FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
18013-2**

ISO/IEC JTC **1**/SC **17**

Secretariat: BSI

Voting begins on:
2020-03-24

Voting terminates on:
2020-05-19

Personal identification — ISO-compliant driving licence —

Part 2: Machine-readable technologies

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

Partie 2: Technologies lisibles par une machine

Reference number
ISO/IEC FDIS 18013-2:2020(E)

COPYRIGHT PROTECTED DOCUMENT

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 ..... **iv**

Introduction ..... **v**

1 Scope **1**

2 Normative references **1**

3 Terms, definitions and abbreviated terms **3**
- 3.1 Terms and definitions 3
- 3.2 Abbreviated terms 5

4 Conformance **5**

5 Machine-readable functionality of IDLs **6**
- 5.1 Overview 6
- 5.2 General principles 6
- 5.3 Mandatory functions 6
  - 5.3.1 General 6
  - 5.3.2 Privilege to drive at time of licensing 6
  - 5.3.3 Reference to driving privilege database 6
  - 5.3.4 Age verification 7
- 5.4 Optional functions 7
  - 5.4.1 Identity verification 7
  - 5.4.2 Biographical data verification 7
  - 5.4.3 Evidence of residence 7
  - 5.4.4 Biometric authentication 7
  - 5.4.5 Reciprocity of driving privileges 7
  - 5.4.6 Document authentication and validation 7

6 Machine-readable technologies supported **7**

7 Organization of data **8**
- 7.1 Overview 8
- 7.2 Mandatory data 8
- 7.3 Optional data 8

8 Data structure **8**
- 8.1 Conceptualisation 8
- 8.2 Data Group 1: mandatory text data elements 9
- 8.3 Data Group 2: optional licence holder details 10
- 8.4 Data Group 3: optional issuing authority details 11
- 8.5 Data Group 4: optional portrait image 12
- 8.6 Data Group 5: optional signature/usual mark image 12
- 8.7 Data groups 6, 7, 8 and 9: optional facial, fingerprint, iris and other biometric templates 12
- 8.8 Data Group 10: reserved for future use 14
- 8.9 Data Group 11: optional domestic data 14

9 Application identifiers **15**

Annex A (normative) **Assembly rules for categories of vehicles/restrictions/conditions field** **16**

Annex B (normative) **Compact encoding** **24**

Annex C (normative) **Standard encoding for ICCs with contacts and for PICCs** **34**

Annex D (normative) **Images** **59**

Bibliography **65**

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 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 18013-2:2008), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 18013-2:2008/Cor 1:2011.

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

— following the revision of ISO/IEC 18013-3 and ISO/IEC 18013-1, magnetic stripe and optical memory machine-readable technologies are no longer supported by this document;

— the vehicle categories in respect of which driving licence may be issued have been updated to incorporate the contemplated amendments to the UN Conventions;

— the restrictions which may be applicable to a driving licence have been updated.

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

ISO/IEC 18013 (all parts) 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), ISO 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 in applying their privacy rules and national/community/regional motor vehicle authorities in taking care of their specific needs.

This document prescribes requirements for the implementation of machine-readable technology on an IDL.

One of the functions of an IDL is to facilitate international interchange. Storing IDL data in a machine-readable form supports this function by speeding up data input and eliminating transcription errors. Consequently, the automation and productivity of traffic law enforcement and other traffic safety processes can be improved.

This document allows issuing authorities to customise machine-readable data for domestic use. Apart from international interchange, the use of an IDL as a domestic driving licence thus provides for domestic standardisation and creates a domestic infrastructure capable of processing IDLs issued by other issuing authorities.

Provision is made for issuing authorities to validate the authenticity and integrity of the mandatory and optional data. In addition, the option of protecting access to optional data (beyond basic access protection) is provided for. The exact mechanism used to achieve such protection (e.g. encryption and/or additional access control) is specified in ISO/IEC 18013-3.

Personal identification — ISO-compliant driving licence —

Part 2:
Machine-readable technologies

1 Scope

The purpose of storing IDL data on machine-readable media on the IDL is to:

— increase productivity (of data and IDL use),

— facilitate electronic data exchange, and

— assist in authenticity and integrity validation.

