 random bytes of content data and status bytes ’90 00’. 8. The IDL shall return an ISO warning or ISO checking error.

B.3.3.6 Test case SE_ISO7816_BAP_6

Test – ID	SE_ISO7816_BAP_6
Purpose	Checking the response to the MUTUAL AUTHENTICATE command with a corrupted MAC.
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall not have been performed.
Test scenario	1. Send the given GET CHALLENGE APDU to the IDL. ’00 84 00 00 08’ 2. Send the given MUTUAL AUTHENTICATE APDU to the IDL. The field <Data> shall be computed with the challenge returned in step 1 and the reference string for the IDL under test. The very last bit of the computed MAC is incremented by 1. The <Lc> and <Le> fields can be 0x28 or 0x38 depending of the BAP configuration. ’00 82 00 00 <Lc> <Data> <Le>’
Expected results	1. The IDL shall return 8 random bytes of content data and status bytes ’90 00’. 2. The IDL shall return an ISO warning or ISO checking error.

B.3.3.7 Test case SE_ISO7816_BAP_7

Test – ID	SE_ISO7816_BAP_7
Purpose	Checking the Secure Messaging encoding of a READ BINARY with short EF ID.
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY APDU to the IDL. ’0C B0 9E 00 0D 97 01 06 8E 08 <Checksum> 00’ 2. Search for the cryptogram DO encoded in tag ‘87’ and decrypt it with current session key. 3. Search for the processing status DO encoded in tag ‘99’ and verify status bytes received. 4. Search for the cryptographic checksum DO encoded in tag ‘8E’ and verify it with the current session key. 5. Search for further DO.
Expected	1. The IDL shall return status bytes ’90 00’.

results	2. The response of step 1 shall contain the read data in a valid cryptogram encoded in tag ‘87’. 3. The response of step 1 should contain SW1-SW2 encoded in tag ‘99’ that equals the status bytes of the secured response. 4. The response of step 1 shall contain a valid cryptographic checksum encoded in tag ‘8E’. 5. The response shall not contain any further data.

B.3.3.8 Test case SE_ISO7816_BAP_8

Test – ID	SE_ISO7816_BAP_8
Purpose	Checking the Secure Messaging encoding of a READ BINARY OddIns (‘B1’) with short EF ID.
Version	1.0
Profile	BAP, OddIns
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY OddIns APDU to the IDL. ’0C B1 00 1E <Lc> 85 <L_{85}> <Cryptogram> 97 01 06 8E 08 <Checksum> 00’ • <Lc> depends of the BAP configuration • <Cryptogram> is encrypted offset DO with padding data. Offset DO is ’54 01 00‘ 2. Search for the cryptogram DO encoded in tag ‘85’ and decrypt it with current session key. 3. Search for the processing status DO encoded in tag ‘99’ and verify status bytes received. 4. Search for the cryptographic checksum DO encoded in tag ‘8E’ and verify it with the current session key. 5. Search for further DO.
Expected results	1. The IDL shall return status bytes ’90 00’. 2. The response of step 1 shall contain the read data in a valid cryptogram encoded in tag ‘85’. The data shall be encapsulated in DO ‘53’. 3. The response of step 1 should contain SW1-SW2 encoded in tag ‘99’ that equals the status bytes of the secured response. 4. The response of step 1 shall contain a valid cryptographic checksum encoded in tag ‘8E’. 5. The response shall not contain any further data but the response trailer.

B.3.3.9 Test case SE_ISO7816_BAP_9

Test – ID	SE_ISO7816_BAP_9
Purpose	Checking the Secure Messaging encoding of a READ BINARY without short EF ID.
Version	1.0
Profile	BAP

Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given SELECT APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 1E' 2. Search for the processing status DO encoded in tag '99' and verify status bytes received. 3. Search for the cryptographic checksum DO encoded in tag '8E' and verify it with the current session key. 4. Send the given READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 06 8E 08 <Checksum> 00' 5. Search for the cryptogram DO encoded in tag '87' and decrypt it with current session key. 6. Search for the processing status DO encoded in tag '99' and verify status bytes received. 7. Search for the cryptographic checksum DO encoded in tag '8E' and verify it with the current session key. 8. Search for further DO.
Expected results	1. The IDL shall return status bytes '90 00'. 2. The response of step 1 should contain SW1-SW2 encoded in tag '99' that equals the status bytes of the secured response. 3. The response of step 1 shall contain a valid cryptographic checksum encoded in tag '8E'. 4. The IDL shall return status bytes '90 00'. 5. The response of step 4 shall contain the read data in a valid cryptogram encoded in tag '87'. 6. The response of step 4 should contain SW1-SW2 encoded in tag '99' that equals the status bytes of the secured response. 7. The response of step 4 shall contain a valid cryptographic checksum encoded in tag '8E'. 8. The response shall not contain any further data but the response trailer.

B.3.3.10 Test case SE_ISO7816_BAP_10

Test – ID	SE_ISO7816_BAP_10
Purpose	Checking the Secure Messaging encoding of a READ BINARY OddIns ('B1') without short EF ID.
Version	1.0
Profile	BAP, OddIns
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given SELECT APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 1E' 2. Search for the processing status DO encoded in tag '99' and verify status bytes

	received. 3. Search for the cryptographic checksum DO encoded in tag '8E' and verify it with the current session key. 4. Send the given READ BINARY OddIns APDU to the IDL. '0C B1 00 00 <Lc> 85 <L_{85}> <Cryptogram> 97 01 06 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following encoded offset : '54 01 00' 5. Search for the cryptogram DO encoded in tag '85' and decrypt it with current session key. 6. Search for the processing status DO encoded in tag '99' and verify status bytes received. 7. Search for the cryptographic checksum DO encoded in tag '8E' and verify it with the current session key. 8. Search for further DO.
Expected results	1. The IDL shall return status bytes '90 00'. 2. The response of step 1 should contain SW1-SW2 encoded in tag '99' that equals the status bytes of the secured response. 3. The response of step 1 shall contain a valid cryptographic checksum encoded in tag '8E'. 4. The IDL shall return status bytes '90 00'. 5. The response of step 4 shall contain the read data in a valid cryptogram encoded in tag '85'. The data shall be encapsulated in DO '53'. 6. The response of step 4 should contain SW1-SW2 encoded in tag '99' that equals the status bytes of the secured response. 7. The response of step 4 shall contain a valid cryptographic checksum encoded in tag '8E'. 8. The response shall not contain any further data but the response trailer.

B.3.3.11 Test case SE_ISO7816_BAP_11

Test – ID	SE_ISO7816_BAP_11
Purpose	Checking the Secure Messaging handling while basic access is granted for the SELECT Command (checksum missing).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given SELECT APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 1E' 2. To verify that the error in step 1 has terminated the SM session, send a valid SM APDU (READ BINARY) to the IDL. '0C B0 9E 00 0D 97 01 06 8E 08 <Checksum> 00'
Expected results	1. The Secure Messaging session is broken and the session keys are no longer valid. The IDL shall return an ISO_Checking_Error in a plain unprotected

	response APDU. 2. The IDL shall return an ISO checking error in a plain unprotected response APDU.

B.3.3.12 Test case SE_ISO7816_BAP_12

Test – ID	SE_ISO7816_BAP_12
Purpose	Checking the Secure Messaging handling while basic access is granted for the SELECT Command (checksum corrupted).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given SELECT APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <CorruptedChecksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 1E' • <CorruptedChecksum> is a valid checksum which has its last byte incremented by one 2. To verify that the error in step 1 has terminated the SM session, send a valid SM APDU (READ BINARY) to the IDL. '0C B0 9E 00 0D 97 01 06 8E 08 <Checksum> 00'
Expected results	1. The Secure Messaging session is broken and the session keys are no longer valid. The IDL shall return an ISO_Checking_Error in a plain unprotected response APDU. 2. The IDL shall return an ISO checking error in a plain unprotected response APDU.

B.3.3.13 Test case SE_ISO7816_BAP_13

Test – ID	SE_ISO7816_BAP_13
Purpose	Checking the Secure Messaging handling while basic access is granted for the SELECT Command (bad Send Sequence Counter).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given SELECT APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <CorruptedChecksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 1E' • <CorruptedChecksum> is computed with a Send Sequence Counter that is not incremented 2. To verify that the error in step 1 has terminated the SM session, send a valid

	SM APDU (READ BINARY) to the IDL. '0C B0 9E 00 0D 97 01 06 8E 08 <Checksum> 00'
Expected results	1. The Secure Messaging session is broken and the session keys are no longer valid. The IDL shall return an ISO_Checking_Error in a plain unprotected response APDU. 2. The IDL shall return an ISO checking error in a plain unprotected response APDU.

B.3.3.14 Test case SE_ISO7816_BAP_14

Test – ID	SE_ISO7816_BAP_14
Purpose	Checking the Secure Messaging handling while basic access is granted for the SELECT Command (invalid class byte).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given SELECT APDU to the IDL. '8C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 1E' 2. If the error code in step 1 was returned in a Secure Messaging response, verify that the secure messaging session has not been aborted. If a plain error code was returned, this step is skipped. Send a valid SM APDU (READ BINARY) to the IDL. '0C B0 00 00 0D 97 01 06 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return an ISO checking error. Note that the behaviour of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. 2. If this step is not skipped, the IDL shall return an ISO checking error in valid Secure Messaging response APDU.

B.3.3.15 Test case SE_ISO7816_BAP_15

Test – ID	SE_ISO7816_BAP_15
Purpose	Checking the enforcement of the Secure Messaging handling while basic access is granted for the SELECT Command.
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given SELECT APDU to the IDL. '00 A4 02 0C 02 00 1E' 2. To verify that the error in step 1 has terminated the SM session, send a valid SM APDU (READ BINARY) to the IDL. '0C B0 9E 00 0D 97 01 06 8E 08 <Checksum> 00'

Expected results	1. The Secure Messaging session is broken and the session keys are no longer valid. The IDL shall return an ISO checking error or '90 00' in a plain unprotected response APDU. 2. The IDL shall return an ISO checking error in a plain unprotected response APDU.

B.3.3.16 Test case SE_ISO7816_BAP_16

Test – ID	SE_ISO7816_BAP_16
Purpose	Checking the Secure Messaging handling while basic access is granted for the READ BINARY Command (checksum missing).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '0C B0 9E 00 03 97 01 06 00' 2. To verify that the error in step 1 has terminated the SM session, send a valid SM APDU (READ BINARY) to the IDL. '0C B0 9E 00 0D 97 01 06 8E 08 <Checksum> 00'
Expected results	1. The Secure Messaging session is broken and the session keys are no longer valid. The IDL shall return an ISO_Checking_Error in a plain unprotected response APDU. 2. The IDL shall return an ISO checking error in a plain unprotected response APDU.

B.3.3.17 Test case SE_ISO7816_BAP_17

Test – ID	SE_ISO7816_BAP_17
Purpose	Checking the Secure Messaging handling while basic access is granted for the READ BINARY Command (checksum corrupted).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY APDU to the IDL. ' 0C B0 9E 00 0D 97 01 06 8E 08 <CorruptedChecksum> 00' • <CorruptedChecksum> is a valid checksum which has its last byte incremented by one 2. To verify that the error in step 1 has terminated the SM session, send a valid SM APDU (READ BINARY) to the IDL. '0C B0 9E 00 0D 97 01 06 8E 08 <Checksum> 00'
Expected results	1. The Secure Messaging session is broken and the session keys are no longer valid. The IDL shall return an ISO_Checking_Error in a plain unprotected response APDU. 2. The IDL shall return an ISO checking error in a plain unprotected response APDU.

B.3.3.18 Test case SE_ISO7816_BAP_18

Test – ID	SE_ISO7816_BAP_18
Purpose	Checking the Secure Messaging handling while basic access is granted for the READ BINARY Command (invalid class byte).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted.
Test scenario	1. Send the given READ BINARY APDU to the IDL. '8C B0 9E 00 0D 97 01 06 8E 08 <Checksum> 00' 2. If the error code in step 1 was returned in a Secure Messaging response, verify that the secure messaging session has not been aborted. If a plain error code was returned, this step is skipped. Send a valid SM APDU (READ BINARY) to the IDL. '0C B0 9E 00 0D 97 01 06 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return an ISO checking error. Note that the behaviour of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. 2. If this step is not skipped, the IDL shall return '90 00' in valid Secure Messaging response APDU.

