FINAL DRAFT
Technical Specification

ISO/IEC DTS 18013-7

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

Secretariat: **BSI**

Voting begins on:
2024-06-04

Voting terminates on:
2024-07-30

Personal identification — ISO-compliant driving licence —

Part 7: Mobile driving licence (mDL) add-on functions

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

Partie 7: Fonctionnalités supplémentaires pour permis de conduire sur téléphone mobile

Reference number
ISO/IEC DTS 18013-7:2024(en)

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 ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **1**
5 Conformance requirement **2**
6 mDL overview **2**
6.1 Standards context 2
6.2 Interfaces 2
6.3 Design objectives 3
6.4 Technical requirements 3
6.4.1 Data structures and data elements 3
6.4.2 Data model 3
6.4.3 Data exchange 3
6.4.4 Security mechanisms 5
6.5 Protocol considerations 6
6.5.1 General 6
6.5.2 Discovery and invocation of mdoc using a custom URI scheme 7
6.5.3 Possible attack 7
6.5.4 Additional flows and methods 7
7 mDL data model **7**
Annex A (normative) **Mechanisms for device retrieval to a website** **9**
Annex B (normative) **Use of OID4VP to retrieve an mdoc** **15**
Bibliography **40**

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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*.

A list of all parts in the ISO 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 and www.iec.ch/national-ommittees.

Introduction

ISO/IEC 18013-5 describes interface and related requirements to facilitate ISO-compliant driving licence functionality on a mobile device, standardizing the mobile driving licence (mDL) functionality.

This document augments the capabilities of the mDL by describing the interface and related requirements for presentation to a mDL reader over the internet.

A mobile document conforming to this document primarily conveys the driving privileges associated with a person. However, the transaction and security mechanism in this document have been designed to support other types of mobile documents, specifically including identification documents.

NOTE ISO/IEC 18013-5 places the onus on the mDL verifier to match data received (in an mdoc) to the person presenting the mdoc. This version of this document does not change this. It is planned for the next version of this document to include (and/or reference) means to alleviate the mDL verifier of this responsibility.

Personal identification — ISO-compliant driving licence —

Part 7:
Mobile driving licence (mDL) add-on functions

1 Scope

This document augments the capabilities of the mobile driving licence (mDL) standardized in ISO/IEC 18013-5 with the following additional functionality:

— presentation of a mobile driving licence to a reader over the internet.

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/IEC 18013-5, *Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application*

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

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

RFC 9101, *N. Sakimura, The OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR), August 2021*

RFC 9112, *R. Fielding et al., HTTP/1.1, June 2022*

OID4VP (OpenID for Verifiable Presentations) — draft 18, *O. Terbu et al., April 2023*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 18013-5 and the following apply.

ISO and IEC maintain terminology 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
mdoc reader
either device or service, or both, that can retrieve data from an mdoc and verify the authenticity of the data

Note 1 to entry: The mdoc reader includes, but is not limited to, the hardware and software components used.

4 Abbreviated terms

OID4VP OpenID for Verifiable Presentations

5 Conformance requirement

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

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

NOTE Conformance of an mDL or an mDL reader with ISO/IEC 18013-5 is not required for conformance with this document, except for those clauses normatively referenced in this document. An mDL or an mDL reader conforming with this document can also be in conformity with ISO/IEC 18013-5.

6 mDL overview

6.1 Standards context

ISO/IEC 18013-5 describes the interface and related requirements to specifically facilitate ISO-compliant driving licence functionality on a mobile device. This document adds functionality by building on top of ISO/IEC 18013-5.

The transaction and security mechanisms in this document have been designed to also be applicable to other types of mobile documents besides the mobile driving licence.

6.2 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 (IA) 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 IA infrastructure and the mDL reader. This interface is defined in ISO/IEC 18013-5. No new requirements are added in this document.

