INTERNATIONAL STANDARD

ISO/IEC 18013-4

Second edition
2019-10

Personal identification — ISO-compliant driving licence —

Part 4: Test methods

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

Partie 4: Méthodes d'essai

Reference number
ISO/IEC 18013-4:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and security devices for personal identification*.

This second edition cancels and replaces the first edition (ISO/IEC 18013-4:2011), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 18013-4:2011/Cor 1:2013.

The main changes compared to the previous edition are as follows:

— in the interest of interoperability of cards used for personal identification, the authentication protocols for the IDL are simplified; Active Authentication is harmonised with other ISO standards and thus BAP configurations 2, 3 and 4, as well as EAP are no longer supported by this document;

— replacing EAP, the optional EACv1 protocol is defined for the IDL, enabling access control to sensitive biometric data stored on an integrated circuit; EACv1 may be used in conjunction with either BAP configuration 1 or PACE;

— the optional PACE protocol enables access control to the data stored on an integrated circuit. The PACE protocol is a password authenticated Diffie Hellman key agreement protocol based on a (short) input string that provides secure communication between a secure integrated circuit on an IDL and a terminal and allows various implementation options (mappings, input strings, algorithms); the PACE protocol implementation for the IDL is restricted to Elliptic Curve Diffie Hellman (ECDH) generic mapping and can be used as a stand-alone protocol or in combination with the EACv1 protocol.

A list of all parts in the ISO/IEC 18013 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The ISO/IEC 18013 series 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.

This document prescribes requirements for testing of the compliance of the machine-readable data content and mechanisms to control 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.

Personal identification — ISO-compliant driving licence —

Part 4: Test methods

1 Scope

This document describes 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 the ISO/IEC 18013 series for:

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

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

This document deals with test methods specific to 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 document.

Hence the purpose of this document is to:

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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, *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*

ISO/IEC 8859-1, *Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1*

ISO/IEC 18013-2:—[1], *Personal identification — ISO-compliant driving licence — Part 2: Machine-readable technologies*

ISO/IEC 18013-3:2017, *Information technology — Personal identification — ISO-compliant driving licence — Part 3: Access control, authentication and integrity validation*

BSI TR-03105-3.2, *Advanced Security Mechanisms for Machine Readable Travel Documents — Extended Access Control (EACv1) — Tests for Security Implementation — Version 1.5*

BSI TR-03111, *Elliptic Curve Cryptography (ECC) — Version 2.0*

ICAO Doc 9303, *Machine Readable Travel Documents*, seventh edition, 2015

[1] Under preparation. Stage at the time of publication: ISO/IEC FDIS 18013-2:2019.

TRICAO, Part 3, RF Protocol and Application Test Standard for eMRTD — Part 3: Tests for Application Protocol and Logical Data Structure, version 2.11

RFC-3369 — *Cryptographic Message Syntax (CMS)*

3 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.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
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

3.2
test case specification
collection of *test cases* (3.1) and general test data applicable to the test cases

4 Abbreviated terms

AA	active authentication
AKID	authority key identifier
AID	application identifier
APDU	application protocol data unit
BAP	basic access protection
BCD	binary coded decimal
CA	chip authentication
DER	distinguished encoding rules
DF	dedicated file
DG	data group
DO	data object
EAC	extended access control
EF	elementary file
ECDSA	elliptic curve digital signature algorithm
FID	file identifier
ICS	implementation conformance statement
IDL	ISO-compliant driving licence

IUT	implementation under test
LDS	logical data structure
MAC	message authentication code
NMA	non-match alert
OID	object identifier
PA	passive authentication
PACE	Password Authenticated Connection Establishment
RF	radio frequency
SAI	scanning area identifier
SE	standard encoding
SIC	secure integrated circuit
SFI	short EF identifier
SMI	security mechanism indicator
SOD	document security object
TA	terminal authentication

5 Conformance

Test case specifications described in this document 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 document. However, passing all applicable tests in this document does not guarantee that no failures will occur under operational conditions.

6 Test design

6.1 General

This clause generally follows the concepts of the OSI Conformance Testing Methodology and Framework as specified in ISO/IEC 9646 (all parts). 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 document.

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.

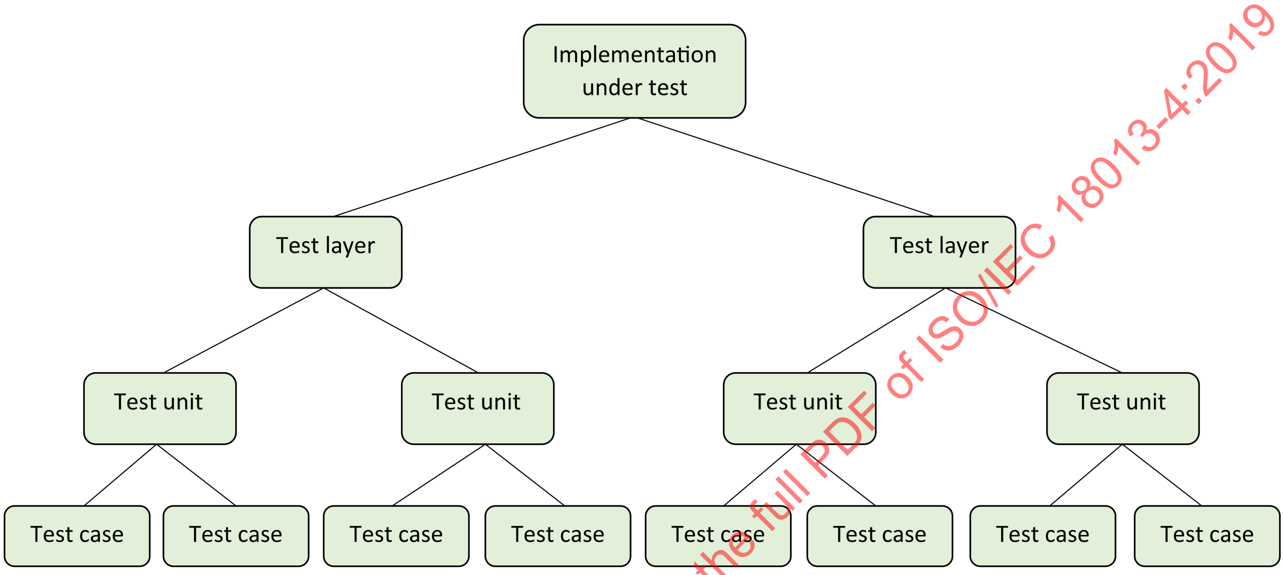

Figure 1 — Test element hierarchy

6.2.2 Implementation under test

6.2.2.1 Overview

One IUT is defined as an IDL with SE for SIC (see ISO/IEC 18013-2:—, Annex C).

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 document:

— 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 IUT:

— SE.

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	Specifies the 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 as "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

6.3.1.1 IUT

The tests in this document 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.

6.3.1.2 Test environment

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

6.3.1.3 Test apparatus

All equipment described in Annexes A to C pertinent to the machine readable techonogy supported by the IUT shall 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; or

— 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 Annexes A to C.

7.2 Profiles

Profiles are defined to identify whether certain optional functionality is supported by the IUT. Support of these optional functions and features depends 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 General

IDL test case specifications are attached in the annexes.

Test methods for driving licence interface devices are currently not included in this document.

7.3.2 Standard encoding on SIC

Test case specifications for SE on SIC cover are as follows:

— LDS tests for SE on SIC. The tests shall be carried out as specified in Annex A.

- Commands tests (applicable to SE on SIC). The tests shall be carried out as specified in Annex B.
- Tests for EACv1 protocol. The tests shall be carried out as specified in Annex C.

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 General

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 the ISO/IEC 7816 series or the ISO/IEC 14443 series can be used. The reader shall support extended length APDUs and command chaining.

If EAC 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 and ISO/IEC 18013-3 specifications define several optional elements that an IDL can support. This includes security mechanisms like PACE, BAP, EAC and AA as well as additional data groups (DG 2 to DG 14).