B.3.4 Test Unit SE_ISO7816_SelEFSM – Protected SELECT EF Command

This unit verifies the implementation of the protected SELECT EF command. The IDL shall be BAP protected.

For all test cases of unit test ISO7816_SelEFSM, basic access shall be granted as tested in ISO7816_BAP_2. All APDUs shall be correctly encoded for Secure Messaging and the IDL responses shall be decoded correctly again.

NOTE If the IDL is EAP protected most of the tests of this unit should be adapted, because each certificate of the the certificates chain contains authorization access rights bytes that describes data group access rights. In these specific cases, the EAP process shall be done just next to the BAP process.

B.3.4.1 Test case SE_ISO7816_SelEFSM_1

Test – ID	SE_ISO7816_SelEFSM_1
Purpose	Checking the SELECT (EF.COM) command (positive test).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF.COM APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier :

	’00 1E’ 2. To verify that EF.COM is selected send a valid READ BINARY APDU to the IDL. ’0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00’
Expected results	1. The IDL shall return the status bytes’90 00’ in valid Secure Messaging response. 2. The IDL shall return byte ‘60’ and the status bytes ’90 00’ in valid Secure Messaging response.

B.3.4.2 Test case SE_ISO7816_SelEFSM_2

Test – ID	SE_ISO7816_SelEFSM_2
Purpose	Checking the robustness of the SELECT command (invalid class byte).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF.COM APDU to the IDL. ’80 A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00’ • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : ’00 1E’ 2. If the error code in step 1 was returned in a Secure Messaging response, verify that the secure messaging session has not been aborted and EF.COM is not selected. If a plain error code was returned, this step is skipped. Send a valid SM APDU (READ BINARY) to the IDL. ’0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00’
Expected results	1. The IDL shall return an ISO checking error. Note that the behaviour of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. 2. If this step is not skipped, the IDL shall return an ISO checking error in valid Secure Messaging response APDU.

B.3.4.3 Test case SE_ISO7816_SelEFSM_3

Test – ID	SE_ISO7816_SelEFSM_3
Purpose	Checking the robustness of the SELECT command (invalid parameter P1).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF.COM APDU to the IDL. ’0C A4 12 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00’ • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : ’00 1E’

	2. To verify that EF.COM is not selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return an ISO checking error in valid Secure Messaging response. 2. The IDL shall return an ISO checking error in valid Secure Messaging response.

B.3.4.4 Test case SE_ISO7816_SelEFSM_4

Test – ID	SE_ISO7816_SelEFSM_4
Purpose	Checking the robustness of the SELECT command (invalid parameter P2).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF.COM APDU to the IDL. '0C A4 02 1C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 1E' 2. To verify that EF.COM is not selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return an ISO checking error in valid Secure Messaging response. 2. The IDL shall return an ISO checking error in valid Secure Messaging response.

B.3.4.5 Test case SE_ISO7816_SelEFSM_5

Test – ID	SE_ISO7816_SelEFSM_5
Purpose	Checking the robustness of the SELECT command (invalid Lc).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF.COM APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following malformated file identifier : '00 1E 01' 2. To verify that EF.COM is not selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'

Expected results	1. The IDL shall return an ISO checking error in valid Secure Messaging response. 2. The IDL shall return an ISO checking error in valid Secure Messaging response.

B.3.4.6 Test case SE_ISO7816_SelEFSM_6

Test – ID	SE_ISO7816_SelEFSM_6
Purpose	Checking the SELECT (EF.SOD) command (positive test).
Version	1.0
Profile	BAP, PA
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF.SOD APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 1D' 2. To verify that EF.SOD is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes 90 00' in valid Secure Messaging response. 2. The IDL shall return byte '77' and the status bytes '90 00' in valid Secure Messaging response.

B.3.4.7 Test case SE_ISO7816_SelEFSM_7

Test – ID	SE_ISO7816_SelEFSM_7
Purpose	Checking the SELECT (EF.DG1) command (positive test).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT DG1 APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 01' 2. To verify that EF. DG1 is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return byte '61' and the status bytes '90 00' in valid Secure Messaging response.

B.3.4.8 Test case SE_ISO7816_SelEFSM_8

Test – ID	SE_ISO7816_SelEFSM_8
Purpose	Checking the SELECT (EF.DG2) command (positive test).
Version	1.0
Profile	BAP, DG2
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF.DG2 APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 02' 2. To verify that EF. DG2 is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return byte '6B' and the status bytes '90 00' in valid Secure Messaging response.

B.3.4.9 Test case SE_ISO7816_SelEFSM_9

Test – ID	SE_ISO7816_SelEFSM_9
Purpose	Checking the SELECT (EF.DG3) command (positive test).
Version	1.0
Profile	BAP, DG3
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF. DG3 APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 03' 2. To verify that EF. DG3 is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return byte '6C' and the status bytes '90 00' in valid Secure Messaging response.

B.3.4.10 Test case SE_ISO7816_SelEFSM_10

Test – ID	SE_ISO7816_SelEFSM_10
Purpose	Checking the SELECT (EF.DG4) command (positive test).

Version	1.0
Profile	BAP, DG4
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF. DG4 APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 04' 2. To verify that EF. DG4 is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return byte '65' and the status bytes '90 00' in valid Secure Messaging response.

B.3.4.11 Test case SE_ISO7816_SelEFSM_11

Test – ID	SE_ISO7816_SelEFSM_11
Purpose	Checking the SELECT (EF.DG5) command (positive test).
Version	1.0
Profile	BAP, DG5
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF. DG5 APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 05' 2. To verify that EF. DG5 is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return byte '67' and the status bytes '90 00' in valid Secure Messaging response.

B.3.4.12 Test case SE_ISO7816_SelEFSM_12

Test – ID	SE_ISO7816_SelEFSM_12
Purpose	Checking the SELECT (EF.DG6) command (positive test).
Version	1.0
Profile	BAP, DG6
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.

Test scenario	1. Send the given SELECT EF. DG6 APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 06' 2. To verify that EF. DG6 is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return byte '75' and the status bytes '90 00' in valid Secure Messaging response.

B.3.4.13 Test case SE_ISO7816_SelEFSM_13

Test – ID	SE_ISO7816_SelEFSM_13
Purpose	Checking the SELECT (EF.DG7) command (positive test).
Version	1.0
Profile	BAP, DG7
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF. DG7 APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 07' 2. To verify that EF. DG7 is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return byte '63' and the status bytes '90 00' in valid Secure Messaging response.

B.3.4.14 Test case SE_ISO7816_SelEFSM_14

Test – ID	SE_ISO7816_SelEFSM_14
Purpose	Checking the SELECT (EF.DG8) command (positive test).
Version	1.0
Profile	BAP, DG8
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF. DG8 APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 08'

	2. To verify that EF. DG8 is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return byte '76' and the status bytes '90 00' in valid Secure Messaging response.

B.3.4.15 Test case SE_ISO7816_SelEFSM_15

Test – ID	SE_ISO7816_SelEFSM_15
Purpose	Checking the SELECT (EF.DG9) command (positive test).
Version	1.0
Profile	BAP, DG9
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF. DG9 APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 09' 2. To verify that EF. DG9 is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return byte '70' and the status bytes '90 00' in valid Secure Messaging response.

B.3.4.16 Test case SE_ISO7816_SelEFSM_16

Test – ID	SE_ISO7816_SelEFSM_16
Purpose	Checking the SELECT (EF.DG10) command (positive test).
Version	1.0
Profile	BAP, DG10
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF. DG10 APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 0A' 2. To verify that EF. DG10 is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return 1 byte and the status bytes '90 00' in valid Secure

	Messaging response.

B.3.4.17 Test case SE_ISO7816_SelEFSM_17

Test – ID	SE_ISO7816_SelEFSM_17
Purpose	Checking the SELECT (EF.DG11) command (positive test).
Version	1.0
Profile	BAP, DG11
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF. DG11 APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 0B' 2. To verify that EF. DG11 is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return the DG11 template tag and the status bytes '90 00' in valid Secure Messaging response.

B.3.4.18 Test case SE_ISO7816_SelEFSM_18

Test – ID	SE_ISO7816_SelEFSM_18
Purpose	Checking the SELECT (EF.DG12) command (positive test).
Version	1.0
Profile	BAP, NMA
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF. DG12 APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 0C' 2. To verify that EF. DG12 is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return byte '71' and the status bytes '90 00' in valid Secure Messaging response.

B.3.4.19 Test case SE_ISO7816_SelEFSM_19

Test – ID	SE_ISO7816_SelEFSM_19
Purpose	Checking the SELECT (EF.DG13) command (positive test).
Version	1.0
Profile	BAP, AA
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF. DG13 APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 0D' 2. To verify that EF. DG13 is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return byte '6F' and the status bytes '90 00' in valid Secure Messaging response.

B.3.4.20 Test case SE_ISO7816_SelEFSM_20

Test – ID	SE_ISO7816_SelEFSM_20
Purpose	Checking the SELECT (EF.DG14) command (positive test).
Version	1.0
Profile	BAP, EAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF. DG14 APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 0E' 2. To verify that EF. DG14 is selected send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return byte '6E' and the status bytes '90 00' in valid Secure Messaging response.

B.3.4.21 Test case SE_ISO7816_SelEFSM_21

Test – ID	SE_ISO7816_SelEFSM_21
Purpose	Checking the SELECT command when the file to be selected does not exist.
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT a file that doesn't exist to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '02 02'
Expected results	1. The IDL shall return an ISO checking error in valid Secure Messaging response.

B.3.5 Test Unit SE_ISO7816_ReadEFSM – Protected READ BINARY Command

This unit verifies the implementation of the protected READ BINARY command. The IDL shall be BAP protected.

For all test cases of unit test ISO7816_ReadEFSM, basic access shall be granted as tested in ISO7816_BAP_2. All APDUs shall be correctly encoded for Secure Messaging and the IDL responses shall be decoded correctly again.

NOTE If the IDL is EAP protected most of the tests of this unit should be adapted, because each certificate of the the certificates chain contains authorization access rights bytes that describes datagroup access rights. In these specific cases, the EAP process shall be performed just after the BAP process.

B.3.5.1 Test case SE_ISO7816_ReadEFSM_1

Test – ID	SE_ISO7816_ReadEFSM_1
Purpose	Checking the READ BINARY command without short EF ID (positive test).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF.COM APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 1E' 2. Read the first byte of EF.COM; send a valid READ BINARY APDU to the IDL. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'

Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return byte '60' and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.2 Test case SE_ISO7816_ReadEFSM_2

Test – ID	SE_ISO7816_ReadEFSM_2
Purpose	Checking the robustness of the READ BINARY command without short EF ID (invalid class byte).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF.COM APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 1E' 2. Send a valid SM APDU (READ BINARY) to the IDL. '80 B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return an ISO checking error. Note that the behaviour of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response.

B.3.5.3 Test case SE_ISO7816_ReadEFSM_3

Test – ID	SE_ISO7816_ReadEFSM_3
Purpose	Checking the robustness of the READ BINARY command without short EF ID (offset beyond EOF).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF.COM APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 1E' 2. Send a valid SM APDU (READ BINARY) to the IDL. '0C B0 7F FF 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return '6B 00'in valid Secure Messaging response.

B.3.5.4 Test case SE_ISO7816_ReadEFSM_4

Test – ID	SE_ISO7816_ReadEFSM_4
Purpose	Checking the robustness of the READ BINARY command without short EF ID (Le beyond EOF).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given SELECT EF.COM APDU to the IDL. '0C A4 02 0C <Lc> 87 <L_{87}> <Cryptogram> 8E 08 <Checksum> 00' • <Lc> depends of the BAP configuration • <Cryptogram> contains the following file identifier : '00 1E' 2. Send a valid SM APDU (READ BINARY) to the IDL. The Le Byte requests more data than available in the EF.COM file. Note: Since the actual file on the IDL could be larger than necessary, the IDL may return valid data in this case. If this happens, the test may have to be repeated with an appropriated offset. '0C B0 00 00 0D 97 01 E0 8E 08 <Checksum> 00'
Expected results	1. The IDL shall return the status bytes'90 00' in valid Secure Messaging response. 2. The IDL shall return status bytes '90 00' or an ISO warning or an ISO checking error.

