FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
18013-5**

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

Secretariat: BSI

Voting begins on:
2021-06-23

Voting terminates on:
2021-08-18

Personal identification — ISO-compliant driving licence —

Part 5: Mobile driving licence (mDL) application

Identification des personnes — Permis de conduire conforme à l'ISO —
Partie 5: Application permis de conduire sur téléphone mobile

Reference number
ISO/IEC FDIS 18013-5:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 https://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*.

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), ISO machine-readable technologies (ISO/IEC 18013-2), access control, authentication and integrity validation (ISO/IEC 18013-3), and associated test methods (ISO/IEC 18013-4). 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 describes interface and related requirements to facilitate ISO-compliant driving licence (IDL) functionality on a mobile device. The requirements are specifically intended to enable verifiers not affiliated with or associated with the issuing authority to gain access to and authenticate the information. In addition, the requirements allow the holder of the driving licence to decide what information to release to a verifier. Other characteristics include the ability to update information frequently, and to authenticate information at a high level of confidence.

A mobile document conforming to this document primarily conveys the driving privileges associated with a person. It does so by providing means to associate the person presenting the mobile document with the mobile document itself. However, the transaction and security mechanisms in this document have been designed to support other types of mobile documents, specifically including identification documents Consequently the mechanisms in this document can be used for any type of mobile identification document, regardless of the additional attributes the mobile document may convey. The details of the data elements to be used by other mobile documents are left to the respective issuing authority and are not within the scope of this document.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO and IEC that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from the patent database available at www.iso.org/patents.

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

Personal identification — ISO-compliant driving licence —

Part 5:
Mobile driving licence (mDL) application

1 Scope

This document establishes interface specifications for the implementation of a driving licence in association with a mobile device. This document specifies the interface between the mDL and mDL reader and the interface between the mDL reader and the issuing authority infrastructure. This document also enables parties other than the issuing authority (e.g. other issuing authorities, or mDL verifiers in other countries) to:

— use a machine to obtain the mDL data;

— tie the mDL to the mDL holder;

— authenticate the origin of the mDL data;

— verify the integrity of the mDL data.

The following items are out of scope for this document:

— how mDL holder consent to share data is obtained;

— requirements on storage of mDL data and mDL private keys.

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.

BSI TR-03111, *Elliptic Curve Cryptography, Version 2.10, June 2018*

FIPS 186-4:2013, *Digital Signature Standard (DSS)*

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

ISO 3166-2:2020, *Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code*

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

ISO/IEC 7816-4:2020, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

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

ISO/IEC 18004, *Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification*

ISO/IEC 18013-1:2018, *Information technology — Personal identification — ISO-compliant driving licence — Part 1: Physical characteristics and basic data set*

ISO/IEC 18013-2:2020, *Personal identification — ISO-compliant driving licence — Part 2: Machine-readable technologies*

ISO/IEC 19785-3:2020, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

NFC Forum, *Connection Handover (CH) Technical Specification, Version 1.5*

NIST SP 800-38D, *M. Dworkin, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007*

OpenID Foundation *OpenID Connect Core 1.0 incorporating errata set 1*

OpenID Foundation *OpenID Connect Discovery 1.0 incorporating errata set 1*

RFC 4122, *P. Leach et al., A Universally Unique IDentifier (UUID) URN Namespace, July 2005*

RFC 4648, *S Josefsson, The Base16, Base32, and Base64 Data Encodings, October 2006*

RFC 5246, *T. Dierks et al., The Transport Layer Security (TLS) Protocol Version 1.2, August 2008*

RFC 5280, *D. Cooper et al., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008*

RFC 5639, *M. Lochter et al., Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010*

RFC 5869, *H. Krawczyk, HMAC-based Extract-and-Expand Key Derivation Function (HKDF), May 2010*

RFC 6066, *D. Eastlake 3rd, Transport Layer Security (TLS) Extensions: Extension Definitions, January 2011*

RFC 7049, *C. Bormann et al., Concise Binary Object Representation (CBOR), October 2013*

RFC 7515, *J. Bradley et al., JSON Web Signature (JWS), May 2015*

RFC 7518, *M. Jones et al., JSON Web Algorithms (JWA), May 2015*

RFC 7519, *J. Bradley et al., JSON Web Token (JWT), May 2015*

RFC 7748, *A. Langley et al., Elliptic Curves for Security, January 2016*

RFC 7905, *A. Langley et al., ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS), June 2016*

RFC 8032, *S. Josefsson et al., Edwards-Curve Digital Signature Algorithm (EdDSA), January 2017*