Since these elements are optional, it is not possible to define the corresponding tests as mandatory for each IDL. Therefore, this document 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 DG 12 to DG14 because the EAC, 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, PACE or EAC)
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		

Table A.1 *(continued)*

Profile	Information for test setup	Applicable (YES or NO)	Protection level (Plain, BAP, PACE or EAC)
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		▨
EAC	Extended Access Control v1		▨
PACE	Password Authenticated Connection Establishment		▨
MRZ	Machine Readable Zone		▨

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:
EAC	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

A.3.1.1 General

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 ISO/IEC 18013-3

A.3.1.2 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: —, 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) The first byte shall be '60'.

A.3.1.3 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:—, 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 sesults	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.3.1.4 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: —, Annex C
Profile	
Preconditions	1) EF.COM has been retrieved from the IDL.
Test scenario	1) Search for the LDS version (Tag '5F01') inside EF.COM. 2) Verify the encoded length of the object with tag '5F01'. 3) Verify the LDS version.
Expected results	1) Tag '5F01' shall be present. 2) The encoded length shall be 02. 3) The specified LDS version shall be '01 XX'h (BCD encoded).

A.3.1.5 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:—, Annex C ISO/IEC 18013-3:2017, 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.3.1.6 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:—, Annex C ISO/IEC 18013-3:2017, 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.3.1.7 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:—, Annex C ISO/IEC 18013-3:2017, 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.3.1.8 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:—, Annex C ISO/IEC 18013-3:2017, 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.3.1.9 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:—, Annex C ISO/IEC 18013-3:2017, 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.3.1.10 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:—, Annex C ISO/IEC 18013-3:2017, Clause 8
Profile	SMI, AA

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 Tag List in EF.COM.
Expected results	1) The parameters for the mechanism id-sm-AA shall be encoded as specified in ISO/IEC 18013-3:2017, 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 Tag List.

A.3.1.11 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:—, Annex C ISO/IEC 18013-3:2017, Clause 8
Profile	SMI, NMA
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 Tag List in EF.COM.

Expected results	1) The parameters for the mechanism id-sm-NMA shall be encoded as specified in ISO/IEC 18013-3:2017, 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 Tag List.

A.3.1.12 Test case SE_LDS_COM_013

Test case-ID	SE_LDS_COM_013
Purpose	This test checks the encoding of the EAC mechanism in the SMI.
Version	1.2
References	ISO/IEC 18013-2:—, Annex C ISO/IEC 18013-3:2017, Clause 8
Profile	SMI, EAC
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 EAC mechanism: 1) Check the presence of the mechanism id-TA. 2) Check the encoding of the parameters for the mechanism id-TA. 3) Check the version of the EAC parameters. 4) Check the data groups.
Expected results	1) The mechanism id-TA shall be present. 2) The parameters for the mechanism id-TA shall be encoded as specified in ISO/IEC 18013-3:2017, D.4. 3) The version shall be ‘01’. 4) The data groups shall only contain any combination of the following integers: '05', '06', '07', '08', '09', '0A', '0B'.

A.3.1.13 Test case SE_LDS_COM_014

Test case-ID	SE_LDS_COM_014
Purpose	This test checks the presence of the EAC mechanism in the SMI.
Version	1.2
References	ISO/IEC 18013-2:—, Annex C ISO/IEC 18013-3:2017, Clause 8
Profile	SMI, EAC 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	Perform the following checks for the security mechanism in the SMI that specifies the EAC mechanism: 1) Check the presence of the mechanism id-TA if EAC is NOT supported.
Expected results	1) The mechanism id-TA shall be absent.

A.3.2 Test unit SE_LDS_DG1 — Tests for EF.DG1

A.3.2.1 General

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 ISO/IEC 8859-1 ISO 3166-1

A.3.2.2 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:—, 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) The first byte shall be '61'.

A.3.2.3 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:—, 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.3.2.4 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:—, Annex C
Profile	
Preconditions	1) EF.DG1 has been retrieved from the IDL.
Test scenario	1) Search for the Mandatory Demographic Data (Tag '5F1F') 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 '5F1F' 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.3.2.5 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:—, 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.3.2.6 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:—, 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.3.2.7 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:—, 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.3.2.8 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:—, 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.3.2.9 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:—, 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.3.2.10 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:—, Annex C ISO 3166-1
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) The 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.3.2.11 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:—, Annex C ISO/IEC 8859-1
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) The Issuing Authority shall be coded according to ISO/IEC 8859-1.

A.3.2.12 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:—, 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 in Alpha-Numeric characters only.

A.3.2.13 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:—, 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 '7F63') inside EF.DG1. 2) Analyze the encoding of the bytes that follow the template tag. 3) Verify the length of the DO with Tag '7F63'.
Expected results	1) Tag '7F63' 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.3.2.14 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:—, A.4 ISO/IEC 18013-2:—, 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.3.2.15 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:—, A.4 ISO/IEC 18013-2:—, 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 delimiter ";"

A.3.2.16 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	1.1
References	ISO/IEC 18013-2:—, A.4 ISO/IEC 18013-2:—, 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 check for each of the "Category of Vehicle/Restriction/Condition" entries: 1) Check the format of the Vehicle Category Code (sub-field #1).
Expected results	1) The Vehicle Category Code contains Alpha-Numeric characters only.

A.3.2.17 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:—, A.4 ISO/IEC 18013-2:—, 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.3.2.18 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:—, A.4 ISO/IEC 18013-2:—, 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.3.2.19 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	1.1
References	ISO/IEC 18013-2:—, A.4 ISO/IEC 18013-2:—, A.5.1 ISO/IEC 18013-2:—, 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 Code. 2) Check the value of the Code.
Expected results	1) Code shall be encoded in a maximum of 5 ANS characters. 2) The value of the Code is one of the values specified in ISO/IEC 18013-2:—, A.5.1 (i.e. "01", "03", "78", "S01", "S02", "S03", "S04" or "S05").

A.3.2.20 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	1.1
References	ISO/IEC 18013-2:—, A.4 ISO/IEC 18013-2:—, A.5.1 ISO/IEC 18013-2:—, 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 Sign. 2) Check the value of the Sign. 3) Check the Sign only occurs in combination with an applicable Code. 4) Check the Sign only occurs in combination with a Value field.
Expected results	1) Sign shall be encoded in a Special characters. 2) The value of the Sign is one of the values specified in ISO/IEC 18013-2:—, A.5.1 (i.e. "<","=",">","<=","=<","<>","><",">=","=>","=="). 3) The value of the Code is one of the following values specified in ISO/IEC 18013-2:—, A.5.1 (i.e. "S01", "S02", "S03" or "S04"). 4) The Value field is not empty.

A.3.2.21 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	1.1

References	ISO/IEC 18013-2:—, A.4 ISO/IEC 18013-2:—, A.5.1 ISO/IEC 18013-2:—, 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 ANS 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

A.3.3.1 General

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:

A.3.3.2 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:—, 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) The first byte shall be '6B'.

A.3.3.3 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:—, 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.3.3.4 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:—, 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.3.3.5 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:—, 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.3.3.6 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:—, 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.3.3.7 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:—, 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 '5F35') inside EF.DG2. 2) Check the length of the DO with Tag '5F35'. 3) Check the value of Gender.
Expected results	1) Tag '5F35' shall 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.3.3.8 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:—, 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 '5F64') inside EF.DG2. 2) Check the length of the DO with Tag '5F64'. 3) Check the encoding of the Height field.
Expected results	1) Tag '5F64' shall 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.3.3.9 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:—, 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 '5F65') inside EF.DG2. 2) Check the length of the DO with Tag '5F65'. 3) Check the encoding of the Weight field.
Expected results	1) Tag '5F65' shall 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.3.3.10 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:—, 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 '5F66') inside EF.DG2. 2) Check the length of the DO with Tag '5F66'. 3) Check the encoding of Eye Colour.
Expected results	1) Tag '5F66' shall be present. 2) The length of Eye Colour shall be 3 bytes. 3) The value of Eye Colour shall be as defined in ISO/IEC 18013-2 (i.e. "BLK", "BLU", "BRO", "GRY", "GRN", "HAZ", "MAR", "PNK", "DIC", or "UNK").