B.3.5.5 Test case SE_ISO7816_ReadEFSM_5

Test – ID	SE_ISO7816_ReadEFSM_5
Purpose	Checking the READ BINARY (EF.COM) command with short EF ID (positive test)
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.COM. '0C B0 9E 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return byte '60' and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.6 Test case SE_ISO7816_ReadEFSM_6

Test – ID	SE_ISO7816_ReadEFSM_6
Purpose	Checking the READ BINARY (EF.SOD) command with short EF ID (positive test).

Version	1.0
Profile	BAP, PA
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.SOD. '0C B0 9D 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return byte '77' and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.7 Test case SE_ISO7816_ReadEFSM_7

Test – ID	SE_ISO7816_ReadEFSM_7
Purpose	Checking the READ BINARY (EF.DG1) command with short EF ID (positive test).
Version	1.0
Profile	BAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.DG1. '0C B0 81 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return byte '61' and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.8 Test case SE_ISO7816_ReadEFSM_8

Test – ID	SE_ISO7816_ReadEFSM_8
Purpose	Checking the READ BINARY (EF.DG2) command with short EF ID (positive test).
Version	1.0
Profile	BAP, DG2
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.DG2. '0C B0 82 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return byte '6B' and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.9 Test case SE_ISO7816_ReadEFSM_9

Test – ID	SE_ISO7816_ReadEFSM_9
Purpose	Checking the READ BINARY (EF.DG3) command with short EF ID (positive test).
Version	1.0
Profile	BAP, DG3
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.DG3. '0C B0 83 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return byte '6C' and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.10 Test case SE_ISO7816_ReadEFSM_10

Test – ID	SE_ISO7816_ReadEFSM_10
Purpose	Checking the READ BINARY (EF.DG4) command with short EF ID (positive test).
Version	1.0
Profile	BAP, DG4
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.DG4. '0C B0 84 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return byte '65' and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.11 Test case SE_ISO7816_ReadEFSM_11

Test – ID	SE_ISO7816_ReadEFSM_11
Purpose	Checking the READ BINARY (EF.DG5) command with short EF ID (positive test).
Version	1.0
Profile	BAP, DG5
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.DG5. '0C B0 85 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected	1. The IDL shall return byte '67' and the status bytes '90 00' in valid Secure

results	Messaging response.

B.3.5.12 Test case SE_ISO7816_ReadEFSM_12

Test – ID	SE_ISO7816_ReadEFSM_12
Purpose	Checking the READ BINARY (EF.DG6) command with short EF ID (positive test).
Version	1.0
Profile	BAP, DG6
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.DG6. '0C B0 86 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return byte '75' and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.13 Test case SE_ISO7816_ReadEFSM_13

Test – ID	SE_ISO7816_ReadEFSM_13
Purpose	Checking the READ BINARY (EF.DG7) command with short EF ID (positive test).
Version	1.0
Profile	BAP, DG7
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.DG7. '0C B0 87 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return byte '63' and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.14 Test case SE_ISO7816_ReadEFSM_14

Test – ID	SE_ISO7816_ReadEFSM_14
Purpose	Checking the READ BINARY (EF.DG8) command with short EF ID (positive test).
Version	1.0
Profile	BAP, DG8
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.

Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.DG8. '0C B0 88 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return byte '76' and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.15 Test case SE_ISO7816_ReadEFSM_15

Test – ID	SE_ISO7816_ReadEFSM_15
Purpose	Checking the READ BINARY (EF.DG9) command with short EF ID (positive test).
Version	1.0
Profile	BAP, DG9
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.DG9. '0C B0 89 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return byte '70' and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.16 Test case SE_ISO7816_ReadEFSM_16

Test – ID	SE_ISO7816_ReadEFSM_16
Purpose	Checking the READ BINARY (EF.DG10) command with short EF ID (positive test).
Version	1.0
Profile	BAP, DG10
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.DG10. '0C B0 8A 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return 1 byte of data content and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.17 Test case SE_ISO7816_ReadEFSM_17

Test – ID	SE_ISO7816_ReadEFSM_17
Purpose	Checking the READ BINARY (EF.DG11) command with short EF ID (positive test).
Version	1.0

Profile	BAP, DG11
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.DG11. '0C B0 8B 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return the DG11 template tag and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.18 Test case SE_ISO7816_ReadEFSM_18

Test – ID	SE_ISO7816_ReadEFSM_18
Purpose	Checking the READ BINARY (EF.DG12) command with short EF ID (positive test).
Version	1.0
Profile	BAP, NMA
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.DG12. '0C B0 8C 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return byte '71' and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.19 Test case SE_ISO7816_ReadEFSM_19

Test – ID	SE_ISO7816_ReadEFSM_19
Purpose	Checking the READ BINARY (EF.DG13) command with short EF ID (positive test).
Version	1.0
Profile	BAP, AA
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.DG13. '0C B0 8D 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return byte '6F' and the status bytes '90 00' in valid Secure Messaging response.

B.3.5.20 Test case SE_ISO7816_ReadEFSM_20

Test – ID	SE_ISO7816_ReadEFSM_20

Purpose	Checking the READ BINARY (EF.DG14) command with short EF ID (positive test).
Version	1.0
Profile	BAP, EAP
Preconditions	1. LDS application shall be selected and basic access shall be granted. 2. An EF shall not be selected.
Test scenario	1. Send the given READ BINARY short EF ID APDU to the IDL to read the first byte of EF.DG14. '0C B0 8E 00 <Lc> 97 01 01 8E 08 <Checksum>
Expected results	1. The IDL shall return byte '6E' and the status bytes '90 00' in valid Secure Messaging response.

B.3.6 Test Unit SE_ISO7816_SelEF – Unprotected SELECT EF Command

This unit verifies the implementation of the unprotected SELECT EF command. It is only applicable to the plain profile.

B.3.6.1 Test case SE_ISO7816_SelEF_1

Test – ID	SE_ISO7816_SelEF_1
Purpose	This test case verifies the SELECT (EF.COM) command (positive test).
Version	1.0
Profile	Plain
Preconditions	1. LDS application shall be selected. 2. An EF shall not be selected.
Test scenario	1. EF.COM shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 1E' 2. To verify that EF.COM is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return byte '60' and the status bytes '90 00'.

B.3.6.2 Test case SE_ISO7816_SelEF_2

Test – ID	SE_ISO7816_SelEF_2
Purpose	This test case checks the robustness of the SELECT command (invalid class byte).
Version	1.0
Profile	Plain
Preconditions	1. LDS application shall be selected.

	2. An EF shall not be selected.
Test scenario	1. EF.COM shall be selected. Send the following SELECT APDU to the IDL. The class tag is set to the invalid value of '80'. '80 A4 02 0C 02 00 1E' 2. To verify that EF.COM is not selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return an ISO checking error. 2. The IDL shall return an ISO checking error.

B.3.6.3 Test case SE_ISO7816_SelEF_3

Test – ID	SE_ISO7816_SelEF_3
Purpose	This test case checks the robustness of the SELECT command (invalid parameter P1).
Version	1.0
Profile	Plain
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF.COM shall be selected. Send the following SELECT APDU to the IDL. The parameter P1 is set to the invalid value of '12'. '00 A4 12 0C 02 00 1E' 2. To verify that EF.COM is not selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return an ISO checking error. 2. The IDL shall return an ISO checking error.

B.3.6.4 Test case SE_ISO7816_SelEF_4

Test – ID	SE_ISO7816_SelEF_4
Purpose	This test case checks the robustness of the SELECT command (invalid parameter P2).
Version	1.0
Profile	Plain
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF.COM shall be selected. Send the following SELECT APDU to the IDL. The parameter P2 is set to the invalid value of '1C'. '00 A4 02 1C 02 00 1E' 2. To verify that EF.COM is not selected, send a valid READ BINARY APDU to the

	IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return an ISO checking error. 2. The IDL shall return an ISO checking error.

B.3.6.5 Test case SE_ISO7816_SelEF_5

Test – ID	SE_ISO7816_SelEF_5
Purpose	This test case checks the robustness of the SELECT command (invalid Lc).
Version	1.0
Profile	Plain
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF.COM shall be selected. Send the following SELECT APDU to the IDL. The parameter Lc is set to the invalid value of '03'. '00 A4 02 1C 03 00 1E' 2. To verify that EF.COM is not selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return an ISO checking error. 2. The IDL shall return an ISO checking error.

B.3.6.6 Test case SE_ISO7816_SelEF_6

Test – ID	SE_ISO7816_SelEF_6
Purpose	This test case verifies the SELECT (EF.SOD) command (positive test).
Version	1.0
Profile	Plain, PA
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF.SOD shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 1D' 2. To verify that EF.SOD is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return byte '77' and the status bytes '90 00'.

B.3.6.7 Test case SE_ISO7816_SelEF_7

Test – ID	SE_ISO7816_SelEF_7
Purpose	This test case verifies the SELECT (EF.DG1) command (positive test).
Version	1.0
Profile	Plain
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF. DG1 shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 01' 2. To verify that EF.DG1 is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return byte '61' and the status bytes '90 00'.

B.3.6.8 Test case SE_ISO7816_SelEF_8

Test – ID	SE_ISO7816_SelEF_8
Purpose	This test case verifies the SELECT (EF.DG2) command (positive test).
Version	1.0
Profile	Plain, DG2
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF. DG2 shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 02' 2. To verify that EF.DG2 is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return byte '75' and the status bytes '90 00'.

B.3.6.9 Test case SE_ISO7816_SelEF_9

Test – ID	SE_ISO7816_SelEF_9
Purpose	This test case verifies the SELECT (EF.DG3) command (positive test).
Version	1.0
Profile	Plain, DG3
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.

Test scenario	1. EF. DG3 shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 03' 2. To verify that EF.DG3 is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return byte '63' and the status bytes '90 00'.

B.3.6.10 Test case SE_ISO7816_SelEF_10

Test – ID	SE_ISO7816_SelEF_10
Purpose	This test case verifies the SELECT (EF.DG4) command (positive test).
Version	1.0
Profile	Plain, DG4
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF.DG4 shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 04' 2. To verify that EF.DG4 is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return byte '65' and the status bytes '90 00'.

B.3.6.11 Test case SE_ISO7816_SelEF_11

Test – ID	SE_ISO7816_SelEF_11
Purpose	This test case verifies the SELECT (EF.DG5) command (positive test).
Version	1.0
Profile	Plain, DG5
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF.DG5 shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 05' 2. To verify that EF.DG5 is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return byte '67' and the status bytes '90 00'.

B.3.6.12 Test case SE_ISO7816_SelEF_12

Test – ID	SE_ISO7816_SelEF_12
Purpose	This test case verifies the SELECT (EF.DG6) command (positive test).
Version	1.0
Profile	Plain, DG6
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF.DG6 shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 06' 2. To verify that EF.DG6 is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return byte '75' and the status bytes '90 00'.

B.3.6.13 Test case SE_ISO7816_SelEF_13

Test – ID	SE_ISO7816_SelEF_13
Purpose	This test case verifies the SELECT (EF.DG7) command (positive test).
Version	1.0
Profile	Plain, DG7
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF.DG7 shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 07' 2. To verify that EF.DG7 is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return byte '63' and the status bytes '90 00'.

B.3.6.14 Test case SE_ISO7816_SelEF_14

Test – ID	SE_ISO7816_SelEF_14
Purpose	This test case verifies the SELECT (EF.DG8) command (positive test).
Version	1.0
Profile	Plain, DG8
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.

Test scenario	1. EF.DG8 shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 08' 2. To verify that EF.DG8 is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return byte '76' and the status bytes '90 00'.