RFC 8152, *J. Schaad, CBOR Object Signing and Encryption (COSE), July 2017*

RFC 8252, *W. Denniss et al., Oauth 2.0 for Native Apps, October 2017*

RFC 8259, *T. Bray, The JavaScript Object Notation (JSON) Data Interchange Format, December 2017*

RFC 8410, *S. Josefsson et al., Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure, August 2018*

RFC 8422, *Y. Nir et al., Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier, August 2018*

RFC 8943, *M. Jones et al., Concise Binary Object Representation (CBOR) Tags for Date, November 2020*

RFC, *CBOR Object Signing and Encryption (COSE): Headers for carrying and referencing X.509 certificates*

Wi-Fi Alliance, *Neighbor Awareness Networking Specification, Version 3.1*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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 https://www.electropedia.org/

3.1
mobile device
portable computing device that at least:

— has a small form factor such that it can easily be carried by a single individual;

— is designed to operate, transmit and receive information without a wired connection;

— possesses local, nonremovable or removable data storage;

— includes a self-contained power source;

— includes a display;

— includes a means for the holder of the portable computing device to interact with the device

Note 1 to entry: Adapted from NIST SP 800-157.

3.2
mdoc
document or application that resides on a *mobile device* (3.1) or requires a mobile device as part of the process to gain access to the document or application

3.3
mdoc reader
device that can retrieve *mdoc* (3.2) data for verification purposes

3.4
mdoc holder
individual to whom an *mdoc* (3.2) is issued

3.5
mdoc verifier
person or organization using and/or controlling an *mdoc reader* (3.3) to verify an *mdoc* (3.2)

3.6
mDL
driving licence that fulfils at least the same function as an IDL but, instead of being paper or plastic based, is an *mdoc* (3.2)

Note 1 to entry: ISO-compliant driving licence (IDL) is defined in ISO/IEC 18013-1.

3.7
mDL reader
mdoc reader (3.3) that can retrieve *mDL* (3.6) data

3.8
mDL holder
individual to whom an *mDL* (3.6) is issued, i.e. legitimate holder of the driving privileges reflected on an mDL

3.9
mDL verifier
person or organization using and/or controlling an *mDL reader* (3.7) to verify an *mDL* (3.6)

3.10
licensing authority
authorized agent organisation that issues a driving licence

EXAMPLE National, federal, state, provincial, regional, territorial, or local Ministry of Transport, Department of Motor Vehicles, or Police Agency.

[SOURCE: ISO/IEC 18013-1:2018, 3.15]

3.11
issuing country
country which issued the driving licence or within which the *licensing authority* (3.10) is located

[SOURCE: ISO/IEC 18013-1:2018, 3.12, modified — The words "according to Annex F" have been removed.]

3.12
issuing authority
licensing authority (3.10), or *issuing country* (3.11) if separate licensing authorities have not been authorized

[SOURCE: ISO/IEC 18013-1:2018, 3.11]

3.13
issuing authority infrastructure
infrastructure under control of the *issuing authority* (3.12)

3.14
issuing authority CA
certificate authority operated by or on behalf of an *issuing authority* (3.12)

3.15
device retrieval
method of data retrieval exclusively using the interface between the *mdoc* (3.2) and the *mdoc reader* (3.3)

3.16
server retrieval
method of data retrieval using the interface between the *mdoc reader* (3.3) and the *issuing authority infrastructure* (3.13)

3.17
server retrieval token
token identifying the *mdoc holder* (3.4) and the *mdoc* (3.2) to the *issuing authority* (3.12)

3.18
PCD mode
mode in which an NFC-enabled *mobile device* (3.1) operates as a PCD

[SOURCE: ISO/IEC 14443-3:2018, 3.7, modified — The words "a PXD" have been replaced with "an NFC-enabled mobile device".]

3.19
PICC mode
mode in which an NFC-enabled *mobile device* (3.1) operates as a PICC

[SOURCE: ISO/IEC 14443-3:2018, 3.8, modified — The words "a PXD" have been replaced with "an NFC-enabled mobile device".]

