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

**Part 4:
Test methods**

iTeh STANDARD PREVIEW
*Technologies de l'information — Identification des personnes — Permis
de conduire conforme à l'ISO —
(standards.iteh.ai)
Partie 4. Méthodes d'essai*

ISO/IEC 18013-4:2011

[https://standards.iteh.ai/catalog/standards/sist/605e23ee-1ec9-4dfe-ad2b-
bb832487b3da/iso-iec-18013-4-2011](https://standards.iteh.ai/catalog/standards/sist/605e23ee-1ec9-4dfe-ad2b-bb832487b3da/iso-iec-18013-4-2011)

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 18013-4:2011](https://standards.iteh.ai/catalog/standards/sist/605e23ee-1ec9-4dfe-ad2b-bb832487b3da/iso-iec-18013-4-2011)

<https://standards.iteh.ai/catalog/standards/sist/605e23ee-1ec9-4dfe-ad2b-bb832487b3da/iso-iec-18013-4-2011>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

Contents

Page

Foreword	v
Introduction.....	vi
1 Scope	1
2 Conformance	1
3 Normative references	2
4 Terms and definitions	2
5 Abbreviated terms	2
6 Test design.....	3
6.1 General	3
6.2 Test hierarchy	3
6.3 Test administration	6
7 IDL Conformity test methods	7
7.1 Overview.....	7
7.2 Profiles.....	7
7.3 IDL test case specifications	7
7.4 Conformance	8
Annex A (normative) Test case specification: LDS in SE on SIC	9
A.1 Introduction.....	9
A.2 General test requirements	9
A.2.1 Preconditions for testing	9
A.2.2 Test setup.....	9
A.2.3 Implementation conformance statement	9
A.3 Test Layer SE_LDS – Logical Data Structure Tests	11
A.3.1 Test Unit SE_LDS_COM – Tests for EF.Com.....	11
A.3.2 Test Unit SE_LDS_DG1 – Tests for EF.DG1	17
A.3.3 Test Unit SE_LDS_DG2 – Tests for EF.DG2	27
A.3.4 Test Unit SE_LDS_DG3 – Tests for EF.DG3	32
A.3.5 Test Unit SE_LDS_DG4 – Tests for EF.DG4	35
A.3.6 Test Unit SE_LDS_DG5 – Tests for EF.DG5	38
A.3.7 Test Unit SE_LDS_DG6 – Tests for EF.DG6	39
A.3.8 Test Unit SE_LDS_DG7 – Tests for EF.DG7	48
A.3.9 Test Unit SE_LDS_DG8 – Tests for EF.DG8	57
A.3.10 Test Unit SE_LDS_DG9 – Tests for EF.DG9	67
A.3.11 Test Unit SE_LDS_SOD – Tests for EF.SOD.....	77
A.3.12 Test Unit SE_LDS_DG12 – Tests for EF.DG12	81
A.3.13 Test Unit SE_LDS_DG13 – Tests for EF.DG13	83
A.3.14 Test Unit SE_LDS_DG14 – Tests for EF.DG14	86
Annex B (normative) Test case specification: Commands for SE on SIC	90
B.1 Introduction.....	90
B.2 General test requirements	90
B.2.1 Preconditions for testing	90
B.2.2 Test setup.....	90
B.2.3 Implementation conformance statement	90
B.2.4 Verification of ISO/IEC 7816-4 status bytes	92
B.2.5 Key pair definition	93
B.2.6 Certificate specification	94
B.3 Test Layer SE_ISO7816 - Security and Command Tests	159