B.3.6.15 Test case SE_ISO7816_SelEF_15

Test – ID	SE_ISO7816_SelEF_15
Purpose	This test case verifies the SELECT (EF.DG9) command (positive test).
Version	1.0
Profile	Plain, DG9
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF.DG9 shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 09' 2. To verify that EF.DG9 is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return byte '70' and the status bytes '90 00'.

B.3.6.16 Test case SE_ISO7816_SelEF_16

Test – ID	SE_ISO7816_SelEF_16
Purpose	This test case verifies the SELECT (EF.DG11) command (positive test).
Version	1.0
Profile	Plain, DG11
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF.DG11 shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 0B' 2. To verify that EF.DG11 is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return the byte value of the tag assigned by the issuing authority and the status bytes '90 00'.

B.3.6.17 Test case SE_ISO7816_SelEF_17

Test – ID	SE_ISO7816_SelEF_17
Purpose	This test case verifies the SELECT (EF.DG12) command (positive test).
Version	1.0
Profile	Plain, NMA
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF.DG12 shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 0C' 2. To verify that EF.DG12 is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return byte '71' and the status bytes '90 00'.

B.3.6.18 Test case SE_ISO7816_SelEF_18

Test – ID	SE_ISO7816_SelEF_18
Purpose	This test case verifies the SELECT (EF.DG13) command (positive test).
Version	1.0
Profile	Plain, AA
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF.DG13 shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 0D' 2. To verify that EF.DG13 is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return byte '6F' and the status bytes '90 00'.

B.3.6.19 Test case SE_ISO7816_SelEF_19

Test – ID	SE_ISO7816_SelEF_19
Purpose	This test case verifies the SELECT (EF.DG14) command (positive test).
Version	1.0
Profile	Plain, EAP

Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. EF.DG14 shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 0E' 2. To verify that EF.DG14 is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return byte '6E' and the status bytes '90 00'.

B.3.6.20 Test case SE_ISO7816_SelEF_20

Test – ID	SE_ISO7816_SelEF_20
Purpose	This test case verifies the SELECT command when the file to be selected does not exist.
Version	1.0
Profile	Plain
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. A non existing file shall be selected. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 02 02' 2. To verify that no file is selected, send a valid READ BINARY APDU to the IDL. '00 B0 00 00 01'
Expected results	1. The IDL shall return an ISO checking error. 2. The IDL shall return an ISO checking error.

B.3.7 Test Unit SE_ISO7816_ReadEF – Unprotected READ BINARY Command

This unit verifies the implementation of the unprotected READ BINARY command. It is only applicable to the plain profile.

B.3.7.1 Test case SE_ISO7816_ReadEF_1

Test – ID	SE_ISO7816_ReadEF_1
Purpose	This test case verifies the READ BINARY command (w/o short EF ID) (positive test).
Version	1.0
Profile	Plain
Preconditions	1. The LDS application shall be selected.
Test scenario	1. Send the following SELECT APDU to the IDL.

	'00 A4 02 0C 02 00 1E' 2. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 at maximum) of the EF.COM. '00 B0 00 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return maximum 256 bytes of data followed by status bytes '90 00'.

B.3.7.2 Test case SE_ISO7816_ReadEF_2

Test – ID	SE_ISO7816_ReadEF_2
Purpose	Test the robustness of the READ BINARY command (w/o short EF ID) (invalid class byte).
Version	1.0
Profile	Plain
Preconditions	1. The LDS application is selected. This test case implicitly tests the SELECT command; so it is required that the IDL has previously passed the SELECT Test SE_ISO7816_ReadEF_1, otherwise this test will fail.
Test scenario	1. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 1E' 2. Send the READ BINARY APDU to the IDL. The class byte is set to the invalid value of '80'. '80 B0 00 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return an ISO checking error.

B.3.7.3 Test case SE_ISO7816_ReadEF_3

Test – ID	SE_ISO7816_ReadEF_3
Purpose	Test the robustness of the READ BINARY command (w/o short EF ID) (offset beyond EOF).
Version	1.0
Profile	Plain
Preconditions	1. The LDS application is selected. This test case implicitly tests the SELECT command; so it is required that the IDL has previously passed the SELECT Test SE_ISO7816_ReadEF_1, otherwise this test will fail.
Test scenario	1. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 1E' 2. Send the READ BINARY APDU to the IDL. The offset is beyond the end of

	the EF.COM file. Note: Since the actual file on the IDL could be larger than necessary, the IDL may return valid data in this case. If this happens, the test may have to be repeated with an appropriated offset. '00 B0 7F FF 00'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return an ISO checking error.

B.3.7.4 Test case SE_ISO7816_ReadEF_4

Test – ID	SE_ISO7816_ReadEF_4
Purpose	Test the robustness of the READ BINARY command (w/o short EF ID) (Le beyond EOF).
Version	1.0
Profile	Plain
Preconditions	1. The LDS application is selected. This test case implicitly tests the SELECT command; so it is required that the IDL has previously passed the SELECT Test SE_ISO7816_ReadEF_1, otherwise this test will fail.
Test scenario	1. Send the following SELECT APDU to the IDL. '00 A4 02 0C 02 00 1E' 2. Send the READ BINARY APDU to the IDL. The Le byte is requests more data than available in the EF.COM file. Note: Since the actual file on the IDL could be larger than necessary, the IDL may return valid data in this case. If this happens, the test may have to be repeated with an appropriated offset. '00 B0 00 00 E0'
Expected results	1. The IDL shall return the status bytes '90 00'. 2. The IDL shall return status bytes '90 00', an ISO warning or an ISO checking error.

B.3.7.5 Test case SE_ISO7816_ReadEF_5

Test – ID	SE_ISO7816_ReadEF_5
Purpose	This test case verifies the READ BINARY command (EF.COM short EF ID) (positive test).
Version	1.0
Profile	Plain
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.COM. '00 B0 9E 00 00'

Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.6 Test case SE_ISO7816_ReadEF_6

Test – ID	SE_ISO7816_ReadEF_6
Purpose	This test case verifies the READ BINARY command (EF.SOD short EF ID) (positive test).
Version	1.0
Profile	Plain, PA
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.SOD. '00 B0 9D 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.7 Test case SE_ISO7816_ReadEF_7

Test – ID	SE_ISO7816_ReadEF_7
Purpose	This test case verifies the READ BINARY command (EF.DG1 short EF ID) (positive test).
Version	1.0
Profile	Plain
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.DG1. '00 B0 81 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.8 Test case SE_ISO7816_ReadEF_8

Test – ID	SE_ISO7816_ReadEF_8
Purpose	This test case verifies the READ BINARY command (EF.DG2 short EF ID) (positive test).
Version	1.0
Profile	Plain, DG2

Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.DG2. '00 B0 82 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.9 Test case SE_ISO7816_ReadEF_9

Test – ID	SE_ISO7816_ReadEF_9
Purpose	This test case verifies the READ BINARY command (EF.DG3 short EF ID) (positive test).
Version	1.0
Profile	Plain, DG3
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.DG3. '00 B0 83 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.10 Test case SE_ISO7816_ReadEF_10

Test – ID	SE_ISO7816_ReadEF_10
Purpose	This test case verifies the READ BINARY command (EF.DG4 short EF ID) (positive test).
Version	1.0
Profile	Plain, DG4
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.DG4. '00 B0 84 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.11 Test case SE_ISO7816_ReadEF_11

Test – ID	SE_ISO7816_ReadEF_11
Purpose	This test case verifies the READ BINARY command (EF.DG5 short EF ID)

	(positive test).
Version	1.0
Profile	Plain, DG5
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.DG5. '00 B0 85 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.12 Test case SE_ISO7816_ReadEF_12

Test – ID	SE_ISO7816_ReadEF_12
Purpose	This test case verifies the READ BINARY command (EF.DG6 short EF ID) (positive test).
Version	1.0
Profile	Plain, DG6
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.DG6. '00 B0 86 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.13 Test case SE_ISO7816_ReadEF_13

Test – ID	SE_ISO7816_ReadEF_13
Purpose	This test case verifies the READ BINARY command (EF.DG7 short EF ID) (positive test).
Version	1.0
Profile	Plain, DG7
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.DG7. '00 B0 87 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.14 Test case SE_ISO7816_ReadEF_14

Test – ID	SE_ISO7816_ReadEF_14
Purpose	This test case verifies the READ BINARY command (EF.DG8 short EF ID) (positive test).
Version	1.0
Profile	Plain, DG8
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.DG8. '00 B0 88 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.15 Test case SE_ISO7816_ReadEF_15

Test – ID	SE_ISO7816_ReadEF_15
Purpose	This test case verifies the READ BINARY command (EF.DG9 short EF ID) (positive test).
Version	1.0
Profile	Plain, DG9
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.DG9. '00 B0 89 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.16 Test case SE_ISO7816_ReadEF_16

Test – ID	SE_ISO7816_ReadEF_16
Purpose	This test case verifies the READ BINARY command (EF.DG11 short EF ID) (positive test).
Version	1.0
Profile	Plain, DG11
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.DG11.

	'00 B0 8B 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.17 Test case SE_ISO7816_ReadEF_17

Test – ID	SE_ISO7816_ReadEF_17
Purpose	This test case verifies the READ BINARY command (EF.DG12 short EF ID) (positive test).
Version	1.0
Profile	Plain, NMA
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.DG12. '00 B0 8C 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.18 Test case SE_ISO7816_ReadEF_18

Test – ID	SE_ISO7816_ReadEF_18
Purpose	This test case verifies the READ BINARY command (EF.DG13 short EF ID) (positive test).
Version	1.0
Profile	Plain, AA
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.DG13. '00 B0 8D 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.19 Test case SE_ISO7816_ReadEF_19

Test – ID	SE_ISO7816_ReadEF_19
Purpose	This test case verifies the READ BINARY command (EF.DG14 short EF ID) (positive test).
Version	1.0

Profile	Plain, EAP
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. Send the READ BINARY APDU to the IDL, this will read the first bytes (256 bytes at maximum) of the EF.DG14. '00 B0 8E 00 00'
Expected results	1. The IDL shall return the status bytes '90 00'.

B.3.7.20 Test case SE_ISO7816_ReafEF_20

Test – ID	SE_ISO7816_ReadEF_20
Purpose	This test case verifies the READ BINARY command when the file to be selected does not exist.
Version	1.0
Profile	Plain
Preconditions	1. The LDS application shall be selected. An EF shall not be selected.
Test scenario	1. A non existing file shall be implicitly selected. Send the following READ BINARY APDU to the IDL. '00 B0 92 00 00'
Expected results	1. The IDL shall return an ISO checking error.

B.3.8 Test Unit SE_ISO7816_AA – Active Authentication

B.3.8.1 Test Case SE_ISO7816_AA_001

Test Case-ID	SE_ISO7816_AA_001
Purpose	Verify the behaviour of a non-BAP protected IDL in response to the INTERNAL AUTHENTICATE command (positive test).
Version	1.0
References	ISO/IEC 18013-3:2009, 8.2 ISO/IEC 7816-4:2005, 7.5.2
Profile	AA, Plain
Preconditions	1. The LDS application shall have been selected. 2. The ActiveAuthenticationPublicKeyInfo stored in data group 13 shall have been read.
Test Scenario	1. Send the given INTERNAL AUTHENTICATE command to the IDL: '00 88 00 00 08 55 66 77 88 11 22 33 44 00'.
Expected Results	1. Response data and '90 00' (without secure messaging).

B.3.8.2 Test Case SE_ISO7816_AA_002

Test Case-ID	SE_ISO7816_AA_002
Purpose	Verify the behaviour of a BAP protected IDL in response to the INTERNAL AUTHENTICATE command (positive test).
Version	1.0
References	ISO/IEC 18013-3:2009, 8.2 ISO/IEC 7816-4:2005, 7.5.2
Profile	AA BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The ActiveAuthenticationPublicKeyInfo stored in data group 13 shall have been read. 4. All commands are encoded as valid Secure Messaging APDUs.
Test Scenario	1. Send the given INTERNAL AUTHENTICATE command: '0C 88 00 00 <Lc> 87 <L87> 01 <cryptogram> 97 01 00 8E 08 <checksum> 00' <cryptogram> contains the following encrypted data: '55 66 77 88 11 22 33 44'
Expected Results	1. Response data and '90 00' in a valid Secure Messaging response APDU.