A.3.3.11 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:—, 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 '5F67') inside EF.DG2. 2) Check the length of the DO with Tag '5F67'. 3) Check the encoding of Hair Colour.

Expected results	1) Tag '5F67' shall be present. 2) The length of Hair Colour shall be 3 bytes. 3) The value of Hair Colour shall be as defined in ISO/IEC 18013-2 (i.e. "BAL", "BLK", "BLN", "BRO", "GRY", "RED", "SDY", "WHI", or "UNK").

A.3.3.12 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:—, 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 '5F11') inside EF.DG2. 2) Check the length of the DO with Tag '5F11'. 3) Check the length and format of the DO with Tag '5F11'. 4) Check the value of Place of Birth.
Expected results	1) Tag '5F11' shall 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.3.3.13 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:—, 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 '5F42') inside EF.DG2. 2) Check the length of the DO with Tag '5F42'. 3) Check the length and format of the DO with Tag '5F42'. 4) Check the value of Place of Residence.

Expected results	1) Tag '5F42' shall 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

A.3.4.1 General

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:

A.3.4.2 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:—, 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) The first byte shall be '6C'.

A.3.4.3 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:—, 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.3.4.4 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:—, 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 ISO/IEC 18013-2:—, Table C.8.

A.3.4.5 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:—, 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.3.4.6 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:—, 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.3.4.7 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:—, 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 '5F68') inside EF.DG3. 2) Check the length of the DO with Tag '5F68'. 3) Check the encoding of Administrative Number.
Expected results	1) Tag '5F68' shall be present. 2) The bytes that follow the Tag '5F68' 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.3.4.8 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:—, 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 '5F69') inside EF.DG3. 2) Check the length of the DO with Tag '5F69'. 3) Check the encoding of Document Discriminator.
Expected results	1) Tag '5F69' shall be present. 2) The length of the DO with Tag '5F69' shall be 1 byte. 3) The Document Discriminator shall be as coded as BCD.

A.3.4.9 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:—, 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 '5F6D') inside EF.DG3. 2) Check the length of the DO with Tag '5F6D'. 3) Check the encoding of Data Discriminator.
Expected results	1) Tag '5F6D' shall be present. 2) The length of the DO with Tag '5F6D' shall be 1 byte. 3) The Data Discriminator shall be as coded as BCD.

A.3.4.10 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:—, 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 '5F6A') inside EF.DG3. 2) Check the length of the DO with Tag '5F6A'. 3) Check the encoding of ISO Issuer ID Number.
Expected results	1) Tag '5F6A' shall be present. 2) The length of the DO with Tag '5F6A' 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

A.3.5.1 General

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:

A.3.5.2 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:—, 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) The first byte shall be '65'.

A.3.5.3 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:—, 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.3.5.4 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:—, 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.3.5.5 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:—, 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.3.5.6 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:—, 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.3.5.7 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:—, 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:—, 8.5 (i.e. '03' or '04').

A.3.5.8 Test case SE_LDS_DG4_007

Test case-ID	SE_LDS_DG4_007
Purpose	This test checks the encoding of the Image (Tag '5F40') in each Portrait Template in EF.DG4.
Version	1.0
References	ISO/IEC 18013-2:—, Annex C and Annex E
Profile	DG4
Preconditions	1) EF.DG4 has been retrieved from the IDL
Test scenario	1) Search for the Image (Tag '5F40') 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 '5F40' shall be present. 2) The bytes that follow the Tag '5F40' 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 '5F40'. 4) The type of Image shall match one of the values in Table E.1 in ISO/IEC 18013-2:—, Table E.1. 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

A.3.6.1 General

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:

A.3.6.2 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:—, 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) The first byte shall be '67'.

A.3.6.3 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	1.2
References	ISO/IEC 18013-2:—, Annex C
Profile	DG5
Preconditions	1) EF.DG5 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.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.3.6.4 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	1.2
References	ISO/IEC 18013-2:—, Annex C
Profile	DG5
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:—, 8.6 (i.e. '03', '04', or '05').

A.3.6.5 Test case SE_LDS_DG5_004

Test case-ID	SE_LDS_DG5_004
Purpose	This test checks the Image of Signature or Mark (Tag '5F43') present in EF.DG5.
Version	1.2
References	ISO/IEC 18013-2:—, Annex C and Annex E
Profile	DG5
Preconditions	1) EF.DG5 has been retrieved from the IDL.
Test scenario	1) Search for the Image of Signature or Mark (Tag '5F43') 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 '5F43' shall be present. 2) The bytes that follow the Tag '5F43' 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:—, Table E.1. 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

A.3.7.1 General

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

A.3.7.2 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:—, 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) The first byte shall be '75'.

A.3.7.3 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:—, 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.3.7.4 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 '7F61') present in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:—, Annex C
Profile	DG6
Preconditions	1) EF.DG6 has been retrieved from the IDL.
Test scenario	1) Search for the Biometric Group Template (Tag '7F61') 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 '7F61' shall be present. 2) The bytes that follow the Tag '7F61' 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.3.7.5 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:—, 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 '7F60' in the Biometric Group Template.

A.3.7.6 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:—, 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 '7F60'. 3) Verify the length of the DO with Tag '7F60'.
Expected results	1) The tag shall be '7F60'. 2) The bytes that follow the Tag '7F60' 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 '7F60'.

A.3.7.7 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:—, 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.3.7.8 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:—, 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.3.7.9 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:—, 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.3.7.10 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:—, 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.3.7.11 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:—, 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.3.7.12 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:—, 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.3.7.13 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:—, 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.3.7.14 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:—, 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 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 18013-2:—, Annex C.

A.3.7.15 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:—, 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 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 18013-2:—, Annex C.

A.3.7.16 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:—, 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 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 18013-2:—, Annex C. 5) The BDB format type shall be valid in combination with the format owner data element.

A.3.7.17 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:—, 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.3.7.18 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 '5F2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:—, 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 '5F2E') inside the Biometric Template. 2) If Tag '5F2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3) If Tag '5F2E' is present, verify the length of the Biometric Data Block DO. 4) If Tag '5F2E' is present, verify that the tag for the Enciphered Biometric Data Block (Tag '7F2E') is absent. 5) If Tag '5F2E' is absent, verify that the tag for the Enciphered Biometric Data Block (Tag '7F2E') is present.
Expected results	1) Tag '5F2E' may be present and shall not occur more than once. 2) If Tag '5F2E' 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 '5F2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4) If Tag '5F2E' is present, Tag '7F2E' shall be absent. 5) If Tag '5F2E' is absent, Tag '7F2E' shall be present.

A.3.7.19 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 '7F2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:—, 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 '7F2E') inside the Biometric Template. 2) If Tag '7F2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3) If Tag '7F2E' is present, verify the length of the Enciphered Biometric Data Block DO. 4) If Tag '7F2E' is present, verify that the tag for the Biometric Data Block (Tag '5F2E') is absent. 5) If Tag '7F2E' is absent, verify that the tag for the Biometric Data Block (Tag '5F2E') is present.
Expected results	1) Tag '7F2E' may be present and shall not occur more than once. 2) If Tag '7F2E' 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 '7F2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4) If Tag '7F2E' is present, Tag '5F2E' shall be absent. 5) If Tag '7F2E' is absent, Tag '5F2E' shall be present.