B.3.1	Test Unit SE_ISO7816_SelDF – SELECT DF Command	160
B.3.2	Test Unit SE_ISO7816_SecBAP– Security conditions of BAP protected IDL	162
B.3.3	Test Unit SE_ISO7816_BAP – Basic Access Protection	180
B.3.4	Test Unit SE_ISO7816_SelEFM – Protected SELECT EF Command.....	190
B.3.5	Test Unit SE_ISO7816_ReadEFM – Protected READ BINARY Command.....	200
B.3.6	Test Unit SE_ISO7816_SelEF – Unprotected SELECT EF Command	208
B.3.7	Test Unit SE_ISO7816_ReadEF – Unprotected READ BINARY Command.....	216
B.3.8	Test Unit SE_ISO7816_AA – Active Authentication	224
B.3.9	Test Unit SE_ISO7816_SecEAP - Security Conditions for EAP protected IDL	228
B.3.10	Test Unit SE_ISO7816_CA - Chip Authentication.....	243
B.3.11	Test Unit SE_ISO7816_CertVer - Certificate verification	261
B.3.12	Test Unit SE_ISO7816_TA - Terminal Authentication	295
B.3.13	Test Unit SE_ISO7816_AccCond - Effective Access Conditions.....	308
B.3.14	Test Unit SE_ISO7816_Update - Update mechanism.....	321
B.3.15	Test Unit SE_ISO7816_Migration – Migration policies	326
B.4	Summary of test cases.....	327
	Bibliography.....	330

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 18013-4:2011](https://standards.iteh.ai/catalog/standards/sist/605e23ee-1ec9-4dfe-ad2b-bb832487b3da/iso-iec-18013-4-2011)

<https://standards.iteh.ai/catalog/standards/sist/605e23ee-1ec9-4dfe-ad2b-bb832487b3da/iso-iec-18013-4-2011>

Foreword

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

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

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

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

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

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

- *Part 1: Physical characteristics and basic data set*
ISO/IEC 18013-4:2011
<https://standards.iteh.ai/catalog/standards/sist/605e23ee-1ec9-4dfe-ad2b-bb832487b3da/iso-iec-18013-4-2011>
- *Part 2: Machine-readable technologies*
- *Part 3: Access control, authentication and integrity validation*
- *Part 4: Test methods*

Introduction

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

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

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

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

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

<https://standards.iteh.ai/catalog/standards/sist/605e23ee-1ec9-4dfe-ad2b-bb832487b3da/iso-iec-18013-4-2011>

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

Part 4: Test methods

1 Scope

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

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

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

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

Hence, this part of ISO/IEC 18013

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

2 Conformance

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

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

3 Normative references

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

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

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

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

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

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

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

4 Terms and definitions

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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/IEC 18013-4:2011](https://standards.iteh.ai/catalog/standards/sist/605e23ee-1ec9-4dfe-ad2b-bb832487b3da/iso-iec-18013-4-2011)

4.1 test case <https://standards.iteh.ai/catalog/standards/sist/605e23ee-1ec9-4dfe-ad2b-bb832487b3da/iso-iec-18013-4-2011>

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

4.2 test case specification

collection of test cases, and general test data applicable to the test cases

5 Abbreviated terms

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

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

<https://standards.iteh.ai/catalog/standards/sist/605e23ee-1ec9-4dfe-ad2b-bb832487b3da/iso-iec-18013-4-2011>
 (standards.iteh.ai)