B.3.8.3 Test Case SE_ISO7816_AA_003

Test Case-ID	SE_ISO7816_AA_003
Purpose	Verify the behaviour of an IDL in response to the INTERNAL AUTHENTICATE command if RND.IFD < 8 bytes.
Version	1.0
References	ISO/IEC 18013-3:2009, 8.2 ISO/IEC 7816-4:2005, 7.5.2
Profile	AA
Preconditions	1. The LDS application shall have been selected. 2. If BAP is supported, the BAP mechanism shall have been performed. 3. The ActiveAuthenticationPublicKeyInfo stored in data group 13 shall have been read. 4. If BAP is supported, all commands are encoded as valid Secure Messaging APDUs.
Test Scenario	1. Send the INTERNAL AUTHENTICATE command with RND.IFD '11 22 33 44'.
Expected Results	1. ISO checking error. If BAP is supported, the response APDU shall be encoded in a valid Secure Messaging format.

B.3.8.4 Test Case SE_ISO7816_AA_004

Test Case-ID	SE_ISO7816_AA_004
Purpose	Verify the behaviour of an IDL in response to the INTERNAL AUTHENTICATE command if RND.IFD > 8 bytes.
Version	1.0
References	ISO/IEC 18013-3:2009, 8.2 ISO/IEC 7816-4:2005, 7.5.2
Profile	AA
Preconditions	1. The LDS application shall have been selected. 2. If BAP is supported, the BAP mechanism shall have been performed. 3. The ActiveAuthenticationPublicKeyInfo stored in data group 13 shall have been read. 4. If BAP is supported, all commands are encoded as valid Secure Messaging APDUs.
Test Scenario	1. Send the INTERNAL AUTHENTICATE command with RND.IFD '11 22 33 44 55 66 77 88 99'.
Expected Results	1. ISO checking error. If BAP is supported, the response APDU shall be encoded in a valid Secure Messaging format.

B.3.8.5 Test Case SE_ISO7816_AA_005

Test Case-ID	SE_ISO7816_AA_005
Purpose	This test checks the RSA signature that has been generated during Active Authentication.
Version	1.0
References	ISO/IEC 18013-3:2009 ISO/IEC 9796-2 RFC-3280 RFC-3279
Profile	AA AA-RSA
Preconditions	1. EF.DG13 has been retrieved from the IDL. 2. EF.DG13 contains a valid RSA public key. 3. The RND.IFD and the signature that has been generated by the IDL are available.
Test Scenario	1. Obtain the plaintext signature from the Internal Authenticate Response. 2. Decipher the Active Authentication signature using the Public Key from EF.DG13. 3. "Signature Opening" - Check the leftmost 2 bits of the Recoverable String. 4. "Signature Opening" - Check the last byte of the Recoverable String. 5. "Intermediate String Recovery" - Retrieve the number of padding bits from the beginning of the Recoverable String. 6. "Trailer Recovery" - Check the last byte of the Recoverable String. 7. "Hash Code Checking" - Retrieve the hash code from the Recoverable String.
Expected Results	1. The length of the signature shall be in accordance with the length of the public key from EF.DG13. 2. The length of the deciphered signature shall be in accordance with the length of the public key from EF.DG13. 3. The leftmost 2 bits of the Recoverable String shall be equal to '01'b. 4. The rightmost 4 bits of the Recoverable String shall be equal to '1100'b. 5. The number of padding bits equal to '0'b following the 3rd bit of the Recoverable String shall be less than 8. 6. The Trailer of the Recoverable String shall be 'BC' for trailer option 1 or 'CC' for trailer option 2 (ISO/IEC 9796-2 digital Signature Scheme 1, with has HASH according to hash-function identifier). 7. The hash code shall match the hash calculated over M1||M2 (M1 is the nonce that has been generated by the IDL; M2 is RDN.IFD).

B.3.8.6 Test Case SE_ISO7816_AA_006

Test Case-ID	SE_ISO7816_AA_006
Purpose	This test checks the ECDSA signature that has been generated by the IDL during Active Authentication.
Version	1.0
References	ISO/IEC 18013-3:2009 RFC-3280 RFC-3279
Profile	AA AA-ECDSA
Preconditions	1. EF.DG13 has been retrieved from the IDL. 2. EF.DG13 contains a valid EC public key.

Test Scenario	1. Obtain the plaintext signature from the Internal Authenticate Response. 2. Verify the signature using ECDSA SHA-1.
Expected Results	1. The length of the signature shall be in accordance with the length of the public key from EF.DG13. 2. Signature verification shall be successful.

B.3.9 Test Unit SE_ISO7816_SecEAP - Security Conditions for EAP protected IDL

On an EAP protected IDL, some data groups containing for example sensitive biometric data shall be protected by the TA mechanisms. While other data groups are accessible after the BAP mechanism has been performed on a BAP protected IDL or without BAP on a plain IDL, the EAP protected data groups shall only be accessible after a successful TA process.

B.3.9.1 Test case SE_ISO7816_SecEAP_1

Test – ID	SE_ISO7816_SecEAP_1
Purpose	SELECT EF command for EF.DG2 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG2
Preconditions	1. DG2 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given SELECT EF APDU for EF.DG2 to the IDL. Though the CA mechanism has been performed, the access to the DG2 shall be denied. '0C A4 02 0C 15 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted file ID ('00 02').
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.2 Test case SE_ISO7816_SecEAP_2

Test – ID	SE_ISO7816_SecEAP_2
Purpose	READ BINARY command with short EF ID for EF.DG2 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG2
Preconditions	1. DG2 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.

Test scenario	1. Send the given READ BINARY APDU for EF.DG2 (short EF ID '02') to the IDL. Though the CA mechanism has been performed, the access to the DG2 shall be denied. '0C B0 82 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.3 Test case SE_ISO7816_SecEAP_3

Test – ID	SE_ISO7816_SecEAP_3
Purpose	READ BINARY command with odd instruction byte and short EF ID for EF.DG2 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG2, OddIns
Preconditions	1. DG2 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG2 (short EF ID '02') to the IDL. Though the CA mechanism has been performed, the access to the DG2 shall be denied. '0C B1 00 02 17 85 <L_{85}> <Cryptogram> 97 01 01 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted DO 54 with the encoded offset 00 : '54 01 00'
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.4 Test case SE_ISO7816_SecEAP_4

Test – ID	SE_ISO7816_SecEAP_4
Purpose	SELECT EF command for EF.DG3 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG3
Preconditions	1. DG3 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given SELECT EF APDU for EF.DG3 to the IDL. Though the CA mechanism has been performed, the access to the DG3 shall be denied. '0C A4 02 0C 15 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00'

	<Cryptogram> contains the encrypted file ID (’00 03’).
Expected results	1. Checking error ’69 82’ within a valid SM response.

B.3.9.5 Test case SE_ISO7816_SecEAP_5

Test – ID	SE_ISO7816_SecEAP_5
Purpose	READ BINARY command with short EF ID for EF.DG3 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG3
Preconditions	1. DG3 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG3 (short EF ID ‘03’) to the IDL. Though the CA mechanism has been performed, the access to the DG3 shall be denied. ’0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’
Expected results	1. Checking error ’69 82’ within a valid SM response.

B.3.9.6 Test case SE_ISO7816_SecEAP_6

Test – ID	SE_ISO7816_SecEAP_6
Purpose	READ BINARY command with odd instruction byte and short EF ID for EF.DG3 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG3, OddIns
Preconditions	1. DG3 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG3 (short EF ID ‘03’) to the IDL. Though the CA mechanism has been performed, the access to the DG3 shall be denied. ’0C B1 00 03 17 85 <L_{85}> <Cryptogram> 97 01 01 8E 08 <Checksum> 00’ <Cryptogram> contains the encrypted DO 54 with the encoded offset 00 : ’54 01 00’
Expected results	1. Checking error ’69 82’ within a valid SM response.

B.3.9.7 Test case SE_ISO7816_SecEAP_7

Test – ID	SE_ISO7816_SecEAP_7
Purpose	SELECT EF command for EF.DG4 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG4
Preconditions	1. DG4 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given SELECT EF APDU for EF.DG4 to the IDL. Though the CA mechanism has been performed, the access to the DG4 shall be denied. '0C A4 02 0C 15 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted file ID ('00 04').
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.8 Test case SE_ISO7816_SecEAP_8

Test – ID	SE_ISO7816_SecEAP_8
Purpose	READ BINARY command with short EF ID for EF.DG4 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG4
Preconditions	1. DG4 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG4 (short EF ID '04') to the IDL. Though the CA mechanism has been performed, the access to the DG4 shall be denied. '0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.9 Test case SE_ISO7816_SecEAP_9

Test – ID	SE_ISO7816_SecEAP_9
Purpose	READ BINARY command with odd instruction byte and short EF ID for EF.DG4 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG4, OddIns
Preconditions	1. DG4 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG4 (short EF ID '04') to the IDL. Though the CA mechanism has been performed, the access to the DG4 shall be denied. '0C B1 00 04 17 85 <L_{85}> <Cryptogram> 97 01 01 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted DO 54 with the encoded offset 00 : '54 01 00'
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.10 Test case SE_ISO7816_SecEAP_10

Test – ID	SE_ISO7816_SecEAP_10
Purpose	SELECT EF command for EF.DG5 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG5
Preconditions	1. DG5 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given SELECT EF APDU for EF.DG5 to the IDL. Though the CA mechanism has been performed, the access to the DG5 shall be denied. '0C A4 02 0C 15 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted file ID ('00 05').
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.11 Test case SE_ISO7816_SecEAP_11

Test – ID	SE_ISO7816_SecEAP_11
Purpose	READ BINARY command with short EF ID for EF.DG5 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG5
Preconditions	1. DG5 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG5 (short EF ID '05') to the IDL. Though the CA mechanism has been performed, the access to the DG5 shall be denied. '0C B0 85 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.12 Test case SE_ISO7816_SecEAP_12

Test – ID	SE_ISO7816_SecEAP_12
Purpose	READ BINARY command with odd instruction byte and short EF ID for EF.DG5 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG5, OddIns
Preconditions	1. DG5 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG5 (short EF ID '05') to the IDL. Though the CA mechanism has been performed, the access to the DG5 shall be denied. '0C B1 00 05 17 85 <L_{85}> <Cryptogram> 97 01 01 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted DO 54 with the encoded offset 00 : '54 01 00'
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.13 Test case SE_ISO7816_SecEAP_13

Test – ID	SE_ISO7816_SecEAP_13
Purpose	SELECT EF command for EF.DG6 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG6
Preconditions	1. DG6 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given SELECT EF APDU for EF.DG6 to the IDL. Though the CA mechanism has been performed, the access to the DG6 shall be denied. '0C A4 02 0C 15 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted file ID ('00 06').
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.14 Test case SE_ISO7816_SecEAP_14

Test – ID	SE_ISO7816_SecEAP_14
Purpose	READ BINARY command with short EF ID for EF.DG6 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG6
Preconditions	1. DG6 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG6 (short EF ID '06') to the IDL. Though the CA mechanism has been performed, the access to the DG6 shall be denied. '0C B0 86 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.15 Test case SE_ISO7816_SecEAP_15

Test – ID	SE_ISO7816_SecEAP_15

Purpose	READ BINARY command with odd instruction byte and short EF ID for EF.DG6 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG6, OddIns
Preconditions	1. DG6 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG6 (short EF ID '06') to the IDL. Though the CA mechanism has been performed, the access to the DG6 shall be denied. '0C B1 00 06 17 85 <L_{85}> <Cryptogram> 97 01 01 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted DO 54 with the encoded offset 00 : '54 01 00'
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.16 Test case SE_ISO7816_SecEAP_16