4 Abbreviated terms

AES	advanced encryption standard
APDU	application protocol data unit
BLE	Bluetooth® low energy
BT SIG	Bluetooth special interest group
CA	certificate authority
CBOR	concise binary object representation
CDDL	concise data definition language
COSE	CBOR object signing and encryption
CSPRNG	cryptographically secure pseudo-random number generator
CRL	certificate revocation list
DER	distinguished encoding rules
DS	document signer
ECDH	elliptic curve Diffie-Hellman key agreement
ECDSA	elliptic curve digital signature algorithm
EdDSA	Edwards-curve digital signature algorithm
GATT	generic attribute profile
HKDF	HMAC-based extract-and-expand key derivation function
HMAC	hash-based MAC
IA	issuing authority
IACA	issuing authority certificate authority
IANA	internet assigned number authority
IDL	ISO-compliant driving licence
IKM	input keying material
JSON	JavaScript object notation
JWK	JSON web key
JWS	JSON web signature
JWT	JSON web token
KDF	key derivation function
MAC	message authentication code
MITM	man-in-the-middle attack

MSO	mobile security object
MTU	maximum transmission unit
NDEF	NFC data exchange format
NFC	near field communication
OCSP	online certificate status protocol
OID	object identifier
OIDC	OpenID connect
PCD	proximity coupling device
PICC	proximity card or object
PKI	public key infrastructure
RF	radiofrequency
RFU	reserved for future use
SHA	secure hash algorithm
TLS	transport layer security
URI	uniform resource identifier
URL	uniform resource locator
UTC	coordinated universal time
UUID	universally unique identifier
VICAL	verified issuer certificate authority list

5 Conformance requirement

An mDL is in conformance with this document if it meets all the requirements specified directly or by reference herein. Conformance with ISO/IEC 18013-1, ISO/IEC 18013-2, ISO/IEC 18013-3, and ISO/IEC 18013-4 is not required for conformance with this document, except for those clauses normatively referenced in this document.

An mDL reader is in conformance with this document if it meets all the requirements specified directly or referenced herein.

An issuing authority infrastructure is in conformance with this document if it meets all the requirements specified directly or referenced herein.

6 mDL overview

6.1 Interfaces

Figure 1 shows the interfaces in scope for this document. The explanation of each interface is as follows.

— Interface 1 in Figure 1 is the interface between the issuing authority infrastructure and the mDL. This interface is out of scope for this document.

— Interface 2 in Figure 1 is the interface between the mDL and the mDL reader. This interface is specified in this document. The interface can be used for connection setup and for the device retrieval method.

— Interface 3 in Figure 1 is the interface between the issuing authority infrastructure and the mDL reader. This interface is specified in this document. The interface can be used for the server retrieval method.

See Reference [9] for examples of use cases.

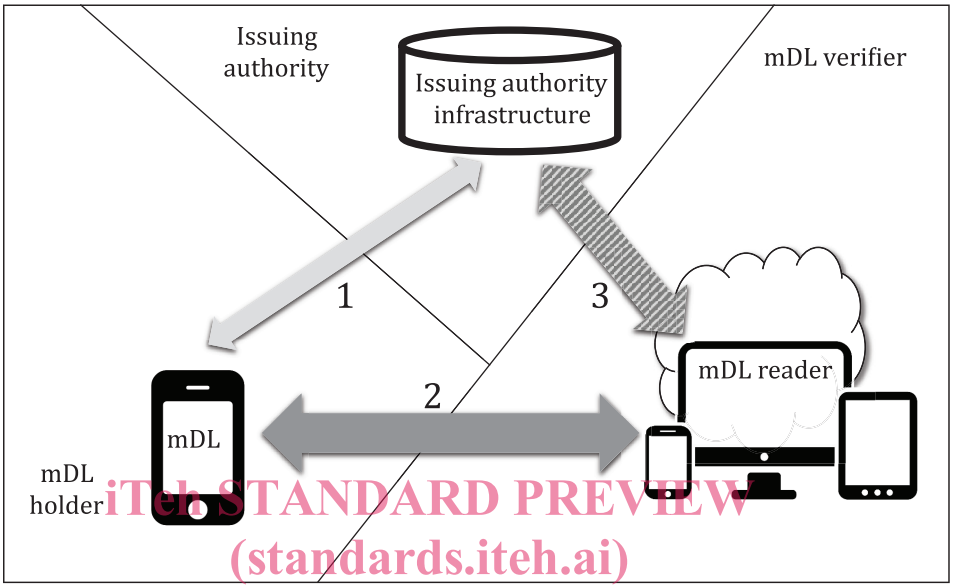

Figure 1 — mDL interfaces

6.2 Functional requirements

The functional requirements include at least the following.

a) An mDL verifier together with an mDL reader shall be able to request, receive and verify the integrity and authenticity of an mDL whether online connectivity is present or not for either the mDL or mDL reader.

b) An mDL verifier not associated with the issuing authority shall be able to verify the integrity and authenticity of an mDL.

c) An mDL verifier shall be enabled to confirm the binding between the person presenting the mDL and the mDL holder.

d) The interface between the mDL and the mDL reader shall support the selective release of mDL data to an mDL reader.

