

First edition  
2021-09

---

---

## 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 18013-5:2021(E)

© ISO/IEC 2021



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

This is a preview of "ISO/IEC 18013-5:2021". Click here to purchase the full version from the ANSI store.

## Contents

	Page
Foreword.....	v
Introduction.....	vi
<b>1 Scope.....</b>	<b>1</b>
<b>2 Normative references.....</b>	<b>1</b>
<b>3 Terms and definitions.....</b>	<b>3</b>
<b>4 Abbreviated terms.....</b>	<b>5</b>
<b>5 Conformance requirement.....</b>	<b>6</b>
<b>6 mDL overview.....</b>	<b>6</b>
6.1 Interfaces.....	6
6.2 Functional requirements.....	7
6.3 Technical requirements.....	8
6.3.1 Data model.....	8
6.3.2 Data exchange.....	8
6.3.3 Security mechanisms.....	13
<b>7 mDL data model.....</b>	<b>15</b>
7.1 mDL document type and namespace.....	15
7.2 mDL data.....	16
7.2.1 Overview.....	16
7.2.2 Portrait of mDL holder.....	21
7.2.3 Issuing authority.....	21
7.2.4 Categories of vehicles/restrictions/conditions.....	21
7.2.5 Age attestation: nearest “true” attestation above request.....	22
7.2.6 Biometric template.....	23
7.2.7 Signature or usual mark.....	23
7.2.8 Domestic data elements.....	23
7.3 Country codes.....	23
<b>8 Transaction.....</b>	<b>23</b>
8.1 Encoding of data structures and data elements.....	23
8.2 Device engagement.....	24
8.2.1 Device engagement information.....	24
8.2.2 Device engagement transmission technology.....	26
8.2.3 Device engagement time-out.....	28
8.3 Data retrieval.....	29
8.3.1 Data model.....	29
8.3.2 Data retrieval methods.....	29
8.3.3 Data retrieval transmission technologies.....	36
<b>9 Security mechanisms.....</b>	<b>47</b>
9.1 Device retrieval.....	47
9.1.1 Session encryption.....	47
9.1.2 Issuer data authentication.....	49
9.1.3 mdoc authentication.....	52
9.1.4 mdoc reader authentication.....	55
9.1.5 Session transcript and cipher suite.....	56
9.2 Server retrieval.....	58
9.2.1 TLS.....	58
9.2.2 JWS.....	58
9.3 Validation and inspection procedures.....	59
9.3.1 Inspection procedure for issuer data authentication.....	59
9.3.2 Inspection procedure for JWS.....	59
9.3.3 Certificate validation procedure.....	60

This is a preview of "ISO/IEC 18013-5:2021". [Click here to purchase the full version from the ANSI store.](#)

<b>Annex A</b> (informative) <b>BLE L2CAP transmission profile</b> .....	<b>61</b>
<b>Annex B</b> (normative) <b>Certificate and CRL profiles</b> .....	<b>62</b>
<b>Annex C</b> (informative) <b>Verified issuer certificate authority list (VICAL) provider</b> .....	<b>90</b>
<b>Annex D</b> (informative) <b>Data structure examples</b> .....	<b>112</b>
<b>Annex E</b> (informative) <b>Privacy and security recommendations</b> .....	<b>135</b>
<b>Annex F</b> (informative) <b>IANA Considerations</b> .....	<b>149</b>
<b>Bibliography</b> .....	<b>153</b>

This is a preview of "ISO/IEC 18013-5:2021". Click here to purchase the full version from the ANSI store.

## 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](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs)).

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](http://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](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://www.iec.ch/understanding-standards).

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 and IEC websites.

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](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

## 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.