Test – ID	SE_ISO7816_SecEAP_16
Purpose	SELECT EF command for EF.DG7 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG7
Preconditions	1. DG7 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given SELECT EF APDU for EF.DG7 to the IDL. Though the CA mechanism has been performed, the access to the DG7 shall be denied. '0C A4 02 0C 15 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted file ID ('00 07').
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.17 Test case SE_ISO7816_SecEAP_17

Test – ID	SE_ISO7816_SecEAP_17
Purpose	READ BINARY command with short EF ID for EF.DG7 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG7
Preconditions	1. DG7 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG7 (short EF ID '07') to the IDL. Though the CA mechanism has been performed, the access to the DG7 shall be denied. '0C B0 87 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.18 Test case SE_ISO7816_SecEAP_18

Test – ID	SE_ISO7816_SecEAP_18
Purpose	READ BINARY command with odd instruction byte and short EF ID for EF.DG7 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG7, OddIns
Preconditions	1. DG7 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG7 (short EF ID '07') to the IDL. Though the CA mechanism has been performed, the access to the DG7 shall be denied. '0C B1 00 07 17 85 <L_{85}> <Cryptogram> 97 01 01 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted DO 54 with the encoded offset 00 : '54 01 00'
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.19 Test case SE_ISO7816_SecEAP_19

Test – ID	SE_ISO7816_SecEAP_19
Purpose	SELECT EF command for EF.DG8 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG8
Preconditions	1. DG8 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given SELECT EF APDU for EF.DG8 to the IDL. Though the CA mechanism has been performed, the access to the DG8 shall be denied. '0C A4 02 0C 15 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted file ID ('00 08').
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.20 Test case SE_ISO7816_SecEAP_20

Test – ID	SE_ISO7816_SecEAP_20
Purpose	READ BINARY command with short EF ID for EF.DG8 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG8
Preconditions	1. DG8 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG8 (short EF ID '08') to the IDL. Though the CA mechanism has been performed, the access to the DG8 shall be denied. '0C B0 88 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.21 Test case SE_ISO7816_SecEAP_21

Test – ID	SE_ISO7816_SecEAP_21
Purpose	READ BINARY command with odd instruction byte and short EF ID for EF.DG8 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG8, OddIns
Preconditions	1. DG8 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG8 (short EF ID '08') to the IDL. Though the CA mechanism has been performed, the access to the DG8 shall be denied. '0C B1 00 08 17 85 <L_{85}> <Cryptogram> 97 01 01 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted DO 54 with the encoded offset 00 : '54 01 00'
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.22 Test case SE_ISO7816_SecEAP_22

Test – ID	SE_ISO7816_SecEAP_22
Purpose	SELECT EF command for EF.DG9 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG9
Preconditions	1. DG9 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given SELECT EF APDU for EF.DG9 to the IDL. Though the CA mechanism has been performed, the access to the DG9 shall be denied. '0C A4 02 0C 15 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted file ID ('00 09').
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.23 Test case SE_ISO7816_SecEAP_23

Test – ID	SE_ISO7816_SecEAP_23
Purpose	READ BINARY command with short EF ID for EF.DG9 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG9
Preconditions	1. DG9 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG9 (short EF ID '09') to the IDL. Though the CA mechanism has been performed, the access to the DG9 shall be denied. '0C B0 89 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.24 Test case SE_ISO7816_SecEAP_24

Test – ID	SE_ISO7816_SecEAP_24
Purpose	READ BINARY command with odd instruction byte and short EF ID for EF.DG9 within an established Secure Messaging session, but before the TA mechanism has been performed.
Version	1.0
Profile	EAP, DG9, OddIns
Preconditions	1. DG5 shall be EAP protected. Otherwise, skip the test. 2. The LDS application shall have been selected. 3. The BAP mechanism shall have been performed (only for BAP protected IDL). 4. The CA mechanism shall have been performed as well. 5. All APDUs are sent as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG9 (short EF ID '09') to the IDL. Though the CA mechanism has been performed, the access to the DG9 shall be denied. '0C B1 00 09 17 85 <L_{85}> <Cryptogram> 97 01 01 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted DO 54 with the encoded offset 00 : '54 01 00'
Expected results	1. Checking error '69 82' within a valid SM response.

B.3.9.25 Test case SE_ISO7816_SecEAP_25

Test – ID	SE_ISO7816_SecEAP_25
Purpose	SELECT EF command for EF.DG14 without BAP on a BAP protected profile.
Version	1.0
Profile	EAP, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall not have been performed.
Test scenario	1. Send the given SELECT EF APDU for EF.DG14 (FID='00 0E') to the IDL. Since the BAP mechanism has not been performed, the access to this file shall be denied. '00 A4 02 0C 02 00 0E'
Expected results	1. Checking error '69 82' as a plain text response without Secure Messaging.

B.3.9.26 Test case SE_ISO7816_SecEAP_26

Test – ID	SE_ISO7816_SecEAP_26
Purpose	SELECT EF command for EF.DG14 with BAP on a BAP protected profile (Positive test).
Version	1.0
Profile	EAP, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. All commands are encoded as valid Secure Messaging APDUs.
Test scenario	1. Send the given SELECT EF APDU for EF.DG14 (FID='00 0E') to the IDL. '0C A4 02 0C 15 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' The <Cryptogram> contains the encoded encrypted FID of the EF.DG14 ('00 0E'). 2. Send the given READ BINARY command on the current file. '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. '90 00' within a valid SM response. 2. '90 00' and 1 byte of data ('6E') within a valid SM response.

B.3.9.27 Test case SE_ISO7816_SecEAP_27

Test – ID	SE_ISO7816_SecEAP_27
Purpose	SELECT EF command for EF.DG14 without BAP on a plain profile (Positive test).
Version	1.0

Profile	EAP, Plain
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall not have been performed.
Test scenario	1. Send the given SELECT EF APDU for EF.DG14 (FID='00 0E') to the IDL. '00 A4 02 0C 02 00 0E' 2. Send the given READ BINARY command on the current file. '00 B0 00 00 01'
Expected results	1. '90 00' as a plain text response without Secure Messaging. 2. '90 00' and 1 byte of data ('6E') as a plain text response without Secure Messaging.

B.3.9.28 Test case SE_ISO7816_SecEAP_28

Test – ID	SE_ISO7816_SecEAP_28
Purpose	READ BINARY command with short EF ID for EF.DG14 without BAP on a BAP protected profile.
Version	1.0
Profile	EAP, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall not have been performed.
Test scenario	1. Send the given READ BINARY APDU for EF.DG14 (short EF ID '0E') to the IDL. Since the BAP mechanism has not been performed, the access to this file shall be denied. '00 B0 8E 00 01'
Expected results	1. Checking error '69 82' as a plain text response without Secure Messaging.

B.3.9.29 Test case SE_ISO7816_SecEAP_29

Test – ID	SE_ISO7816_SecEAP_29
Purpose	READ BINARY command with short EF ID for EF.DG14 with BAP on a BAP protected profile (Positive test).
Version	1.0
Profile	EAP, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. All commands are encoded as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG14 (short EF ID '0E') to the IDL. '0C B0 8E 00 0D 97 01 01 8E 08 <Checksum> 00'

Expected results	1. ’90 00’ and 1 byte of data (‘6E’) within a valid SM response.

B.3.9.30 Test case SE_ISO7816_SecEAP_30

Test – ID	SE_ISO7816_SecEAP_30
Purpose	READ BINARY command with short EF ID for EF.DG14 without BAP on a plain profile (Positive test).
Version	1.0
Profile	EAP, Plain
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall not have been performed.
Test scenario	1. Send the given READ BINARY APDU for EF.DG14 (short EF ID ‘0E’) to the IDL. ’00 B0 8E 00 01’
Expected results	1. ’90 00’ and 1 byte of data (‘6E’) as a plain text response without Secure Messaging.

B.3.9.31 Test case SE_ISO7816_SecEAP_31

Test – ID	SE_ISO7816_SecEAP_31
Purpose	READ BINARY command with odd instruction byte and with short EF ID for EF.DG14 without BAP on a BAP protected profile.
Version	1.0
Profile	EAP, BAP, OddIns
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall not have been performed.
Test scenario	2. Send the given READ BINARY APDU for EF.DG14 (short EF ID ‘0E’) to the IDL. Since the BAP mechanism has not been performed, the access to this file shall be denied. ’00 B1 00 0E 03 54 01 00 01’
Expected results	2. Checking error ’69 82’ as a plain text response without Secure Messaging.

B.3.9.32 Test case SE_ISO7816_SecEAP_32

Test – ID	SE_ISO7816_SecEAP_32
Purpose	READ BINARY command with odd instruction and with short EF ID for EF.DG14 with BAP on a BAP protected profile (Positive test).
Version	1.0

Profile	EAP, BAP, OddIns
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. All commands are encoded as valid Secure Messaging APDUs.
Test scenario	1. Send the given READ BINARY APDU for EF.DG14 (short EF ID '0E') to the IDL. '0C B1 00 0E 17 85 <L_{85}> <Cryptogram> 97 01 06 8E 08 <Checksum> 00' The <Cryptogram> contains the encrypted DO 54 with the encoded offset 00 '54 01 00'. 2. Verify the DG14 data returned.
Expected results	1. 6 bytes of data, and '90 00' within a valid SM response. 2. The DG14 data shall start with '6E'.

B.3.9.33 Test case SE_ISO7816_SecEAP_33

Test – ID	SE_ISO7816_SecEAP_33
Purpose	READ BINARY command with odd instruction and with short EF ID for EF.DG14 without BAP on a plain profile (Positive test).
Version	1.0
Profile	EAP, Plain, OddIns
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall not have been performed.
Test scenario	1. Send the given READ BINARY APDU for EF.DG14 (short EF ID '0E') to the IDL. '00 B1 00 0E 03 54 01 00 01'
Expected results	1. '90 00' and 1 byte of data ('6E') as a plain text response without Secure Messaging.

B.3.10 Test Unit SE_ISO7816_CA - Chip Authentication

The CA mechanism uses the manage security environment command (MSE:Set KAT) to verify that the chip is genuine.

The MSE:Set Kat command is used to implement CA, i.e. to establish new session keys for secure messaging using a key agreement protocol. The inspection system and the IDL generate a shared secret based on the public key data stored in DG14. This secret is used to derive new session keys. These session keys are used to protect the subsequent commands. If secure messaging was already in progress (BAP protected IDL), the response to the MSE:Set Kat command is protected with the old session keys, after which they are replaced with the new ones and secure messaging is restarted. If secure messaging was not yet in progress (Plain IDL), it is now started with the new session keys. The genuineness of the IDL chip is implicitly verified by its ability to perform Secure Messaging using the new session keys.

The test cases specified in this unit verify the correct implementation of the MSE:Set KAT command.

In DG14, ICAuthPublicKeyInfo defining CA public key may contain an optional keyIdentifier. This is useful if the chip supports multiple keys for CA. The MSE:Set Kat command can be called either with implicit key

selection if no key identifier is included in DG14 or with the explicit key reference defined in DG14. All the tests in this unit should be used with implicit or explicit key reference depending on the presence of the key identifier in DG14.

The DG14 may contain more than one ICAuthPublicKeyInfo. In this case, all appropriate tests must be performed for each key. The corresponding test case is only rated as PASS if all passes are completed successfully.

B.3.10.1 Test case SE_ISO7816_CA_1

Test – ID	SE_ISO7816_CA_1
Purpose	MSE:Set KAT command with correct ephemeral public key without BAP.
Version	1.0
Profile	EAP, Plain
Preconditions	1. The LDS application shall have been selected. 2. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '00 22 41 A6 <Lc> 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier>' The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify the chip ability to start a Secure Messaging with the new session keys, a Secured READ BINARY APDU on DG1 file (short EF ID='01') is send to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	1. '90 00'. The status word shall be returned as plain data without SM encoding. 2. '90 00' in a valid Secure Messaging response. The returned data shall be encoded with the NEW session keys.

