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
Contents

Foreword ........................................................................................................................................................................... vi
Introduction .......................................................................................................................................................................... vii

1 Scope ............................................................................................................................................................................... 1
2 Normative references ....................................................................................................................................................... 1
3 Terms and definitions ....................................................................................................................................................... 3
4 Abbreviated terms ............................................................................................................................................................. 4
5 Conformance requirement .................................................................................................................................................. 6
6 mDL overview ................................................................................................................................................................. 6
   6.1 Introduction ................................................................................................................................................................... 6
   6.2 Functional requirements ............................................................................................................................................. 7
   6.3 Technical requirements ............................................................................................................................................... 7
       6.3.1 Data model .......................................................................................................................................................... 7
       6.3.2 Data exchange ...................................................................................................................................................... 8
       6.3.3 Security mechanisms ........................................................................................................................................ 12
7 Data model ....................................................................................................................................................................... 12
   7.1 Overview .................................................................................................................................................................... 12
   7.2 Encoding of data structure and data elements ..................................................................................................... 12
       7.2.1 nSpace and DocType ......................................................................................................................................... 12
       7.2.2 General ............................................................................................................................................................... 12
       7.2.3 DocType ............................................................................................................................................................. 12
       7.2.4 nSpace ............................................................................................................................................................... 13
   7.3 mDL data ................................................................................................................................................................... 13
       7.3.1 Overview ............................................................................................................................................................ 13
       7.3.2 Portrait of mDL Holder ..................................................................................................................................... 13
       7.3.3 Issuing authority .................................................................................................................................................. 16
       7.3.4 Categories of vehicles/restrictions/conditions ............................................................................................... 16
       7.3.5 Age attestation: Nearest "true" attestation above request .............................................................................. 16
       7.3.6 Biometric template ............................................................................................................................................ 17
       7.3.7 Signature or usual mark ...................................................................................................................................... 17
       7.3.8 Online token ....................................................................................................................................................... 17
       7.3.9 Domestic data elements .................................................................................................................................. 17
   7.4 Country codes ........................................................................................................................................................... 17

8 Transaction ..................................................................................................................................................................... 18
   8.1 Device engagement ..................................................................................................................................................... 18
       8.1.1 Device engagement information ....................................................................................................................... 18
       8.1.2 Device engagement transmission technology ................................................................................................. 20
   8.2 Data retrieval ............................................................................................................................................................. 22
       8.2.1 Data retrieval methods ...................................................................................................................................... 22
       8.2.2 Data retrieval transmission technologies ...................................................................................................... 28
9 Security mechanisms ......................................................................................................................................................... 36
   9.1 Overview .................................................................................................................................................................... 36
   9.2 Offline retrieval .......................................................................................................................................................... 38
       9.2.1 Session encryption .............................................................................................................................................. 38
       9.2.2 Issuer data authentication ................................................................................................................................... 40
       9.2.3 mDL authentication ........................................................................................................................................... 43
       9.2.4 mDL Reader authentication ............................................................................................................................... 45
   9.3 Online retrieval ............................................................................................................................................................ 46
       9.3.1 TLS ...................................................................................................................................................................... 46
       9.3.2 JWS .................................................................................................................................................................... 47

Annex A (informative) Mobile driving licence use cases .................................................................................................. 48
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-heits-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
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 DIS 18013-5:2020(E)


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
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

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APDU</td>
<td>Application Protocol Data Unit</td>
</tr>
<tr>
<td>BER</td>
<td>Basic Encoding Rules</td>
</tr>
<tr>
<td>BLE</td>
<td>Bluetooth Low Energy</td>
</tr>
<tr>
<td>BT SIG</td>
<td>Bluetooth Interest Group</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CBOR</td>
<td>Concise Binary Object Representation</td>
</tr>
<tr>
<td>CDDL</td>
<td>Concise data definition language</td>
</tr>
<tr>
<td>COSE</td>
<td>CBOR Object Signing and Encryption</td>
</tr>
<tr>
<td>CSPRNG</td>
<td>Cryptographically Secure Pseudo-random Number Generator</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>DER</td>
<td>Distinguished Encoding Rules</td>
</tr>
<tr>
<td>DO</td>
<td>Data Object</td>
</tr>
<tr>
<td>DS</td>
<td>Document Signer</td>
</tr>
<tr>
<td>ECDH</td>
<td>Elliptic Curve Diffie-Hellman</td>
</tr>
<tr>
<td>ECDSA</td>
<td>Elliptic Curve Digital Signature Algorithm</td>
</tr>
<tr>
<td>EdDSA</td>
<td>Edwards-curve Digital Signature Algorithm</td>
</tr>
<tr>
<td>GATT</td>
<td>Generic Attribute Profile</td>
</tr>
<tr>
<td>HKDF</td>
<td>HMAC-based Extract-and-Expand Key Derivation Function</td>
</tr>
<tr>
<td>IA</td>
<td>Issuing Authority</td>
</tr>
<tr>
<td>IAACA</td>
<td>Issuing Authority Certificate Authority</td>
</tr>
<tr>
<td>IAPC</td>
<td>Issuing Authority Point of Contact</td>
</tr>
<tr>
<td>IDL</td>
<td>ISO-compliant driving licence</td>
</tr>
<tr>
<td>IKM</td>
<td>Input Keying Material</td>
</tr>
<tr>
<td>JWT</td>
<td>JSON Web Token</td>
</tr>
<tr>
<td>JWS</td>
<td>JSON Web Signature</td>
</tr>
<tr>
<td>JWA</td>
<td>JSON Web Algorithms</td>
</tr>
<tr>
<td>KDF</td>
<td>Key Derivation Function</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>MITM</td>
<td>Man-in-the-middle attack</td>
</tr>
<tr>
<td>ML</td>
<td>Master List</td>
</tr>
<tr>
<td>MSO</td>
<td>Mobile Security Object</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
</tr>
<tr>
<td>NDEF</td>
<td>NFC Data Exchange Format</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>OCSP</td>
<td>Online Certificate Status Protocol</td>
</tr>
<tr>
<td>OID</td>
<td>Object Identifier</td>
</tr>
<tr>
<td>OIDC</td>
<td>OpenID Connect</td>
</tr>
<tr>
<td>PIX</td>
<td>Proprietary Application Identifier Extension</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>RID</td>
<td>Registered Application Provider Identifier</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
</tbody>
</table>
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.
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.
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)*)