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.

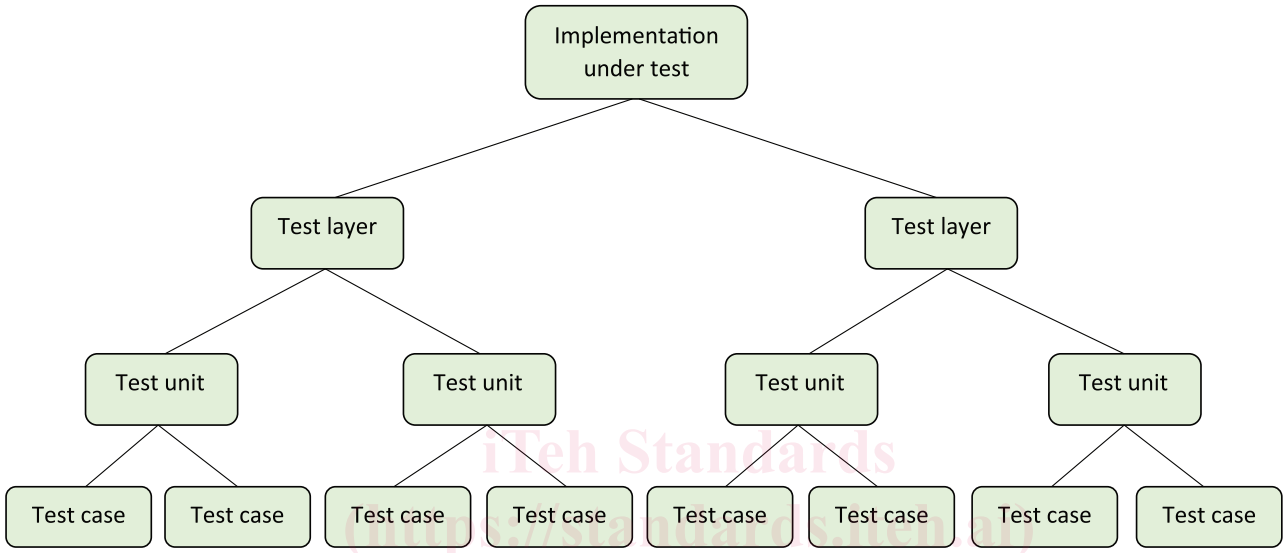

Figure 1 — Test element hierarchy

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.