A.3.7.20 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:—, 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.3.7.21 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:—, 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.3.7.22 Test case SE_LDS_DG6_022

Test case-ID	SE_LDS_DG6_022
Purpose	This test checks the encoding of the Security Block (Tag '5F3D') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG6.
Version	1.0
References	ISO/IEC 18013-2:—, 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 '5F3D') inside the Biometric Template. 2) If Tag '5F3D' is present, analyze the encoding of the bytes that follow the Security Block tag. 3) If Tag '5F3D' is present, verify the length of the Security Block DO.

Expected results	1) Tag '5F3D' may be present and shall not occur more than once. 2) If Tag '5F3D' 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 '5F3D' 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

A.3.8.1 General

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

A.3.8.2 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:—, 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) The first byte shall be '63'.

A.3.8.3 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:—, 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.3.8.4 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 '7F61') present in EF.DG7.

Version	1.0
References	ISO/IEC 18013-2:—, Annex C
Profile	DG7
Preconditions	1) EF.DG7 has been retrieved from the IDL.
Test scenario	1) Search for the Biometric Group Template (Tag '7F61') 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 '7F61' shall be present. 2) The bytes that follow the Tag '7F61' 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.3.8.5 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:—, 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 '7F60' in the Biometric Group Template.

A.3.8.6 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:—, 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 '7F60'. 3) Verify the length of the DO with Tag '7F60'.
Expected results	1) The tag shall be '7F60'. 2) The bytes that follow the Tag '7F60' 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 '7F60'.

A.3.8.7 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:—, 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.3.8.8 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:—, 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.3.8.9 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:—, 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.3.8.10 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:—, 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.3.8.11 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:—, 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.3.8.12 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:—, 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.3.8.13 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:—, 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.3.8.14 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:—, 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 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 18013-2:—, Annex C.

A.3.8.15 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:—, 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 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 18013-2:—, Annex C.

A.3.8.16 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:—, 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 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 18013-2:—, Annex C. 5) The BDB Format Type shall be valid in combination with the format owner data element.

A.3.8.17 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:—, 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.3.8.18 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 '5F2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:—, 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 '5F2E') inside the Biometric Template. 2) If Tag '5F2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3) If Tag '5F2E' is present, verify the length of the Biometric Data Block DO. 4) If Tag '5F2E' is present, verify that the tag for the Enciphered Biometric Data Block (Tag '7F2E') is absent. 5) If Tag '5F2E' is absent, verify that the tag for the Enciphered Biometric Data Block (Tag '7F2E') is present.
Expected results	1) Tag '5F2E' may be present and shall not occur more than once. 2) If Tag '5F2E' 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 '5F2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4) If Tag '5F2E' is present, Tag '7F2E' shall be absent. 5) If Tag '5F2E' is absent, Tag '7F2E' shall be present.

A.3.8.19 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 '7F2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:—, 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 '7F2E') inside the Biometric Template. 2) If Tag '7F2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3) If Tag '7F2E' is present, verify the length of the Enciphered Biometric Data Block DO. 4) If Tag '7F2E' is present, verify that the tag for the Biometric Data Block (Tag '5F2E') is absent. 5) If Tag '7F2E' is absent, verify that the tag for the Biometric Data Block (Tag '5F2E') is present.
Expected results	1) Tag '7F2E' may be present and shall not occur more than once. 2) If Tag '7F2E' 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 '7F2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4) If Tag '7F2E' is present, Tag '5F2E' shall be absent. 5) If Tag '7F2E' is absent, Tag '5F2E' shall be present.

A.3.8.20 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:—, 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.3.8.21 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:—, 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.3.8.22 Test case SE_LDS_DG7_022

Test case-ID	SE_LDS_DG7_022
Purpose	This test checks the encoding of the Security Block (Tag '5F3D') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG7.
Version	1.0
References	ISO/IEC 18013-2:—, 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 '5F3D') inside the Biometric Template. 2) If Tag '5F3D' is present, analyze the encoding of the bytes that follow the Security Block tag. 3) If Tag '5F3D' is present, verify the length of the Security Block DO.

Expected results	1) Tag '5F3D' may be present and shall not occur more than once. 2) If Tag '5F3D' 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 '5F3D' 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

A.3.9.1 General

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

A.3.9.2 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:—, 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) The first byte shall be '76'.

A.3.9.3 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:—, 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.3.9.4 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 '7F61') present in EF.DG8.

Version	1.0
References	ISO/IEC 18013-2:—, Annex C
Profile	DG8
Preconditions	1) EF.DG8 has been retrieved from the IDL.
Test scenario	1) Search for the Biometric Group Template (Tag '7F61') 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 '7F61' shall be present. 2) The bytes that follow the Tag '7F61' 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.3.9.5 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:—, 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 '7F60' in the Biometric Group Template.

A.3.9.6 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:—, 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 '7F60'. 3) Verify the length of the DO with Tag '7F60'.
Expected results	1) The tag shall be '7F60'. 2) The bytes that follow the Tag '7F60' 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 '7F60'.

A.3.9.7 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:—, 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.3.9.8 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:—, 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.3.9.9 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:—, 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.3.9.10 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:—, 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.3.9.11 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:—, 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.3.9.12 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:—, 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.3.9.13 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:—, 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.3.9.14 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:—, 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 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 18013-2:—, Annex C.

A.3.9.15 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:—, 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 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 18013-2:—, Annex C.

A.3.9.16 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:—, 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 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 18013-2:—, Annex C. 5) The BDB Format Type shall be valid in combination with the format owner data element.

A.3.9.17 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:—, 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.3.9.18 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 '5F2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:—, 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 '5F2E') inside the Biometric Template. 2) If Tag '5F2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3) If Tag '5F2E' is present, verify the length of the Biometric Data Block DO. 4) If Tag '5F2E' is present, verify that the tag for the Enciphered Biometric Data Block (Tag '7F2E') is absent. 5) If Tag '5F2E' is absent, verify that the tag for the Enciphered Biometric Data Block (Tag '7F2E') is present.
Expected results	1) Tag '5F2E' may be present and shall not occur more than once. 2) If Tag '5F2E' 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 '5F2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4) If Tag '5F2E' is present, Tag '7F2E' shall be absent. 5) If Tag '5F2E' is absent, Tag '7F2E' shall be present.

A.3.9.19 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 '7F2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:—, 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 '7F2E') inside the Biometric Template. 2) If Tag '7F2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3) If Tag '7F2E' is present, verify the length of the Enciphered Biometric Data Block DO. 4) If Tag '7F2E' is present, verify that the tag for the Biometric Data Block (Tag '5F2E') is absent. 5) If Tag '7F2E' is absent, verify that the tag for the Biometric Data Block (Tag '5F2E') is present.
Expected results	1) Tag '7F2E' may be present and shall not occur more than once. 2) If Tag '7F2E' 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 '7F2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4) If Tag '7F2E' is present, Tag '5F2E' shall be absent. 5) If Tag '7F2E' is absent, Tag '5F2E' shall be present.

A.3.9.20 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:—, 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.3.9.21 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:—, 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.3.9.22 Test case SE_LDS_DG8_022

Test case-ID	SE_LDS_DG8_022
Purpose	This test checks the encoding of the Security Block (Tag '5F3D') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG8.
Version	1.0
References	ISO/IEC 18013-2:—, 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 '5F3D') inside the Biometric Template. 2) If Tag '5F3D' is present, analyze the encoding of the bytes that follow the Security Block tag. 3) If Tag '5F3D' is present, verify the length of the Security Block DO.

Expected results	1) Tag '5F3D' may be present and shall not occur more than once. 2) If Tag '5F3D' 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 '5F3D' 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

A.3.10.1 General

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

A.3.10.2 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:—, 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) The first byte shall be '70'.

A.3.10.3 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:—, 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.3.10.4 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 '7F61') present in EF.DG9.

Version	1.0
References	ISO/IEC 18013-2:—, Annex C
Profile	DG9
Preconditions	1) EF.DG9 has been retrieved from the IDL.
Test scenario	1) Search for the Biometric Group Template (Tag '7F61') 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 '7F61' shall be present. 2) The bytes that follow the Tag '7F61' 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.3.10.5 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:—, 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 '7F60' in the Biometric Group Template.