6 Test design

6.1 General

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

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

6.2 Test hierarchy

6.2.1 Structure

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

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

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

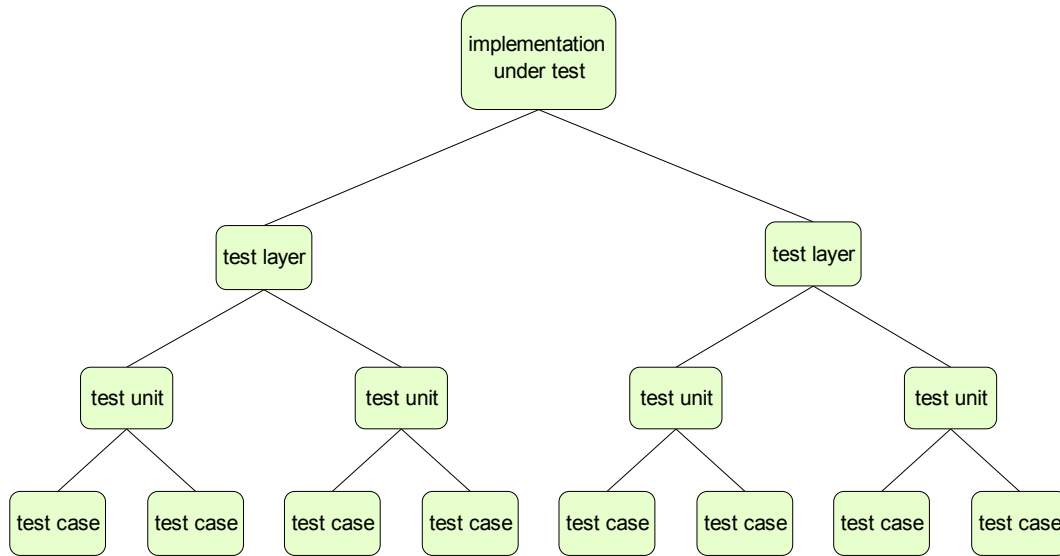


Figure 1 — Test element hierarchy

6.2.2 Implementation under test

6.2.2.1 Overview

Three IUTs are defined:

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

6.2.2.2 Profile

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

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

The Profile specification shall include:

- Profile-ID
- Profile description

6.2.3 Test layer

6.2.3.1 Overview

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

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

The other layers are not applicable.

Each test layer comprises a number of test units.

6.2.3.2 Layer 7 – Logical data structure tests

Layer 7 tests cover LDS requirements. LDS requirements include:

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

6.2.3.3 Layer 6 – Command tests

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

- Compact encoding
- Standard encoding.

6.2.4 Test unit

iTeh STANDARD PREVIEW

(standards.iteh.ai)

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:
<https://standards.iteh.ai/catalog/standards/sist/605e23ee-1ec9-4dfe-ad2b-bb832487b3da/iso-iec-18013-4-2011>

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

6.2.5 Test case

Each test case is defined by the following information:

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

Preconditions	Define the state in which the IUT needs to be before the test case can be executed, including test cases that shall have been successfully passed, if any. If these preconditions are not fulfilled, the test is skipped and marked as such in the test report.
Test scenario	<p>Defines the test steps that shall be taken.</p> <p>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.</p> <p>Each test step is defined by the following information:</p> <ul style="list-style-type: none"> • 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

6.3 Test administration

6.3.1 Preconditions for testing

<https://standards.iteh.ai/catalog/standards/sist/605e23ee-1ec9-4dfe-ad2b-b0c325193da/iso-iec-18013-4-2011>

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

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

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

6.3.2 Implementation conformance statement

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

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

6.3.3 Test report

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

- test layer
- test unit

- test case
- test step

If a test is not applicable, this is noted.

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

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

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

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

7 IDL Conformity test methods

7.1 Overview

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

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

7.2 Profiles

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

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

Profiles for each IUT are defined in each annex.

7.3 IDL test case specifications

7.3.1 Scope

IDL test case specifications are attached in the annexes.

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

7.3.2 Standard encoding on SIC

Test case specifications for SE on SIC cover:

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

7.3.3 Compact encoding

Test case specifications for CE cover:

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

7.3.4 Standard encoding on optical memory

Test case specifications for SE on Optical Memory cover:

- LDS tests for SE on Optical Memory

7.4 Conformance

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

ITeH STANDARD PREVIEW
(standards.iteh.ai)
<https://standards.iteh.ai/catalog/standards/sist/605e23ee-1ec9-4dfe-ad2b-bb832487b3da/iso-iec-18013-4-2011>

Annex A (normative)

Test case specification: LDS in SE on SIC

A.1 Introduction

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

A.2 General test requirements

A.2.1 Preconditions for testing

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

All tests are mandatory unless marked as optional or conditional.

A.2.2 Test setup

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

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

A.2.3 Implementation conformance statement

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

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

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

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