This document thus specifies the following:

— mandatory and optional machine-readable data;

— the logical data structure;

— encoding rules for the machine-readable technologies currently supported.

To prevent unauthorised access to the data contained on a contactless IC (e.g. by eavesdropping), the privacy of the licence holder is protected via basic access protection requiring a human-readable and/or machine-readable key/password on the IDL to access the data on the PIC (via protected-channel communication). The implementation details of this function are defined in ISO/IEC 18013-3.

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 5218, *Information technology — Codes for the representation of human sexes*

ISO/IEC 7812-1, *Identification cards — Identification of issuers — Part 1: Numbering system*

ISO/IEC 7816-1, *Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics*

ISO/IEC 7816-2, *Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimensions and location of the contacts*

ISO/IEC 7816-3, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

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

ISO/IEC 7816-5, *Identification cards — Integrated circuit cards — Part 5: Registration of application providers*

ISO/IEC 7816-6, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange*

ISO/IEC 7816-11:2017, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) — Part 1*

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

ISO/IEC 10918-1, *Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines — Part 1*

ISO/IEC 14443-1, *Cards and security devices for personal identification — Contactless proximity objects — Part 1: Physical characteristics*

ISO/IEC 14443-2, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio frequency power and signal interface*

ISO/IEC 14443-3, *Cards and security devices for personal identification — Contactless proximity objects — Part 3: Initialization and anticollision*

ISO/IEC 14443-4, *Cards and security devices for personal identification — Contactless proximity objects — Part 4: Transmission protocol*

ISO/IEC 15444-1, *Information technology — JPEG 2000 image coding system: Core coding system*

ISO/IEC 15948, *Information technology — Computer graphics and image processing — Portable Network Graphics (PNG): Functional specification*

ISO/IEC 18013 (all parts), *Information technology — Personal identification — ISO-compliant driving licence*

ISO/IEC 19785-1:2015, *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*

ISO/IEC 19785-3:2015, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

ISO/IEC 19794-2:2005, *Information technology — Biometric data interchange formats — Part 2: Finger minutiae data*

ISO/IEC 19794-3:2006, *Information technology — Biometric data interchange formats — Part 3: Finger pattern spectral data*

ISO/IEC 19794-4:2005, *Information technology — Biometric data interchange formats — Part 4: Finger image data*

ISO/IEC 19794-5:2005, *Information technology — Biometric data interchange formats — Part 5: Face image data*

ISO/IEC 19794-6:2005, *Information technology — Biometric data interchange formats — Part 6: Iris image data*

IEC 61966-2-1, *Multimedia systems and equipment — Colour measurement and management — Part 2-1: Colour management — Default RGB colour space — sRGB*

IAFIS-IC-0110(v3), *WSQ Gray-scale Fingerprint Image Compression Specification*, Federal Bureau of Investigation, Criminal Justice Information Services Division (1997)

ICAO, *Doc9303 Machine Readable Travel Documents*, Seventh Edition 2015

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 18013-1 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/

3.1.1
basic access protection
BAP
protection method requiring a human-readable and/or machine-readable key/password on the IDL to access the data on the secure IC via protected-channel communication

3.1.2
binary coded decimal
BCD
binary coding of a sequence of integers using 4 bits for each integer (where the bit weights are 8421) and encoding two integers per byte, and where a 0 digit is appended to the left of an integer sequence containing an uneven number of digits before encoding

Note 1 to entry: Only unsigned BCD is used in this document.

Note 2 to entry: For purposes of this document, the definition of numeric characters in ISO/IEC 18013-1 in terms of ISO/IEC 8859-1 is deemed to be for identification purposes of the numeric characters only, and does not pertain to the manner in which numeric characters have to be encoded. Encoding rules are explicitly specified in this document.

EXAMPLE See Table 1.