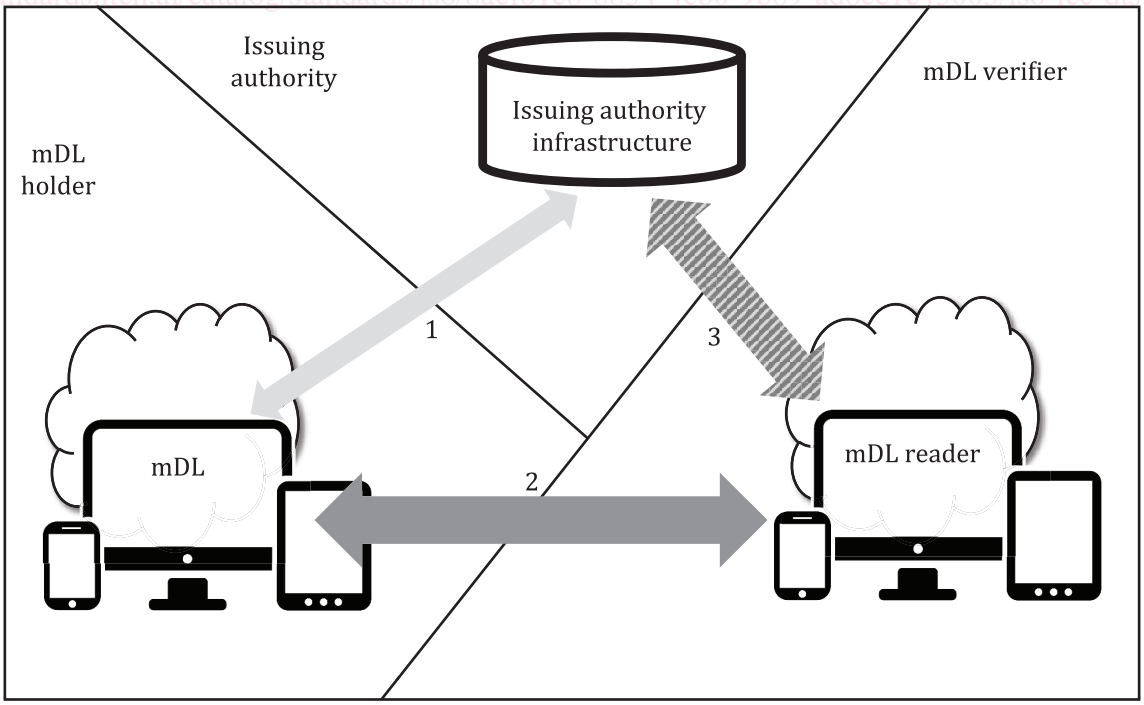

Figure 1 — mDL interfaces

6.3 Design objectives

The objectives underlying the requirements in this document include at least the following:

a) An mDL verifier together with an mDL reader is able to request and receive and mDL, and validate its integrity and authenticity.

b) An mDL verifier not associated with the IA is able to verify the integrity and authenticity of an mDL.

c) An mDL verifier is 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 supports the selective release of mDL data to an mDL reader.

NOTE As in ISO 18013-5, the portrait image can be used for verifying that the person presenting the mDL is the mDL holder. Depending on the transaction details, in an unattended transaction this data element might not be able to serve the purpose of confirming that the person presenting the mDL is the mDL holder. Other methods can be used as well, but are out of scope of this document. Other mechanisms are described in References [1] and[2]. A future version of this document might add additional mechanisms for verifying that the person presenting the mDL is the mDL holder.

6.4 Technical requirements

6.4.1 Data structures and data elements

The descriptions and requirements for Concise Binary Object Representation (CBOR), Concise Data Definition Language (CDDL), and version elements in ISO/IEC 18013-5 shall apply in this document.

Additionally, unless explicitly stated otherwise for a data structure, an mdoc or mdoc reader shall not give an error purely on the basis that it does not know the element. This requirement also applies when the CDDL definition of the data structure does not allow the presence of additional key-value pairs in the map, next to the specified ones.

6.4.2 Data model

The data model is described in Clause 7. It describes the identifier and format of the data elements.

6.4.3 Data exchange

6.4.3.1 Overview

An mDL or mDL reader shall support at least one of the flows and may support more.

a) Using the device retrieval messages structures and transmission channel as defined in 6.4.3.3 that is setup:

   1) using remote engagement, as defined in 6.4.3.2, or

   2) using an out-of-band mechanism, as defined in 6.4.3.2.

b) Using OID4VP as a transmission channel, as defined in Annex B.

The different flows are depicted in Figure 2.