B.3.10.2 Test case SE_ISO7816_CA_2

Test – ID	SE_ISO7816_CA_2
Purpose	MSE:Set KAT command with correct ephemeral public key with BAP.
Version	1.0
Profile	EAP, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as valid Secure Messaging APDUs.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data:

	91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier> The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify the chip ability to start a Secure Messaging with the new session keys, a Secured READ BINARY APDU on DG1 (short EF ID='01') is send to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. '90 00' in a valid Secure Messaging response using the OLD session keys. 2. '90 00' in a valid Secure Messaging response. The returned data shall be encoded with the NEW session keys.

B.3.10.3 Test case SE_ISO7816_CA_3

Test – ID	SE_ISO7816_CA_3
Purpose	MSE:Set KAT command with correct ephemeral public key without BAP, but afterwards try to use an APDU without Secure Messaging.
Version	1.0
Profile	EAP, Plain
Preconditions	1. The LDS application shall have been selected. 2. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '00 22 41 A6 <Lc> 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier>' The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. Send a clear READ BINARY APDU on DG1 (short EF ID='01') to the chip. '00 B0 81 00 01'
Expected results	1. '90 00'. The status word shall be returned as plain data without SM encoding. 2. Checking error. The chip shall not accept any APDUs without secure messaging. The error must be returned as plain text response without Secure Messaging.

B.3.10.4 Test case SE_ISO7816_CA_4

Test – ID	SE_ISO7816_CA_4
Purpose	MSE:Set KAT command with correct ephemeral public key with BAP, but afterwards the old session keys are used.
Version	1.0
Profile	EAP, BAP

Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data: 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier> The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. Instead of using the new session keys, the old session keys are used to send a Secured READ BINARY APDU on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. '90 00' in a valid Secure Messaging response using the OLD session keys. 2. Checking error. The chip shall delete the OLD session keys and shall not accept any APDUs with these session keys. The error must be returned as plain text response without Secure Messaging.

B.3.10.5 Test case SE_ISO7816_CA_5

Test – ID	SE_ISO7816_CA_5
Purpose	MSE:Set KAT command with invalid ephemeral public key (different key sizes) on non-BAP IDL. No SM must be started.
Version	1.0
Profile	EAP ECDH, Plain
Preconditions	1. The LDS application shall have been selected. 2. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '00 22 41 A6 <Lc> 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier>' The ephemeral public key shall be generated with domain parameters specifying a different key size (e.g. for a 224 bit key in DG14 a 192 bit ephemeral key pair is created). The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that APDU without Secure Messaging are still supported, send a clear READ BINARY APDU on DG1 (short EF ID='01') to the chip. '00 B0 81 00 01'

Expected results	1. Checking error, or warning ’63 00’ without Secure Messaging. Since there are invalid domain parameters used to generate the ephemeral key pair, the key agreement process shall always fail. 2. ’90 00’. The status word and returned data shall be returned as plain data without SM encoding.

B.3.10.6 Test case SE_ISO7816_CA_6

Test – ID	SE_ISO7816_CA_6
Purpose	MSE:Set KAT command with invalid ephemeral public key (different key sizes) on BAP IDL. Previously established session keys remain valid.
Version	1.0
Profile	EAP ECDH, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as valid Secure Messaging APDUs.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: ’0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ <Cryptogram> contains the following encrypted data: 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier> The ephemeral public key shall be generated with domain parameters specifying a different key size (e.g. for a 224 bit key in DG14 a 192 bit ephemeral key pair is created). The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that old session keys can still be used, the old session keys are used to send a Secured READ BINARY APDU on DG1 (short EF ID=’01’) to the chip. ’0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00’
Expected results	1. Checking error, or warning ’63 00’ within the Secure Messaging with OLD session keys. Since there are invalid domain parameters used to generate the ephemeral key pair, the key agreement process shall always fail. 2. ’90 00’ in a valid Secure Messaging response. The returned data shall be encoded with OLD session keys.

B.3.10.7 Test case SE_ISO7816_CA_7

Test – ID	SE_ISO7816_CA_7
Purpose	MSE:Set KAT command with a valid ephemeral public key but without Secure Messaging on BAP protected IDL.

Version	1.0
Profile	EAP, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '00 22 41 A6 <Lc> 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier>' The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that the chip does not activate the new session keys based on the key agreement, the new session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00' 3. To verify that the chip has deleted the old (BAP based) session keys, the old session keys are used to send a Secured READ BINARY APDU on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. Checking error. The use of Secure Messaging shall be enforced by the chip. The error code shall be returned as plain data without Secure Messaging encoding. 2. Checking error. The error code shall be returned as plain data without Secure Messaging encoding. 3. Checking error. The error code shall be returned as plain data without Secure Messaging encoding.

B.3.10.8 Test case SE_ISO7816_CA_8

Test – ID	SE_ISO7816_CA_8
Purpose	MSE:Set KAT command with a valid ephemeral public key but with invalid class byte on non-BAP protected IDL.
Version	1.0
Profile	EAP, Plain
Preconditions	1. The LDS application shall have been selected. 2. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '80 22 41 A6 <Lc> 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier>' The class byte has been set to en invalid value of 80. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that the chip does not activate the new session keys based on the key agreement, the new session keys are used to send a secured READ

	BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. Checking error. Invalid class. The error shall be sent in plain text. 2. Checking error. As a Secure Message is sent without an opened SM, the chip shall return a Secure Messaging error in a plain text response.

B.3.10.9 Test case SE_ISO7816_CA_9

Test – ID	SE_ISO7816_CA_9
Purpose	MSE:Set KAT command with a valid ephemeral public key but with invalid class byte on BAP protected IDL.
Version	1.0
Profile	EAP, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '8C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data: 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier> The class byte has been set to an invalid value of 8C. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that the chip does not activate the new session keys based on the key agreement, the new session keys are used send to a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. Checking error. Invalid class. Note the behaviour of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or SM response. 2. Checking error. As invalid session keys are used, the chip shall return a secure Messaging error in a plain text response regardless if the Secure Messaging was a already closed in step 1.

B.3.10.10 Test case SE_ISO7816_CA_10

Test – ID	SE_ISO7816_CA_10
Purpose	MSE:Set KAT command with invalid DO tag for the ephemeral public key on non-BAP protected IDL.

Version	1.0
Profile	EAP, Plain
Preconditions	1. The LDS application shall have been selected. 2. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '00 22 41 A6 <Lc> 93 <L_{93}> <ephemeral public key> 84 <L_{84}> <key identifier>' The DO for the ephemeral public key has an invalid tag 93. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that the chip does not activate the new session keys based on the key agreement, the new session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. Checking error. Invalid parameter. The error shall be sent in plain text. 2. Checking error. As a Secure Message is sent without an opened SM, the chip shall return a Secure Messaging error in a plain text response.

B.3.10.11 Test case SE_ISO7816_CA_11

Test – ID	SE_ISO7816_CA_11
Purpose	MSE:Set KAT command with invalid DO tag for the ephemeral public key on BAP protected IDL.
Version	1.0
Profile	EAP, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as valid Secure Messaging APDUs.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data: 93 <L_{93}> <ephemeral public key> 84 <L_{84}> <key identifier> The DO for the ephemeral public key has an invalid tag 93. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that old session keys are still valid, the old session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip.

	’0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00’
Expected results	1. Checking error. Invalid parameter. The error shall be encoded in a Secure Messaging using the OLD session keys. 2. ’90 00’ in a valid Secure Messaging response using the OLD session keys.

B.3.10.12 Test case SE_ISO7816_CA_12

Test – ID	SE_ISO7816_CA_12
Purpose	MSE:Set KAT command with an incorrect private key reference on non-BAP protected IDL.
Version	1.0
Profile	EAP, Plain
Preconditions	1. The LDS application shall have been selected. 2. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: ’00 22 41 A6 <Lc> 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier>’ A key identifier shall be included in the APDU. This key identifier does not exist in any ICAuthPublicKeyInfo structure of DG14. 2. To verify that the chip does not activate the new session keys based on the key agreement, the new session keys are used to send a secured READ BINARY command on DG1 (short EF ID=’01’) to the chip. ’0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00’
Expected results	1. Checking error. Invalid parameter. The error shall be sent in plain text. 2. Checking error. As a Secure Message is sent without an opened SM, the chip shall return a Secure Messaging error in a plain text response.

B.3.10.13 Test case SE_ISO7816_CA_13

Test – ID	SE_ISO7816_CA_13
Purpose	MSE:Set KAT command with an incorrect private key reference on BAP protected IDL.
Version	1.0
Profile	EAP KeyIdentifier, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as valid Secure Messaging APDUs.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL:

	’0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ <Cryptogram> contains the following encrypted data: 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier> A key identifier shall be included in the APDU. This key identifier does not exist in any ICAuthPublicKeyInfo structure of DG14. 2. To verify that old session keys are still valid, the old session keys are used to send a secured READ BINARY command on DG1 (short EF ID=’01’) to the chip. ’0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00’
Expected results	1. Checking error. Invalid parameter. The error shall be encoded in a Secure Messaging using the OLD session keys. 2. ’90 00’ in a valid Secure Messaging response using the OLD session keys.

B.3.10.14 Test case SE_ISO7816_CA_14

Test – ID	SE_ISO7816_CA_14
Purpose	Check the CA failure (using DH) – wrong value (value strictly bigger than the Prime) on non-BAP protected IDL.
Version	1.0
Profile	EAP DH, Plain
Preconditions	1. The LDS application shall have been selected. 2. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: ’00 22 41 A6 <Lc> 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier>’ Use an ephemeral public key with a wrong point (value strictly bigger than the Prime). Ephemeral public key = prime p + 1. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that the chip does not activate the new session keys based on the key agreement, the new session keys are used to send a secured READ BINARY command on DG1 (short EF ID=’01’) to the chip. ’0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00’
Expected results	1. Checking error or warning processing ’63 00’. The error shall be sent in plain text. 2. Checking error. As a Secure Message is sent without an opened SM, the chip shall return a Secure Messaging error in a plain text response.

B.3.10.15 Test case SE_ISO7816_CA_15

Test – ID	SE_ISO7816_CA_15
Purpose	Check the CA failure (using DH) – wrong value (value strictly bigger than the Prime) on BAP protected IDL.
Version	1.0
Profile	EAP DH, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as valid Secure Messaging APDUs.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data: 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier> Use an ephemeral public key with a wrong point (value strictly bigger than the Prime). Ephemeral public key = prime p + 1. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that old session keys are still valid, the old session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. Checking error or warning processing '63 00'. The error shall be encoded in a Secure Messaging using the OLD session keys and old SSC. 2. '90 00' in a valid Secure Messaging response using the OLD session keys.

B.3.10.16 Test case SE_ISO7816_CA_16

Test – ID	SE_ISO7816_CA_16
Purpose	Check the CA failure (using ECDH) – wrong point (value does not belong to the curve) on non-BAP protected IDL.
Version	1.0
Profile	EAP ECDH, Plain
Preconditions	1. The LDS application shall have been selected. 2. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '00 22 41 A6 <Lc> 91 <L_{91}> <ephemeral public key>

	84 <L_{84}> <key identifier>' Use an ephemeral public key with a wrong point (value does not belong to the curve). The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that the chip does not activate the new session keys based on the key agreement, the new session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. Checking error or warning processing '63 00'. The error shall be sent in plain text. 2. Checking error. As a Secure Message is sent without an opened SM, the chip shall return a Secure Messaging error in a plain text response.

B.3.10.17 Test case SE_ISO7816_CA_17

Test – ID	SE_ISO7816_CA_17
Purpose	Check the CA failure (using ECDH) – wrong point (value does not belong to the curve) on BAP protected IDL.
Version	1.0
Profile	EAP ECDH, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as valid Secure Messaging APDUs.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data: 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier> Use an ephemeral public key with a wrong point (value does not belong to the curve). The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that old session keys are still valid, the old session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. Checking error or warning processing '63 00'. The error shall be encoded in a Secure Messaging using the OLD session keys and old SSC. 2. '90 00' in a valid Secure Messaging response using the OLD session keys.