Table 1 — BCD examples

Integer	BCD
5	0000 0101
20	0010 0000
387	0000 0011 1000 0111

3.1.3
biometric data block
BDB
block of data with a defined format that contains one or more biometric samples or *biometric templates* (3.1.5)

3.1.4
biometric information record
BIR
BioAPI Consortium Patron Format biometric record header

3.1.5
biometric template
biometric sample (i.e. information obtained from a biometric device, either directly or after further processing) or combination of biometric samples that is suitable for storage as a reference for future comparison

Note 1 to entry: This definition is an expansion of a definition in ISO/IEC 19785-1:2015.

3.1.6
card holder
person using an IDL, who is not necessarily the legitimate licence holder

3.1.7
common biometric exchange file format
CBEFF
file format that promotes interoperability of biometric-based applications and systems by specifying a standard structure for a *BIR* (3.1.4) and a set of abstract data elements and values that can be used to create the header part of a CBEFF-compliant BIR

Note 1 to entry: This definition is based on descriptive language in ISO/IEC 19785-1:2015.

3.1.8
compact encoding
encoding method when the memory capacity available for the IDL application does not exceed 5 kB, typically applicable to 2D bar code symbologies, *RFID* (3.1.13) and limited memory-capacity ICs (PICs and ICs with contacts)

Note 1 to entry: Compact encoding generates one constructed data object containing all *data groups* (3.1.9). Selective reading is not possible and the read device reads all data at the same time, where after the data is parsed. Using this method for machine-readable technologies with large memory capacity is not recommended as it can result in prolonged reading time.

Note 2 to entry: Compact encoding may also be used where the total memory capacity exceeds 5 kB (e.g. ICs with contacts and PICs) but where the capacity available to the IDL application is limited due to capacity being reserved for other applications.

3.1.9
data group
DG
collection of related data elements

3.1.10
delimiter
D
character used to separate data elements in a machine-readable data stream

3.1.10.1
data group delimiter
multiplication sign "×"

Note 1 to entry: Character D7 of ISO/IEC 8859-1.

3.1.10.2
field delimiter
division sign "÷"

Note 1 to entry: Character F7 of ISO/IEC 8859-1.

3.1.10.3
sub-field delimiter
sub-delimiter
semicolon ";"

Note 1 to entry: Character 3B of ISO/IEC 8859-1.

3.1.10.4
end of file delimiter
pilcrow "¶"

Note 1 to entry: Character B6 of ISO/IEC 8859-1.

3.1.11
digital signature
data appended to, or cryptographic transformation of, a data string that proves the origin and the integrity of the data string and protects against forgery, e.g. by the recipient of the data string

3.1.12
standard encoding
encoding method when the memory capacity available for the IDL application exceeds 5 kB, typically applicable to ICs (PICs and ICs with contacts)

3.1.13
radio-frequency identification
RFID
ISO/IEC 14443-compliant IC designed primarily for data storage

3.2 Abbreviated terms

DF	dedicated file
EF	elementary file
F	fixed length field
IC	integrated circuit
ICC	integrated circuit card
LDS	logical data structure
MF	master file
PIC	proximity integrated circuit
PICC	proximity integrated circuit card
V	variable length field

4 Conformance

A driving licence is in conformance with this document if it meets all mandatory requirements specified directly or by reference herein. Compliance with ISO/IEC 18013-1 is not required for compliance with this document, except for those parts of ISO/IEC 18013-1 directly referenced in this document outside of Clause 3. Conversely, the incorporation of a machine-readable technology which is not compliant with this document does not necessarily render the IDL non-compliant with ISO/IEC 18013-1.

5 Machine-readable functionality of IDLs

5.1 Overview

The subclauses that follow specify the functions (mandatory and optional) to be supported by any machine-readable data elements used on an IDL. The optional domestic data elements incorporated at the discretion of an issuing authority may support additional functions than those specified below.