A.3.10.6 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:—, 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 '7F60'. 3) Verify the length of the DO with Tag '7F60'.
Expected results	1) The tag shall be '7F60'. 2) The bytes that follow the Tag '7F60' 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 '7F60'.

A.3.10.7 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:—, 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.3.10.8 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:—, 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.3.10.9 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:—, 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 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 18013-2:—, Annex C.

A.3.10.10 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:—, 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.3.10.11 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:—, 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.3.10.12 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:—, 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.3.10.13 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:—, 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.3.10.14 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:—, 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 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 18013-2:—, Annex C.

A.3.10.15 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:—, 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 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 18013-2:—, Annex C.

A.3.10.16 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:—, 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 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 18013-2:—, Annex C. 5) The BDB Format Type shall be valid in combination with the format owner data element.

A.3.10.17 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:—, 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.3.10.18 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 '5F2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:—, 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 '5F2E') inside the Biometric Template. 2) If Tag '5F2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3) If Tag '5F2E' is present, verify the length of the Biometric Data Block DO. 4) If Tag '5F2E' is present, verify that the tag for the Enciphered Biometric Data Block (Tag '7F2E') is absent. 5) If Tag '5F2E' is absent, verify that the tag for the Enciphered Biometric Data Block (Tag '7F2E') is present.
Expected results	1) Tag '5F2E' may be present and shall not occur more than once. 2) If Tag '5F2E' 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 '5F2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4) If Tag '5F2E' is present, Tag '7F2E' shall be absent. 5) If Tag '5F2E' is absent, Tag '7F2E' shall be present.

A.3.10.19 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 '7F2E') in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:—, 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 '7F2E') inside the Biometric Template. 2) If Tag '7F2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3) If Tag '7F2E' is present, verify the length of the Enciphered Biometric Data Block DO. 4) If Tag '7F2E' is present, verify that the tag for the Biometric Data Block (Tag '5F2E') is absent. 5) If Tag '7F2E' is absent, verify that the tag for the Biometric Data Block (Tag '5F2E') is present.
Expected results	1) Tag '7F2E' may be present and shall not occur more than once. 2) If Tag '7F2E' 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 '7F2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4) If Tag '7F2E' is present, Tag '5F2E' shall be absent. 5) If Tag '7F2E' is absent, Tag '5F2E' shall be present.

A.3.10.20 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:—, 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.3.10.21 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:—, 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.3.10.22 Test case SE_LDS_DG9_022

Test case-ID	SE_LDS_DG9_022
Purpose	This test checks the encoding of the Security Block (Tag '5F3D') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:—, 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 '5F3D') inside the Biometric Template. 2) If Tag '5F3D' is present, analyze the encoding of the bytes that follow the Security Block tag. 3) If Tag '5F3D' is present, verify the length of the Security Block DO.

Expected results	1) Tag '5F3D' may be present and shall not occur more than once. 2) If Tag '5F3D' 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 '5F3D' 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

A.3.11.1 General

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 ISO/IEC 18013-3

A.3.11.2 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
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) The first byte shall be '77'.

A.3.11.3 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
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.3.11.4 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 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 EF.SOD template shall be a ContentInfo data element of the SignedData Type as specified in RFC-3369.

A.3.11.5 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 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 18013-3:2017, 8.1.4. 3) The eContentType shall have OID as specified in ISO/IEC 18013-3:2017, Table 2. 4) Tag 'A0' may be present and shall occur only once. 5) Tag 'A1' shall be absent.

A.3.11.6 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 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 available from a trusted source. 4) The digestAlgorithms list shall be one of the algorithms specified in ISO/IEC 18013-3:2017, 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 18013-3:2017, 8.1.5 [i.e. the algorithm shall be using RSASSA-PSS, RSASSA-PKCS1-v1.5, or ECDSA (ANSI X9.62)]. 13) The signature shall be valid.

A.3.11.7 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 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 18013-3:2017, 8.1.5.1. 3) The version shall be 0. 4) The digestAlgorithms list shall be one of the digest algorithms specified in ISO/IEC 18013-3:2017, 8.1.4 (i.e. SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512). 5) The Hash Sequence shall contain 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 contain 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.3.11.8 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 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 a trusted source). 4) The Issuing Authority Certificate has been retrieved from a trusted source.

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 SubjectKeyIdentifier extension of the country signing certificate matches the AuthorityKeyIdentifier of the 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). The validity period of the signing certificate shall be within the validity period of the country signing certificate. 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 18013-3:2017, 8.1.5 (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 marked critical and only the digitalSignature bit shall be set. 11) The signatureAlgorithm shall indicate one of the algorithms specified in ISO/IEC 18013-3:2017, 8.1.5 (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

A.3.12.1 General

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 ISO/IEC 18013-3

A.3.12.2 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
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) The first byte shall be '71'.

A.3.12.3 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
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.3.12.4 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 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.3.12.5 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	1.2
References	ISO/IEC 18013-3
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' or '4'. 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 ISO/IEC 18013-3 [TR-ICAO Part 3]

Test cases, which were defined in ISO/IEC 18013-4:2011, are replaced by test cases defined in [TR-ICAO Part 3].

Apply [TR-ICAO Part 3], clause 4.7.

For eMRTD, read IDL.

For EF.DG15, read EF.DG13.

For R1, read ISO/IEC 18013-2:— and ISO/IEC 18013-3:2017

In test case LDS_J_05, delete Test Scenario step 4 and Expected Result step 4.

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:— ISO/IEC 18013-3:2017 [TR-ICAO Part 3]

EAP is not supported in ISO/IEC 18013-3:2017.

Apply [TR-ICAO Part 3], clause 4.5.

For eMRTD, read IDL.

For [R1], read [Doc 9303].

For [R5] read [BSI TR-03111].

In test case LDS_E_07 Expected result step 3 delete:

- ecdsa-plain-SHA1: (OID: 0.4.0.127.0.7.1.1.4.1.1)
- ecdsa-plain-RIPEMD160: (OID: 0.4.0.127.0.7.1.1.4.1.6)

The following test case shall not be applied:

- Test case LDS_E_08.

A.3.15 Test unit SE_LDS_CardAccess — Tests for EF.CardAccess

Apply [TR-ICAO Part 3], clause 4.6.

For eMRTD, read IDL.

For [R1], read [Doc 9303]

In Test case LDS_I_02 step 2, replace the algorithm identifier list by the following:

- id-PACE-ECDH-GM-3DES-CBC-CBC
  (OID : 0.4.0.127.0.7.2.2.4.2.1)
- id-PACE-ECDH-GM-AES-CBC-CMAC-128
  (OID : 0.4.0.127.0.7.2.2.4.2.2)
- id-PACE-ECDH-GM-AES-CBC-CMAC-192
  (OID : 0.4.0.127.0.7.2.2.4.2.3)

- id-PACE-ECDH-GM-AES-CBC-CMAC-256
  (OID : 0.4.0.127.0.7.2.2.4.2.4)

In Test case LDS_I_02 step 5, remove the following ParameterId from the list:

- '00' if 1024-bit MODP Group with 160-bit Prime Order Subgroup is used.
- '01' if 2048-bit MODP Group with 224-bit Prime Order Subgroup is used.
- '02' if 2048-bit MODP Group with 256-bit Prime Order Subgroup is used.

In Test case LDS_I_03 step 2, replace the protocol identifier list by the following:

- id-PACE-ECDH-GM
  (OID : 0.4.0.127.0.7.2.2.4.2)

In Test case LDS_I_03 step 3, replace the algorithm identifier list by the following:

- ecPublicKey (OID: 1.2.840.10045.2.1)

In Test case LDS_I_03 step 4, the parameters shall only follow KAEG specification (ECDH). Remove DH verification.