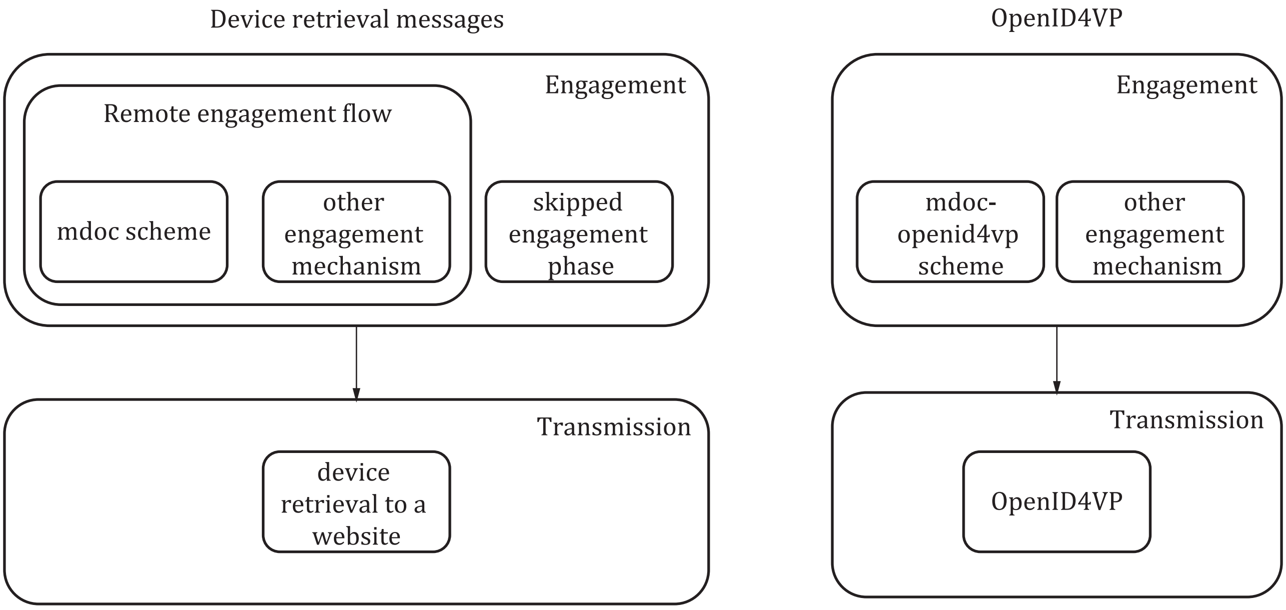

Figure 2 — Flows for unattended cases

An mDL and mDL reader shall support at least one of the following data retrieval methods and may support more. Table 1 shows the requirements.

— device retrieval as defined in 6.4.3.3;

— OID4VP as defined in Annex B.

Table 1 — Data retrieval methods

Data retrieval method	Support		Reference in this document
	mDL	mDL reader	
Device retrieval	C[a]	C[a]	6.4.3.3
OID4VP	C[a]	C[a]	Annex B

Key

C conditional

[a] Support for at least one of these methods is mandatory.

6.4.3.2 Device retrieval engagement phase

The engagement mechanism for remote engagement can be used to exchange the information required to set up a secure data retrieval mechanism between the mDL and mDL reader. When performing remote engagement, the following flow shall be used:

a) The mDL reader transmits the ReaderEngagement structure to the mDL.

b) The mDL sets up a data transmission channel with the mDL reader using the information from the ReaderEngagement structure.

c) The mDL sends a DeviceEngagement structure to the mDL reader using the newly setup data transmission channel.

The ReaderEngagement and DeviceEngagement structures are defined in A.1 and A.2. A possible mechanism for transmission of the ReaderEngagement structure is defined in A.4. Support for this transmission mechanism is recommended for the mDL and mDL reader, since this is the only mechanism currently provided in this document. However, other mechanisms for transmitting the ReaderEngagement structure, which are not defined in this document, can be used.

When the mDL and mDL reader have an existing two-way data transmission channel that is set up out-of-band for exchange of data, the device retrieval engagement phase can be skipped.

6.4.3.3 Device retrieval data retrieval phase

The general data retrieval architecture is described in ISO/IEC 18013-5. If an mDL or mDL reader supports the device retrieval data retrieval phase, they shall use the mdoc request and mdoc response structures as specified in ISO/IEC 18013-5.

A.6.2 defines a transmission technology for device retrieval that may be supported by an mDL or an mDL reader.

NOTE ISO/IEC 18013-5 defines the server retrieval data retrieval method. This document does not specify any additional requirements for server retrieval.

6.4.4 Security mechanisms

6.4.4.1 Security architecture

The security of mDL data exchanged with an mDL reader is designed to preserve the triad of confidentiality, integrity, and authenticity by design and by default.