5.2 General principles

The use of machine-readable functionality in IDLs is optional. If used, all the data elements identified in ISO/IEC 18013-1 as mandatory for international interchange, except for the signature and portrait of the licence holder, shall be included in the machine-readable data. The machine-readable data elements may also include any other data/information that appears visually on the IDL (such as the identification of the issuing country), as well as additional data elements not reflected visually on the IDL. No machine-readable data/information shall conflict with the human-readable data/information. Machine-readable data elements shall, except for optional domestic data (see 8.9), have the exact same meaning as the human-readable data elements on the IDL.

NOTE A conflict between human-readable data elements and machine-readable data elements can cast suspicion upon the licence holder.

Rewriting, updating and appending functions may be supported to the extent allowed by the technology (or technologies) used. If implemented, such functions shall comply with the principles set out herein. Security options are established to support authenticity and integrity of machine-readable data.

It shall be possible to read mandatory data without restriction (with the exception of basic access protection in the case of a PIC IDL). Optional data may be protected, in which case the protection mechanism (and associated parameters) shall be noted or referenced. The various protection mechanisms are specified in ISO/IEC 18013-3. The optional domestic data may be protected in any manner without restriction.

Changes to machine-readable data elements by the issuing authority are allowed only to data-elements that do not appear in human-readable format on the IDL. Issuing authorities shall uniquely identify each new version (see 8.4) of optional machine-readable data (typically after changing the originally recorded optional data). Issuing authorities shall issue a new IDL when changes to machine-readable data elements will lead to inconsistencies with human-readable data elements on the IDL.

5.3 Mandatory functions

5.3.1 General

Machine-readable data elements included on an IDL shall support/enable the functions described in the following subclauses.

5.3.2 Privilege to drive at time of licensing

Using the IDL to determine (from machine-readable data elements) the driving privileges [and associated restrictions, conditions and validity period(s)] granted to the licence holder by the issuing authority identified on the IDL. It is recognized that this information does not confirm that the issuing authority presently (i.e. at the time when the machine-readable data on an IDL is read by an entity trying to establish a licence holder's driving privileges) considers the licence holder's driving privileges to be valid.

5.3.3 Reference to driving privilege database

Using the machine-readable data elements (such as the licence number) on the IDL to reference records of driving privileges maintained by the issuing authority.

5.3.4 Age verification

Using the machine-readable data elements on the IDL to assure that the licence holder meets various age thresholds for certain products and services, including driving privileges (in the case where the age threshold to drive a particular category of vehicle domestically in the issuing country is lower than the age permitted internationally).

5.4 Optional functions

5.4.1 Identity verification

Using the machine-readable data elements on the IDL to confirm, by way of a visual comparison of the portrait image, that the card holder is the licence holder.

5.4.2 Biographical data verification

Using the machine-readable data elements on the IDL to confirm, by way of visual inspection of the biographical data printed on the portrait side of the card, that such data have not been altered.

5.4.3 Evidence of residence

Ability to use the IDL as evidence that the licence holder resided at a specific location at the time the IDL was issued. It is recognized that this information does not confirm that the issuing authority presently considers the licence holder's residential information to be correct.

5.4.4 Biometric authentication

Ability to use a machine-readable biometric template or templates on the IDL to determine whether the card holder is the licence holder by means of a machine-assisted biometric verification process (i.e. a one-to-one match).

5.4.5 Reciprocity of driving privileges

Ability for a country other than the issuing country to use the machine-readable data elements on the IDL to establish whether a mutual recognition agreement (or agreements) exists with the issuing authority.

5.4.6 Document authentication and validation

Ability to reference items on or qualities about the IDL to verify the document is authentic (i.e. produced by the issuing authority reflected both in the human- and machine-readable data) and that no data has been altered since issuing.

6 Machine-readable technologies supported

Technologies suitable for both compact encoding and standard encoding are supported.

For compact encoding, a typical minimum capacity of 300 usable bytes is required.

Given the minimum data capacity needed to support the mandatory data requirements, the IDL may contain any or a combination of the following machine-readable technologies:

— RFID — Compact encoding, specified in Annex B.

— Two-dimensional bar code — Compact encoding, specified in Annex B.

— IC with contacts — Standard encoding, specified in Annex C (failing which, compact encoding only if limited memory capacity is available for the IDL application, specified in Annex B).