The following test case shall not be applied:

- Test case LDS_I_04

A.3.16 Test unit SE_LDS_MRZ — Tests for 1-line MRZ

A.3.16.1 General

Test unit-ID	SE_LDS_MRZ (Standard Encoding — Machine Readable Zone)
Purpose	The test cases in this test unit verify the structure and content of the 1-line Machine Readable Zone.
References	ISO/IEC 18013-3

A.3.16.2 Test case SE_LDS_MRZ_001

Test case-ID	SE_LDS_MRZ_001
Purpose	This test checks the length of the MRZ.
Version	1.2
References	ISO/IEC 18013-3
Profile	MRZ
Preconditions	1) The MRZ has been read from the IDL.
Test scenario	1) Count the characters of the MRZ.
Expected results	1) The MRZ shall consist of 30 characters

A.3.16.3 Test case SE_LDS_MRZ_002

Test case-ID	SE_LDS_MRZ_002
Purpose	This test checks the encoding of the "Identifier" element of the MRZ.
Version	1.2
References	ISO/IEC 18013-3

Profile	MRZ
Preconditions	1) The MRZ has been read from the IDL.
Test scenario	1) Analyse the 1st character of the MRZ.
Expected results	1) The 1st character of the MRZ shall have a value of “D”.

A.3.16.4 Test case SE_LDS_MRZ_003

Test case-ID	SE_LDS_MRZ_003
Purpose	This test checks the encoding of the “Configuration” element of the MRZ.
Version	1.2
References	ISO/IEC 18013-3
Profile	MRZ
Preconditions	1) The MRZ has been read from the IDL.
Test scenario	1) Analyse the 2nd character of the MRZ.
Expected results	1) The 2nd character of the MRZ shall have a value conforming to the specification of the configuration data element specified in ISO/IEC 18013-3:2017, 8.3.2.5.3.

A.3.16.5 Test case SE_LDS_MRZ_004

Test case-ID	SE_LDS_MRZ_004
Purpose	This test checks the encoding of the “Discretionary data” element of the MRZ.
Version	1.2
References	ISO/IEC 18013-3
Profile	MRZ
Preconditions	1) The MRZ has been read from the IDL.
Test scenario	1) Analyse the 3rd to 29th character of the MRZ.
Expected results	1) The 3rd to 29th characters of the MRZ shall only contain characters of the following character set: 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z < excluding the space character.

A.3.16.6 Test case SE_LDS_MRZ_005

Test case-ID	SE_LDS_MRZ_005
Purpose	This test checks the encoding and value of the “Check digit” element.
Version	1.2
References	ISO/IEC 18013-3
Profile	MRZ
Preconditions	1) The MRZ has been read from the IDL.
Test scenario	1) Analyse the 30th character of the MRZ. 2) Calculate the check digit over the characters in positions 1-29.
Expected results	1) The 30th character of the MRZ shall have a numerical value. 2) The value of the encoded check digit shall match the calculated check digit.

A.3.16.7 Test case SE_LDS_MRZ_006

Test case-ID	SE_LDS_MRZ_006

Purpose	This test checks the consistency of the “Configuration” element with the actual configuration of the IDL.
Version	1.2
References	ISO/IEC 18013-3
Profile	MRZ
Preconditions	1) The MRZ has been read from the IDL. 2) The 2nd character of the MRZ has been analysed.
Test scenario	1) If the 2nd character contains a value other than “<”, perform the security mechanism indicated in the “Configuration” element.
Expected results	1) The “Configuration” element shall be consistent with the actual configuration of the card (e.g for “P”, it shall be possible to establish a secure channel using PACE, etc.)

A.3.16.8 Test case SE_LDS_MRZ_007

Test case-ID	SE_LDS_MRZ_007
Purpose	This test checks successful establishment of BAP using the correct MRZ.
Version	1.2
References	ISO/IEC 18013-3
Profile	MRZ, BAP
Preconditions	1) The MRZ has been read from the IDL.
Test scenario	1) Establish BAP using the correct MRZ.
Expected results	1) Establishment of BAP shall be successful.

A.3.16.9 Test case SE_LDS_MRZ_008

Test case-ID	SE_LDS_MRZ_008
Purpose	This test checks that BAP shall not be established when using an incorrect MRZ.
Version	1.2
References	ISO/IEC 18013-3
Profile	MRZ, BAP
Preconditions	1) The MRZ has been read from the IDL. 2) At least 1 character of the “Discretionary data” element has been modified.
Test scenario	1) Establish BAP using the modified MRZ.
Expected results	1) Establishment of BAP shall fail.

A.3.16.10 Test case SE_LDS_MRZ_009

Test case-ID	SE_LDS_MRZ_009
Purpose	This test checks successful performance of NMA using the correct MRZ.
Version	1.2
References	ISO/IEC 18013-3
Profile	MRZ, NMA
Preconditions	1) The MRZ has been read from the IDL.
Test scenario	1) Perform NMA using the correct MRZ.
Expected results	1) Performance of NMA shall be successful.

A.3.16.11 Test case SE_LDS_MRZ_010

Test case-ID	SE_LDS_MRZ_010
Purpose	This test checks that NMA shall not be successful when using an incorrect MRZ.
Version	1.2
References	ISO/IEC 18013-3
Profile	MRZ, NMA
Preconditions	1) The MRZ has been read from the IDL. 2) At least 1 character of the “Discretionary data” element has been modified.
Test scenario	1) Perform NMA using the modified MRZ.
Expected results	1) Performance of NMA shall fail.

A.3.16.12 Test case SE_LDS_MRZ_011

Test case-ID	SE_LDS_MRZ_011
Purpose	This test checks successful establishment of PACE using the correct MRZ.
Version	1.2
References	ISO/IEC 18013-3
Profile	MRZ, PACE
Preconditions	1) The MRZ has been read from the IDL.
Test Scenario	1) Establish PACE using the correct MRZ.
Expected Results	1) Establishment of PACE shall be successful.

A.3.16.13 Test case SE_LDS_MRZ_012

Test case-ID	SE_LDS_MRZ_012
Purpose	This test checks that PACE shall not be established when using an incorrect MRZ.
Version	1.2
References	ISO/IEC 18013-3
Profile	MRZ, PACE
Preconditions	1) The MRZ has been read from the IDL. 2) At least 1 character of the “Discretionary data” element has been modified.
Test scenario	1) Establish PACE using the modified MRZ.
Expected results	1) Establishment of PACE shall fail.

Annex B
(normative)

Test case specification: Commands for SE on SIC

B.1 General

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 PACE, BAP, EAC 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 the ISO/IEC 7816 series or the ISO/IEC 14443 series can be used. The reader shall support extended length APDUs and command chaining.

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

For SIC supporting EAC, 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 PACE, BAP, EAC and AA as well as additional data groups (DG 2 to DG 14).

