DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 18013-5

ISO/IEC JTC **1**/SC **17** Secretariat: **BSI**

Voting begins on:
2020-02-05

Voting terminates on:
2020-04-29

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

ICS: 35.240.15

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 18013-5:2020(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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 17 Cards and security devices for personal identification.

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

— *Part 1: Physical characteristics and basic data set.* Part 1 describes the basic terms for this document including physical characteristics, basic data element set, visual layout, and physical security features;

— *Part 2: Machine-readable technologies.* Part 2 describes the technologies that may be used for this document, including the logical data structure and data mapping for each technology;

— *Part 3: Access control, authentication and integrity validation.* Part 3 describes the electronic security features that may be incorporated under this document, including mechanisms for controlling access to data, verifying the origin of an IDL, and confirming data integrity;

— *Part 4: Test methods.* Part 4 describes the test methods that can be used to determine if an IDL conforms to the requirements for machine readable technologies specified in Part 2 and to the electronic security features specified in Part 3.

— *Part 5: Mobile Driving Licence (mDL) application.* Part 5 describes interface specifications for the implementation of a driving licence in association with a mobile device.

Introduction

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 major advantages include the ability to update information frequently, and to authenticate information at a high level of confidence.

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), 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.

The purpose of an IDL with one or more machine-readable technologies storing IDL data is to

— increase productivity (of data and IDL use),

— facilitate IDL data exchange, and

— assist in authenticity and integrity validation.

— Provide strong security and privacy features

Personal identification — ISO-compliant driving licence —

Part 5:
Mobile driving licence (mDL) application

1 Scope

The purpose of this document is to standardize interface specifications for the implementation of a driving licence in association with a mobile device (mDL). This document standardizes the interface between the mDL and mDL Reader, and the interface between the mDL Reader and the issuing authority infrastructure. The standard also allow parties other than the issuing authority (e.g. other issuing authorities, or mDL Verifiers in other countries) to:

a) use a machine to obtain the mDL data,

b) tie the mDL to the mDL Holder,

c) authenticate the origin of the mDL data, and

d) verify the integrity of the mDL data.

The following items are out of scope for this document:

a) how user consent to share data is obtained

b) requirements on storage of mDL data and mdL private keys

2 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.

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

CA/Browser Forum *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*

draft-iets-cose-x509-04: *CBOR Object Signing and Encryption (COSE): Headers for carrying and referencing X.509 certificates*

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

FIPS PUB 140-2, *Security requirements for cryptographic modules, May 2001*

ICAO Doc 9303-12, *Machine Readable Travel Documents, Part 12: Public Key Infrastructure for MRTDs, Seventh Edition,* 2015

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

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

ISO/IEC 7812:2017, *Identification cards -- Identification of issuers -- Part 1: Numbering system*

ISO/IEC 7816-3:2006, *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols*

ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 10113-2:2004, *Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions*

ISO/IEC 14443-2:2016, *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface*

ISO/IEC 14443-3:2016, *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision*

ISO/IEC 14443-4:2018, *Cards and security devices for personal identification -- Contactless proximity objects -- Part 4: Transmission protocol*

ISO/IEC 14443-3:2018, *Cards and security devices for personal identification -- Contactless proximity objects -- Part 3: Initialization and anticollision*

ISO/IEC 15408:2009, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*

ISO/IEC 18004:2015, *Information technology – Automatic identification and data capture techniques – QR Code 2005 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 18013-2:2008, *Information technology -- 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*

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

ISO/IEC 19790:2012, *Information technology -- Security techniques -- Security requirements for cryptographic modules*

NFC Forum, *Bluetooth Secure Simple Pairing Using NFC, NFCForum-AD-BTSSP_1_2, May* 2019

NFC Forum, *Connection Handover, Version 1.5,* 2019

NFC Forum, *Technical Specification - NFC Data Exchange Format (NDEF)*

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

NIST SP 800-157, *H. Ferraiolo et al., Guidelines for Derived Personal Identity Verification (PIV) Credentials, December 2014*

OpenID Connect Core 1.0, *N. Sakimura et. al., Defines the core OpenID Connect functionality: authentication built on top of OAuth 2.0 and the use of claims to communicate information about the End-User, November* 2014

OpenID Connect Discovery *N. Sakimura et. al., Defines how clients/readers dynamically discover information about OpenID Providers, November* 2014

OpenID Connect Dynamic Registration *N. Sakimura et. al., Defines how clients/readers dynamically register with OpenID Providers, November* 2014

RFC 2104, *H. Krawczyk et al., HMAC: Keyed-Hashing for Message Authentication, February 2017*

RFC 2616, *R. Fielding et al., Hypertext Transfer Protocol -- HTTP/1.1, June 1999*

