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