Since these elements are optional, it is not possible to define the corresponding tests as mandatory for each IDL. Therefore, this document 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 IDs are explicitly defined for DG 12 to DG14 because the EAC, 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, PACE or EAC)
Plain	Neither BAP nor PACE 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		
DG10	IDL contains elementary file with LDS Data Group 10		
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		
EAC (CA+TA)	Extended Access Control v1. Chip Authentication is based on Elliptic Curve Diffie-Hellman and Terminal Authentication is based on Elliptic curve algorithm		
CA-KAT	Chip Authentication with MSE:Set KAT		
CA-ATGA	Chip Authentication with MSE:Set AT & General Authenticate		
CA-KEYREF	Chip Authentication may use Explicit key selection (KeyId is used in ChipAuthenticationInfo and ChipAuthenticationPublicKeyInfo) (CA-KEYREF profile used in [TR-ICAO Part 3])		
TA-MIG	Terminal Authentication supports the migration of the cryptographic algorithm (MIG profile used in [BSI TR-03105-3.2])		
TA-DATE	Terminal Authentication supports Certificate date validation (DATE profile used in [BSI TR-03105-3.2])		
PACE	Password Authenticated Connection Establishment		

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:
EAC	Provide the Chip Authentication configuration list described in the EF.DG14 (Algorithm OID + Public Key parameters):
	Chip Authentication with MSE:Set AT & General Authenticate for 3DES algorithm support
	YES/NO
	Provide the Invalid key ID for explicit key selection (required for Test case ISO7816_I_14 and Test case ISO 7816_II_13 of explicit key selection is supported)
	Provide the Terminal authentication ECDSA algorithm (Key Size + Hash Algorithm):
	Provide the Primary trust point certificate information (Certification Authority Reference, Effective date, Expiration date): Note that for the test scenarios covered by this test plan the time span between “Effective date” and “Expiration date” shall be at least 2 months, otherwise some tests will fail.
	Provide the Primary trust point private key in PKCS 8 format:
	Provide the list of the supported target Terminal Authentication ECDSA algorihm (Key Size + Hash Algorithm):
DG11	Provide the template tag:

Table B.2 *(continued)*

Supported Profile	Configuration information
PACE	Provide the configuration list described in the EF.CardAccess (Algorithm OID + Domain parameters):
	Provide an invalid key reference for PACE (used in test case SE_ISO7816_PACE_09):
	Provide an invalid password identifier for PACE (used in test case SE_ISO7816_PACE_08):
	Provide a valid PACE OID not supported by the SIC (used in test case SE_ISO7816_PACE_68 — if such an OID can't be provided, SE_ISO7816_PACE_68 is not applicable):
	Provide the command to send to the SIC to verify the chip's ability to still require Secured APDU: If not provided, use '00 B0 81 00 00'.

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

For most of the test cases defined in this document, 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 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 ISO/IEC 7816-4:2013, 5.6.

B.3 Test layer SE_ISO7816 — Security and command tests

B.3.1 Test unit SE_ISO7816_SelDF — SELECT DF Command

B.3.1.1 General

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.3.1.2 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.3.1.3 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.3.1.4 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.3.1.5 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.3.1.6 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.3.1.7 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.3.1.8 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

B.3.2.1 General

This unit tests the security conditions of a BAP protected IDL. It shall not be possible to 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 SFI and unsecured READ BINARY while access is granted.

When accessing to EAC protected DG, extended access control shall be granted.

B.3.2.2 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.3.2.3 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.3.2.4 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.3.2.5 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.3.2.6 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.3.2.7 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.3.2.8 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.3.2.9 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.3.2.10 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.3.2.11 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.3.2.12 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.3.2.13 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.3.2.14 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.3.2.15 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.3.2.16 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.3.2.17 Test case SE_ISO7816_SecBAP_16

Test – ID	SE_ISO7816_SecBAP_16
Purpose	Selecting EF.DG14
Version	1.2
Profile	BAP, (EAC or PACE or AA-ECDSA)
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.3.2.18 Test case SE_ISO7816_SecBAP_17

Test – ID	SE_ISO7816_SecBAP_17
Purpose	Accesing the EF.COM by READ BINARY with SFI.
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.3.2.19 Test case SE_ISO7816_SecBAP_18

Test – ID	SE_ISO7816_SecBAP_18
Purpose	Accessing the EF.SOD (READ BINARY with SFI).
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.3.2.20 Test case SE_ISO7816_SecBAP_19

Test – ID	SE_ISO7816_SecBAP_19
Purpose	Accessing the EF.DG1 (READ BINARY with SFI).
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.3.2.21 Test case SE_ISO7816_SecBAP_20

Test – ID	SE_ISO7816_SecBAP_20
Purpose	Accessing the EF.DG2 (READ BINARY with SFI).
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.3.2.22 Test case SE_ISO7816_SecBAP_21

Test – ID	SE_ISO7816_SecBAP_21
Purpose	Accessing the EF.DG3 (READ BINARY with SFI).
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.3.2.23 Test case SE_ISO7816_SecBAP_22

Test – ID	SE_ISO7816_SecBAP_22
Purpose	Accessing the EF.DG4 (READ BINARY with SFI).
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.3.2.24 Test case SE_ISO7816_SecBAP_23

Test – ID	SE_ISO7816_SecBAP_23
Purpose	Accessing the EF.DG5 (READ BINARY with SFI).
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.3.2.25 Test case SE_ISO7816_SecBAP_24

Test – ID	SE_ISO7816_SecBAP_24
Purpose	Accessing the EF.DG6 (READ BINARY with SFI).
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.3.2.26 Test case SE_ISO7816_SecBAP_25

Test – ID	SE_ISO7816_SecBAP_25
Purpose	Accessing the EF.DG7 (READ BINARY with SFI).
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.3.2.27 Test case SE_ISO7816_SecBAP_26

Test – ID	SE_ISO7816_SecBAP_26
Purpose	Accessing the EF.DG8 (READ BINARY with SFI).
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.3.2.28 Test case SE_ISO7816_SecBAP_27

Test – ID	SE_ISO7816_SecBAP_27
Purpose	Accessing the EF.DG9 (READ BINARY with SFI).
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.3.2.29 Test case SE_ISO7816_SecBAP_28

Test – ID	SE_ISO7816_SecBAP_28
Purpose	Accessing the EF.DG10 (READ BINARY with SFI).
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.3.2.30 Test case SE_ISO7816_SecBAP_29

Test – ID	SE_ISO7816_SecBAP_29
Purpose	Accessing the EF.DG11 (READ BINARY with SFI).
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.3.2.31 Test case SE_ISO7816_SecBAP_30

Test – ID	SE_ISO7816_SecBAP_30
Purpose	Accessing the EF.DG12 (READ BINARY with SFI).
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.3.2.32 Test case SE_ISO7816_SecBAP_31

Test – ID	SE_ISO7816_SecBAP_31
Purpose	Accessing the EF.DG13 (READ BINARY with SFI).
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.3.2.33 Test case SE_ISO7816_SecBAP_32

Test – ID	SE_ISO7816_SecBAP_32
Purpose	Reading the EF.DG14 (READ BINARY with SFI).
Version	1.2
Profile	BAP, (EAC or PACE or AA-ECDSA)
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.3.2.34 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 (SFI) 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.3.2.35 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 (SFI) 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 Driving 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_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 (SFI) 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 Driving 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_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 (SFI) 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 Driving 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_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 (SFI) 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 Driving 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_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 (SFI) 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 Driving 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_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 (SFI) 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 Driving 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_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 (SFI) 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 Driving 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_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 (SFI) 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 Driving 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_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 (SFI) 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 Driving 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_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 (SFI) 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 Driving 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_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 (SFI) 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 Driving 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_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 (SFI) 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 Driving 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_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 (SFI) 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 Driving 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_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 (SFI) 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 Driving 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.3.2.49 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	1.2
Profile	BAP, (EAC or PACE or AA-ECDSA)
Preconditions	1) LDS application shall be selected and basic access shall be granted.
Test scenario	1) Send the given READ BINARY (SFI) 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 Driving 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

B.3.3.1 General

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.3.3.2 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.3.3.3 Test case SE_ISO7816_BAP_2

Test – ID	SE_ISO7816_BAP_2
Purpose	Checking the response to the MUTUAL AUTHENTICATE command (positive test).
Version	1.2
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. ’00 82 00 00 28 <Data> 28’
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.3.3.4 Test case SE_ISO7816_BAP_3

Test – ID	SE_ISO7816_BAP_3
Purpose	Checking the authentication failure response to the MUTUAL AUTHENTICATE command.
Version	1.2
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 an incorrect reference string for the IDL under test. ’00 82 00 00 28 <Data> 28’
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.3.3.5 Test case SE_ISO7816_BAP_4