B.3.10.18 Test case SE_ISO7816_CA_18

Test – ID	SE_ISO7816_CA_18
Purpose	Check the CA failure (using ECDH) – wrong value, providing a (0,0) public key on non-BAP protected IDL.
Version	1.0
Profile	EAP ECDH, Plain
Preconditions	1. The LDS application shall have been selected. 2. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '00 22 41 A6 <Lc> 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier>' Use an ephemeral public key coded as '04||x||y' where both x and y have a size according to the prime but filled with '00'. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that the chip does not activate the new session keys based on the key agreement, the new session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. Checking error or warning processing '63 00'. The error shall be sent in plain text. 2. Checking error. As a Secure Message is sent without an opened SM, the chip shall return a Secure Messaging error in a plain text response.

B.3.10.19 Test case SE_ISO7816_CA_19

Test – ID	SE_ISO7816_CA_19
Purpose	Check the CA failure (using ECDH) – wrong value, providing a (0,0) public key on BAP protected IDL.
Version	1.0
Profile	EAP ECDH, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as valid Secure Messaging APDUs.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data: 91 <L_{91}> <ephemeral public key>

	84 <L_{84}> <key identifier> Use an ephemeral public key coded as '04||x||y' where both x and y have a size according to the prime but filled with '00'. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that old session keys are still valid, the old session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. Checking error or warning processing '63 00'. The error shall be encoded in a Secure Messaging using the OLD session keys and old SSC. 2. '90 00' in a valid Secure Messaging response using the OLD session keys.

B.3.10.20 Test case SE_ISO7816_CA_20

Test – ID	SE_ISO7816_CA_20
Purpose	Check the CA success (using ECDH) – test borderline cases for x- and y-coordinates (small x coordinate) on non-BAP protected IDL.
Version	1.0
Profile	EAP ECDH, Plain
Preconditions	1. The LDS application shall have been selected. 2. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '00 22 41 A6 <Lc> 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier>' Use an ephemeral public with an x- coordinate requiring less than [$\log_{256}$ q] bytes to be represented. Pad with zero bytes. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that the chip activates Secure Messaging with the new session keys based on the key agreement, the new session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. '90 00'. The status word shall be returned as plain data without SM encoding. 2. '90 00' in a valid Secure Messaging response. The returned data shall be encoded with the NEW session keys.

B.3.10.21 Test case SE_ISO7816_CA_21

Test – ID	SE_ISO7816_CA_21
Purpose	Check the CA success (using ECDH) – test borderline cases for x- and y-

	coordinates (small x coordinate) on BAP protected IDL.
Version	1.0
Profile	EAP ECDH, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as valid Secure Messaging APDUs.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data: 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier> Use an ephemeral public with an x- coordinate requiring less than [$\log_{256}$ q] bytes to be represented. Pad with zero bytes. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify the chip ability to continue the Secure Messaging with the new keys, the new session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. '90 00' in a valid Secure Messaging response encoded with the OLD session keys. 2. '90 00' in a valid Secure Messaging response. The returned data shall be encoded with the NEW session keys.

B.3.10.22 Test case SE_ISO7816_CA_22

Test – ID	SE_ISO7816_CA_22
Purpose	Check the CA success (using ECDH) – test borderline cases for x- and y-coordinates (large x coordinate) on non-BAP protected IDL.
Version	1.0
Profile	EAP ECDH, Plain
Preconditions	1. The LDS application shall have been selected. 2. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '00 22 41 A6 <Lc> 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier>' Use an ephemeral public with an x- coordinate having its highest bit set to 1. The key identifier shall be included in the APDU if and only if it is specified in

	the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that the chip activates Secure Messaging with the new session keys based on the key agreement, the new session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. '90 00'. The status word shall be returned as plain data without SM encoding. 2. '90 00' in a valid Secure Messaging response. The returned data shall be encoded with the NEW session keys.

B.3.10.23 Test case SE_ISO7816_CA_23

Test – ID	SE_ISO7816_CA_23
Purpose	Check the CA success (using ECDH) – test borderline cases for x- and y-coordinates (large x coordinate) on BAP protected IDL.
Version	1.0
Profile	EAP ECDH, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as valid Secure Messaging APDUs
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data: 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier> Use an ephemeral public with an x- coordinate having its highest bit set to 1. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify the chip ability to continue the Secure Messaging with the new keys, the new session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. '90 00' in a valid Secure Messaging response encoded with the OLD session keys. 2. '90 00' in a valid Secure Messaging response. The returned data shall be encoded with the NEW session keys.

B.3.10.24 Test case SE_ISO7816_CA_24

Test – ID	SE_ISO7816_CA_24
Purpose	Check the CA success (using ECDH) – test borderline cases for x- and y-

	coordinates (small y coordinate) on non-BAP protected IDL.
Version	1.0
Profile	EAP ECDH, Plain
Preconditions	1. The LDS application shall have been selected. 2. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '00 22 41 A6 <Lc> 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier>' Use an ephemeral public with an y- coordinate requiring less than [$\log_{256}$ q] bytes to be represented. Pad with zero bytes. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that the chip activates Secure Messaging with the new session keys based on the key agreement, the new session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. '90 00'. The status word shall be returned as plain data without SM encoding. 2. '90 00' in a valid Secure Messaging response. The returned data shall be encoded with the NEW session keys.

B.3.10.25 Test case SE_ISO7816_CA_25

Test – ID	SE_ISO7816_CA_25
Purpose	Check the CA success (using ECDH) – test borderline cases for x- and y-coordinates (small y coordinate) on BAP protected IDL.
Version	1.0
Profile	EAP ECDH, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as valid Secure Messaging APDUs.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data: 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier> Use an ephemeral public with an y- coordinate requiring less than [$\log_{256}$ q] bytes to be represented. Pad with zero bytes. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14.

	2. To verify the chip ability to continue the Secure Messaging with the new keys, the new session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. '90 00' in a valid Secure Messaging response encoded with the OLD session keys. 2. '90 00' in a valid Secure Messaging response. The returned data shall be encoded with the NEW session keys.

B.3.10.26 Test case SE_ISO7816_CA_26

Test – ID	SE_ISO7816_CA_26
Purpose	Check the CA success (using ECDH) – test borderline cases for x- and y-coordinates (large y coordinate) on non-BAP protected IDL.
Version	1.0
Profile	EAP ECDH, Plain
Preconditions	1. The LDS application shall have been selected. 2. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '00 22 41 A6 <Lc> 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier>' Use an ephemeral public with an y- coordinate having its highest bit set to 1. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify that the chip activates Secure Messaging with the new session keys based on the key agreement, the new session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. '90 00': The status word shall be returned as plain data without SM encoding. 2. '90 00' in a valid Secure Messaging response. The returned data shall be encoded with the NEW session keys.

B.3.10.27 Test case SE_ISO7816_CA_27

Test – ID	SE_ISO7816_CA_27
Purpose	Check the CA success (using ECDH) – test borderline cases for x- and y-coordinates (large y coordinate) on BAP protected IDL.
Version	1.0
Profile	EAP ECDH, BAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed.

	3. The ICAuthPublicKeyInfo stored in DG14 shall have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as valid Secure Messaging APDUs.
Test scenario	1. Send the given MSE:Set KAT APDU to the IDL: '0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data: 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <key identifier> Use an ephemeral public with an y- coordinate having its highest bit set to 1. The key identifier shall be included in the APDU if and only if it is specified in the ICAuthPublicKeyInfo structure stored in DG14. 2. To verify the chip ability to continue the Secure Messaging with the new keys, the new session keys are used to send a secured READ BINARY command on DG1 (short EF ID='01') to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. '90 00' in a valid Secure Messaging response encoded with the OLD session keys. 2. '90 00' in a valid Secure Messaging response. The returned data shall be encoded with the NEW session keys.

B.3.11 Test Unit SE_ISO7816_CertVer - Certificate verification

During the TA process the certificate chain from the trust point stored in the chips EF.COM file down to the inspection systems CV certificate is verified. This is done by an alternating sequence of MSE: Set DST and Verify Certificate commands. This unit covers all certificate verification test cases which do NOT update the chips persistent memory. This means that all tests in this unit can be repeated with the same set of certificates.

B.3.11.1 Test case SE_ISO7816_CertVer_1

Test – ID	SE_ISO7816_CertVer_1
Purpose	Positive test with a valid chain of CV certificates.
Version	1.0
Profile	EAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The CA mechanism shall have been performed as well. 4. The Certification Authority Reference shall have been read from the EF.COM file (Current trust root). 5. All APDUs are sent as valid SecureMessaging APDUs. 6. All response data shall be SM protected.
Test scenario	1. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the "Certificate set 1" chapter as CERT_L1_01. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted DOs

	7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 2. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the “Certificate set 1” chapter as CERT_L0_01. ‘0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ • <Cryptogram> contains the following encrypted DOs 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	1. ’90 00’ in a valid SM response. 2. ’90 00’ in a valid SM response.

B.3.11.2 Test case SE_ISO7816_CertVer_2

Test - ID	SE_ISO7816_CertVer_2
Purpose	Test with an invalid Certification Authority Reference.
Version	1.0
Profile	EAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The CA mechanism shall have been performed as well. 4. The Certification Authority Reference shall have been read from the EF.COM file (Current trust root). 5. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	1. Send the optional given MSE: Set DST APDU to the IDL. ‘0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ • <Cryptogram> contains the following encrypted DOs 83 <L_{83}> <BAD AKID> • The Certification Authority Reference read from the EF.COM is changed in the last character to create an invalid reference. 2. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the “Certificate set 1” chapter as CERT_L1_01. ‘0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ • <Cryptogram> contains the following encrypted DOs 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the “Certificate set 1” chapter as CERT_L0_01. ‘0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ • <Cryptogram> contains the following encrypted DOs 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>

Expected results	1. '90 00' or checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 2. If the result of step 1 is '90 00': Checking error or '63 00' in a valid SM response. If the result of step 1 is NOT '90 00': '90 00' in a valid SM response. No verification key shall be activated. 3. If the result of step 1 is '90 00': Checking error or '63 00' in a valid SM response. If the result of step 1 is NOT '90 00': '90 00' in a valid SM response. Since the previous certificate was not verified successfully, it shall not be possible to use it as the trust point for the Certificate verification.

B.3.11.3 Test case SE_ISO7816_CertVer_3

Test - ID	SE_ISO7816_CertVer_3
Purpose	Test with an invalid certificate signature.
Version	1.0
Profile	EAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The CA mechanism shall have been performed as well. 4. The Certification Authority Reference shall have been read from the EF.COM file (Current trust root). 5. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	1. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the "Certificate set 1" chapter as CERT_L1_01. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted DOs 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <bad certificate signature> • The signature object of the certificate has been changed in last digit to make it invalid 2. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the "Certificate set 1" chapter as CERT_L0_01. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted DOs 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	1. Checking error or '63 00' in a valid SM response. 2. Checking error or '63 00' in a valid SM response. Since the previous certificate was not verified successfully, it shall not be possible to use it as the trust point for the Certificate verification.

B.3.11.4 Test case SE_ISO7816_CertVer_4

Test - ID	SE_ISO7816_CertVer_4
Purpose	Test with a missing certificate signature.
Version	1.0
Profile	EAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The CA mechanism shall have been performed as well. 4. The Certification Authority Reference shall have been read from the EF.COM file (Current trust root). 5. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	1. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the “Certificate set 1” chapter as CERT_L1_01. ‘0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ • <Cryptogram> contains the following encrypted DOs 7F 4E <L_{7F4E}> <certificate body> • The certificate signature object is omitted. 2. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the “Certificate set 1” chapter as CERT_L0_01. ‘0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ • <Cryptogram> contains the following encrypted DOs 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	1. Checking error or ’63 00’ in a valid SM response. 2. Checking error or ’63 00’ in a valid SM response. Since the previous certificate was not verified successfully, it shall not be possible to use it as the trust point for the Certificate verification.

B.3.11.5 Test case SE_ISO7816_CertVer_5

Test - ID	SE_ISO7816_CertVer_5
Purpose	Test with a missing certificate body.
Version	1.0
Profile	EAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The CA mechanism shall have been performed as well. 4. The Certification Authority Reference shall have been read from the EF.COM file (Current trust root). 5. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	1. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the “Certificate set 1”