RFC 3339, *G. Klyne et al., Date and Time on the Internet: Timestamps, July 2002*

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

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 5652, *R. Housley, Cryptographic Message Syntax (CMS), September 2009*

RFC 5754, *S. Turner, Using SHA2 Algorithms with Cryptographic Message Syntax, January 2009*

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

RFC 6960, *S. Santesson et al., X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013*

RFC 7049, *C. Bormann et al., Concise Binary Object Representation (CBOR), Oct 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, Jan 2016*

RFC 7905, *A. Langley et al., ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS), Jun 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 8259, *T. Bray, The JavaScript Object Notation (JSON) Data Interchange Format, December 2017*

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

RFC 8446, *E. Rescorla et al., The Transport Layer Security (TLS) Protocol Version 1.3, August 2018*

RFC 8610, *H. Birkholz et al., Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures, June 2019*

SP 800-56A Rev. 3, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*

Wi-Fi Alliance *Neighbor Awareness Networking Technical Specification, Version 3.0, December* 2018

Wi-Fi Alliance *Neighbor Awareness Networking Specification v3.0 draft Addendum version 0.0.2., April* 2019

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
mobile device
portable computing device that at least:

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

(ii) is designed to operate, transmit and receive information without a wired connection;

(iii) possesses local, nonremovable or removable data storage; and

(iv) includes a self-contained power source

(v) includes a display; and

(vi) includes a mean for the user to interact with a device

[SOURCE: NIST SP 800-157, modified]

3.2
mDL
driving licence that fulfils at least the same function as an IDL (ISO/IEC 18013-1) but, instead of being paper or plastic based, resides on a mobile device or requires a mobile device as part of the process to gain access to the driving licence

3.3
mDL Holder
legitimate holder of the driving privileges reflected on an mDL

3.4
mDL Reader
device that can retrieve mDL data for verification purposes

3.5
mDL Verifier
a person or organization using and/or controlling an mDL Reader to verify an mDL

3.6
issuing authority infrastructure
infrastructure under control of the issuing authority

4 Abbreviated terms

APDU	Application Protocol Data Unit
BER	Basic Encoding Rules
BLE	Bluetooth Low Energy
BT SIG	Bluetooth 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
DO	Data Object
DS	Document Signer
ECDH	Elliptic Curve Diffie-Hellman
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
IA	Issuing Authority
IACA	Issuing Authority Certificate Authority
IAPC	Issuing Authority Point of Contact
IDL	ISO-compliant driving licence
IKM	Input Keying Material
JWT	JSON Web Token
JWS	JSON Web Signature
JWA	JSON Web Algorithms
KDF	Key Derivation Function
MAC	Message Authentication Code
MITM	Man-in-the-middle attack
ML	Master List
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
PIX	Proprietary Application Identifier Extension
PKI	Public Key Infrastructure
RID	Registered Application Provider Identifier
TLS	Transport Layer Security

TLV	Tag Length Value
UHF	Ultra High Frequency
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
UUID	Universally unique identifer

5 Conformance requirement

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

An mDL Reader is in conformance with this document if it meets all mandatory requirements specified directly or by reference herein.

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

6 mDL overview

6.1 Introduction

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

1) This is the interface between the issuing authority infrastructure and the mDL. This interface is out of scope for this document.

2) This 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 offline data retrieval.

3) This 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 online data retrieval method.