Test – ID	SE_ISO7816_BAP_4
Purpose	Checking the authentication failure response to the MUTUAL AUTHENTICATE command.
Version	1.2
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 given MUTUAL AUTHENTICATE APDU to the IDL. The field <Data> shall be computed with the challenge ’00 00 00 00 00 00 00 00’. ’00 82 00 00 28 <Data> 28’ 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 given MUTUAL AUTHENTICATE APDU to the IDL. The field <Data> shall be computed with the challenge returned in step 2. ’00 82 00 00 28 <Data> 28’
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.3.3.6 Test case SE_ISO7816_BAP_5

Test – ID	SE_ISO7816_BAP_5
Purpose	Checking of the MUTUAL AUTHENTICATE command (robustness test).
Version	1.2
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. '80 82 00 00 28 <Data> 28' 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. '00 82 60 00 28 <Data> 28' 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. '00 82 00 60 28 <Data> 28' 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). '00 82 00 00 29 <Data> 28'
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.3.3.7 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	1.2
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. ’00 82 00 00 28 <Data> 28’
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.3.3.8 Test case SE_ISO7816_BAP_7

Test – ID	SE_ISO7816_BAP_7
Purpose	Checking the Secure Messaging encoding of a READ BINARY with SFI.
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 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 ‘87’. 3) The response of step 1 shall 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.3.3.9 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 SFI.
Version	1.2
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’ — <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.3.3.10 Test case SE_ISO7816_BAP_9

Test – ID	SE_ISO7816_BAP_9
Purpose	Checking the Secure Messaging encoding of a READ BINARY without SFI.
Version	1.2
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’ — <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.3.3.11 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 SFI.
Version	1.2
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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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 <L85> <Cryptogram> 97 01 06 8E 08 <Checksum> 00’ — <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.3.3.12 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	1.2
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 <L87> 01 <Cryptogram> 00’ — <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.3.3.13 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	1.2
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 <L87> 01 <Cryptogram> 8E 08 <CorruptedChecksum> 00’ — <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.3.3.14 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	1.2
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 <L87> 01 <Cryptogram> 8E 08 <CorruptedChecksum> 00' — <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.3.3.15 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	1.2
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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' — <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.3.3.16 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.3.3.17 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.3.3.18 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.3.3.19 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.3.3.20 Test case SE_ISO7816_BAP_19

Test – ID	SE_ISO7816_BAP_19
Purpose	This test checks the BAP configuration
Version	1.2
Profile	BAP
Preconditions	1) Input string for the IDL under test has been provided
Test scenario	1) Verifies the value of the first byte of the Input String
Expected results	1) The first byte shall be '31'

B.3.4 Test unit SE_ISO7816_SelEFSM — Protected SELECT EF command

B.3.4.1 General

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

For all test cases of unit test ISO7816_SelEFSM, basic access shall be granted as tested in ISO7816_BAP_2 for BAP and [TR-ICAO Part 3] 7816_P_1 for PACE. All APDUs shall be correctly encoded for Secure Messaging and the IDL responses shall be decoded correctly again.

If the IDL is BAP and PACE protected, PACE shall be used.

When accessing to EAC protected DG, extended access control shall be granted.

B.3.4.2 Test case SE_ISO7816_SelEFSM_1

Test – ID	SE_ISO7816_SelEFSM_1
Purpose	Checking the SELECT (EF.COM) command (positive test).
Version	1.2
Profile	BAP or PACE
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.3 Test case SE_ISO7816_SelEFSM_2

Test – ID	SE_ISO7816_SelEFSM_2
Purpose	Checking the robustness of the SELECT command (invalid class byte).
Version	1.2
Profile	BAP or PACE
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.4 Test case SE_ISO7816_SelEFSM_3

Test – ID	SE_ISO7816_SelEFSM_3
Purpose	Checking the robustness of the SELECT command (invalid parameter P1).

Version	1.2
Profile	BAP or PACE
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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_4

Test – ID	SE_ISO7816_SelEFSM_4
Purpose	Checking the robustness of the SELECT command (invalid parameter P2).
Version	1.2
Profile	BAP or PACE
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.6 Test case SE_ISO7816_SelEFSM_5

Test – ID	SE_ISO7816_SelEFSM_5
Purpose	Checking the robustness of the SELECT command (invalid File identifier).
Version	1.2
Profile	BAP or PACE
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.7 Test case SE_ISO7816_SelEFSM_6

Test – ID	SE_ISO7816_SelEFSM_6
Purpose	Checking the SELECT (EF.SOD) command (positive test).
Version	1.2
Profile	(BAP or PACE), PA
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.8 Test case SE_ISO7816_SelEFSM_7

Test – ID	SE_ISO7816_SelEFSM_7
Purpose	Checking the SELECT (EF.DG1) command (positive test).
Version	1.2
Profile	BAP or PACE
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.9 Test case SE_ISO7816_SelEFSM_8

Test – ID	SE_ISO7816_SelEFSM_8
Purpose	Checking the SELECT (EF.DG2) command (positive test).
Version	1.2
Profile	(BAP or PACE), DG2
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.10 Test case SE_ISO7816_SelEFSM_9

Test – ID	SE_ISO7816_SelEFSM_9
Purpose	Checking the SELECT (EF.DG3) command (positive test).
Version	1.2
Profile	(BAP or PACE), DG3
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.11 Test case SE_ISO7816_SelEFSM_10

Test – ID	SE_ISO7816_SelEFSM_10
Purpose	Checking the SELECT (EF.DG4) command (positive test).
Version	1.2
Profile	(BAP or PACE), DG4
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.12 Test case SE_ISO7816_SelEFSM_11

Test – ID	SE_ISO7816_SelEFSM_11
Purpose	Checking the SELECT (EF.DG5) command (positive test).
Version	1.2
Profile	(BAP or PACE), DG5
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.13 Test case SE_ISO7816_SelEFSM_12

Test – ID	SE_ISO7816_SelEFSM_12
Purpose	Checking the SELECT (EF.DG6) command (positive test).
Version	1.2
Profile	(BAP or PACE), DG6

Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.14 Test case SE_ISO7816_SelEFSM_13

Test – ID	SE_ISO7816_SelEFSM_13
Purpose	Checking the SELECT (EF.DG7) command (positive test).
Version	1.2
Profile	(BAP or PACE), DG7
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.15 Test case SE_ISO7816_SelEFSM_14

Test – ID	SE_ISO7816_SelEFSM_14
Purpose	Checking the SELECT (EF.DG8) command (positive test).
Version	1.2
Profile	(BAP or PACE), DG8
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.16 Test case SE_ISO7816_SelEFSM_15

Test – ID	SE_ISO7816_SelEFSM_15
Purpose	Checking the SELECT (EF.DG9) command (positive test).
Version	1.2
Profile	(BAP or PACE), DG9
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.17 Test case SE_ISO7816_SelEFSM_16

Test – ID	SE_ISO7816_SelEFSM_16
Purpose	Checking the SELECT (EF.DG10) command (positive test).
Version	1.2
Profile	(BAP or PACE), DG10
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.18 Test case SE_ISO7816_SelEFSM_17

Test – ID	SE_ISO7816_SelEFSM_17
Purpose	Checking the SELECT (EF.DG11) command (positive test).
Version	1.2
Profile	(BAP or PACE), DG11
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.19 Test case SE_ISO7816_SelEFSM_18

Test – ID	SE_ISO7816_SelEFSM_18
Purpose	Checking the SELECT (EF.DG12) command (positive test).
Version	1.2
Profile	(BAP or PACE), NMA
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.20 Test case SE_ISO7816_SelEFSM_19

Test – ID	SE_ISO7816_SelEFSM_19
Purpose	Checking the SELECT (EF.DG13) command (positive test).
Version	1.2
Profile	(BAP or PACE), AA
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.21 Test case SE_ISO7816_SelEFSM_20

Test – ID	SE_ISO7816_SelEFSM_20
Purpose	Checking the SELECT (EF.DG14) command (positive test).
Version	1.2
Profile	(BAP, (EAC or AA-ECDSA)) or PACE
Preconditions	1) LDS application shall be selected. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ — <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.3.4.22 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	1.2
Profile	BAP or PACE