The security architecture aims to achieve the following goals:

a) Protection against forgery: Data elements are signed by the IA. The degree of protection against forgery depends on the degree to which the IA's keys are protected. Minimizing the validity period of the data limits the value of the data.

b) Protection against cloning: The mDL produces a signature or message authentication code over session data. The private key used to authenticate the session data is stored only in the mDL. The corresponding public key in turn is signed by the IA. The degree of protection against cloning depends on the degree to which the mDL authentication key is protected. In addition to protecting DeviceKey by secure storage, an mdoc/mDL may require the user to be authenticated before this key is usable. This depends on the jurisdiction/issuer's policy (e.g. AAL as per eIDAS Regulation, NIST SP 800-63, ISO/IEC 29115).

c) Protection against eavesdropping: Communications between mDL and mDL readers are encrypted and authenticated. The mDL reader can detect man-in-the-middle (MITM) attacks by validating the anti-cloning signature or message authentication code, which is created using a key for which the public part is signed by the IA in the mobile security object (MSO), see ISO/IEC 18013-5. If mdoc reader authentication is used, the mDL can detect MITM attacks before returning any data.

d) Protection against unauthorized access: An mDL is protected from unauthorized access by an mDL reader by multiple mechanisms. When session encryption is used, the encryption key used for communications between the mDL and mDL reader is derived from an ephemeral key pair from both the mDL and mDL reader. The mDL can optionally authenticate the mDL reader by means of an mDL reader authentication certificate and a signature created by the mDL reader using the corresponding private key. The mDL reader certificate is signed by a certificate authority trusted by the mDL for this purpose.

e) Protection of the mDL holder against relayed engagement information: the mDL includes in the device engagement data, the origin information of the engagement channel or the data transmission channel for the mDL reader to confirm it. The origin is determined by the mDL independently from the information transmitted in the reader engagement structure. The transaction is cancelled by the mDL reader when the origin is different from the expected value.

Revocation of an mDL is out of scope for this document. However, the MSO includes update information and validity time frames which enable the mDL reader to check the freshness of the data. The IA shall define appropriate periods of validity that balance freshness with offline capability, considering that a shorter validity period mitigates certain security risks.

6.4.4.2 Security mechanisms support requirements

Table 2 describes the security mechanisms that can be implemented by an mDL or an mDL reader. Issuer data authentication, and mdoc authentication shall be implemented by the mDL and mDL reader. Session encryption shall be implemented if the device retrieval to a website mechanism, specified in A.6 is used. mdoc reader authentication is optional for the mDL and mDL reader.

mdoc authentication, mdoc reader authentication and session encryption shall use the session transcript as defined in A.8

A.5 contains further requirements on the use of mdoc mac authentication.

NOTE 1 ISO/IEC 18013-5 describes the use of the X.509 certificates when using mdoc reader authentication. Other mechanisms for providing the mDL reader public key and trust information can also be used.

The certificate and CRL profile requirements in ISO/IEC 18013-5 shall be applied for the following profiles: IACA root certificate, IACA link certificate, document signer certificate, mdoc reader authentication certificate, Online Certificate Status Protocol (OCSP) signer certificate, CRL profile.

NOTE 2 ISO/IEC 18013-5 defines that OCSP can be used for document signer certificate and that use of the mdoc reader authentication certificate profile is a recommendation, not a requirement.

All certificates issued by an IACA or another CA shall be validated according to ISO/IEC 18013-5.

An mDL reader needs access to the issuing authority's certificate authority (IACA) root certificate to verify issuer data authentication. An optional method to get access to these certificates is described in ISO/IEC 18013-5 using a verified issuer certificate authority list (VICAL) provider.

See the privacy and security recommendations in ISO/IEC 18013-5 for additional information on privacy and security.

Table 2 — Security mechanisms

Security mechanisms	Support	Reference
Session encryption	Conditional (see 6.4.3)	A.6
Issuer data authentication	Mandatory	ISO/IEC 18013-5
mdoc authentication	Mandatory	ISO/IEC 18013-5
mdoc reader authentication	Optional	ISO/IEC 18013-5

6.4.4.3 Additional verification requirements

If the OriginInfo as defined in A.3 contains the domain origin field, the mDL reader shall verify whether it matches the domain of where the mDL was requested.

The behaviour of the mDL reader when it receives the domain origin field with an empty string is out of scope of this document.

The mDL reader shall also verify any other elements in the OriginInfo that it understands and for which it can obtain the info to verify it. If the verification fails, the mDL reader shall terminate the transaction and invalidate any received data.

6.5 Protocol considerations

6.5.1 General

This clause reflects security and privacy considerations that implementers of flows and methods described in this document can consider.