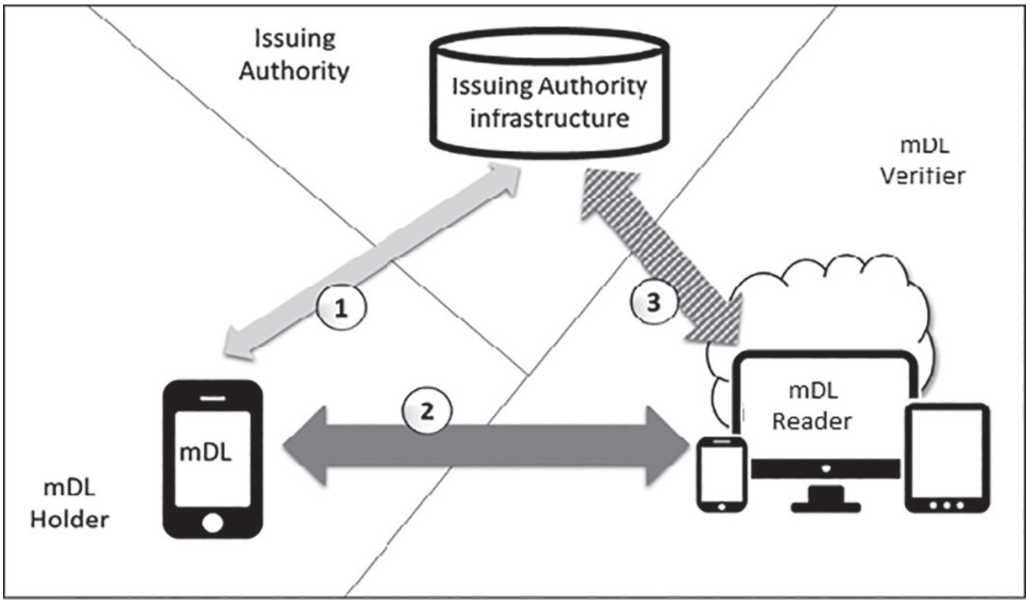

Figure 1 — mDL interfaces

See Annex A for examples of use cases.

6.2 Functional requirements

The specific functional requirements covered in this part of ISO/IEC 18013 for the mDL include at least:

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 on either the mDL or mDL Reader.

b) Verifiers 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.

The interface between the issuing authority and the mDL shall support the ability to update information. The mechanism of this ability is out of scope for this document.

6.3 Technical requirements

6.3.1 Data model

The mDL data model is described in 7.

6.3.2 Data exchange

6.3.2.1 Overview

Data exchange is divided into three phases: initialization phase, device engagement phase and data retrieval phase (see 8 and Figure 2). After initialization between the mDL and the mDL Reader three main transaction flows are distinguished:

— Device engagement, followed by exchange of data by offline retrieval between the mDL and the mDL Reader (see (1) in Figure 2)

— Device engagement, followed by exchange of online token using offline retrieval between the mDL and the mDL Reader, followed by exchange of data by online retrieval between the mDL Reader and the issuing authority. (see (2) in Figure 2)

— Device engagement, followed by exchange of data by online retrieval between the mDL Reader and the issuing authority infrastructure. (see (3) in Figure 2)

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

NOTE The transaction has been designed such that it is not be necessary for the mDL Holder to physically hand over the mobile device to the mDL Verifier.

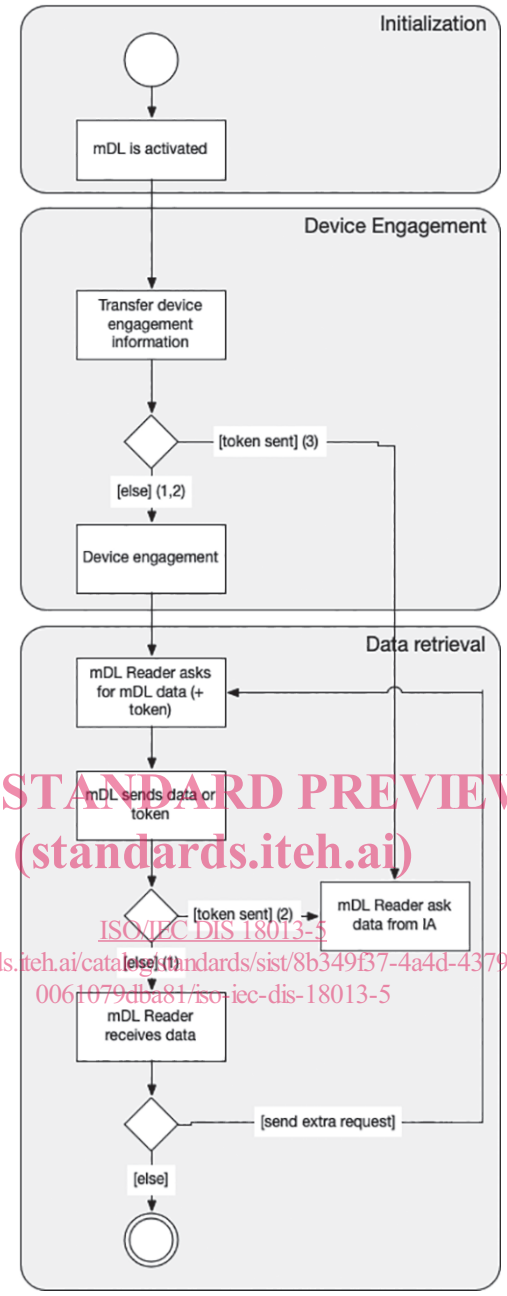

Figure 2 — mDL transaction flow

6.3.2.2 Initialization

During initialization, an mDL is activated (by the mDL Holder, or potentially triggered by NFC). No requirements are specified for this phase

6.3.2.3 Device engagement

During device engagement, information required to setup and secure data retrieval is exchanged between the mDL to the mDL Reader. Transmission technologies available to transfer the device engagement data are as follows:

a) NFC (Type 4 tag Platform using NDEF, see NFC Forum, *Technical Specification - NFC Data Exchange Format (NDEF)*)