6.3 Technical requirements

6.3.1 Data model

The mDL data is organized as individual data elements which can be requested and returned independently from each other. The mDL data model is described in Clause 7. It describes the identifier and format of the data elements.

NOTE The concepts used in this document have been designed so that other mobile credentials, e.g. mobile identity or other credentials that substitute Table 5 with a different set of data elements, can also make use of the engagement and retrieval protocols described in this document. Specifically, the mdoc data model, which is illustrated in Figure 2, is based on elements with unique identifiers within a namespace. The number of elements can vary, and the model is indifferent to the value and data format of each element. As such the data model is generic and can apply to any kind of document.

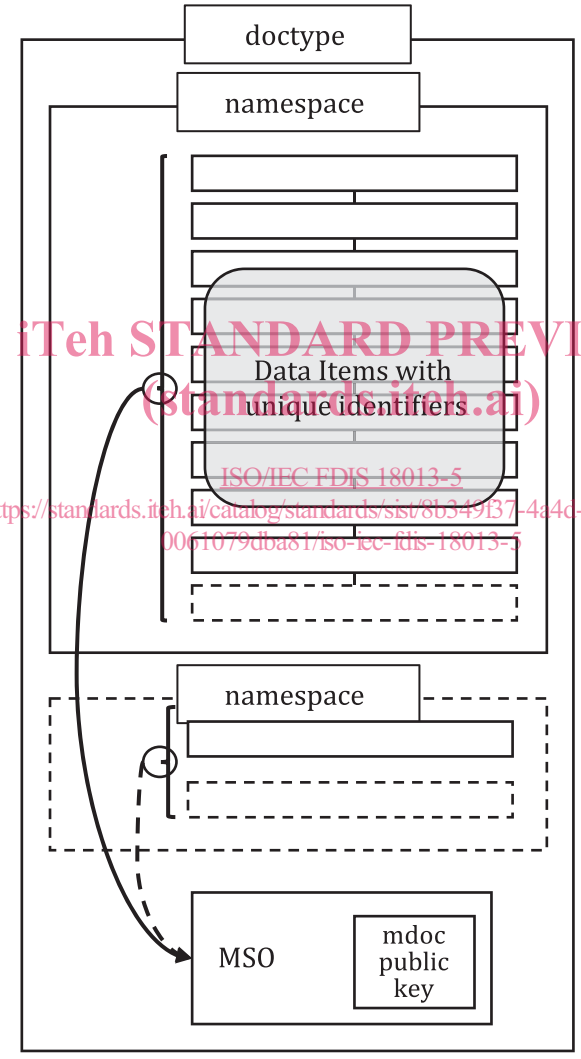

Figure 2 — mdoc data model

6.3.2 Data exchange

6.3.2.1 Overview

The mDL and mDL reader are implemented as an mdoc and mdoc reader, for which the requirements are described in Clause 8 and Clause 9.

Data exchange is divided into three phases: the initialization phase, the device engagement phase, and the data retrieval phase (as illustrated in Figure 3). After initialization between the mDL and the mDL reader three different transaction flows are distinguished:

— device engagement, followed by exchange of data using device retrieval between the mDL and the mDL reader [see (1) in Figure 3];

— device engagement, followed by exchange of server retrieval information using device retrieval between the mDL and the mDL reader, followed by exchange of data using server retrieval between the mDL reader and the issuing authority infrastructure [see (2) in Figure 3];

— device engagement, followed by exchange of data using server retrieval between the mDL reader and the issuing authority infrastructure [see (3) in Figure 3].

NOTE 1 For device retrieval, there is no requirement for any device involved in the transaction to be connected to the internet.

If the mDL reader receives the server retrieval token and URL from the mDL, either during device engagement or device retrieval, it may either use device retrieval or server retrieval. If it chooses to use device retrieval, either BLE, NFC or Wi-Fi Aware can be used to retrieve the information. If it chooses to use server retrieval, either OIDC or WebAPI can be used to retrieve the information.

NOTE 2 The transaction has been designed such that it is not necessary for the mDL holder to physically hand over the mobile device to the mDL verifier.

NOTE 3 The transaction protocols in this document provide generic means for a user to share connection information and optionally a server retrieval token.

The device data retrieval transport applies to any kind of data as it is designed to transport an encrypted blob.

The request and response commands (transported encrypted) are applicable to any kinds of document based on the mdoc data model and/or request for server retrieval token. Furthermore, the request and response commands are wallet compliant as elements from different documents can be requested and the response can include multiple documents from the same or different kinds.

The server retrieval method relies on OpenID Connect that is not specific to mDL, or on WebAPI that relies on the generic mdoc data model.

