Technical Report

ISO/IEC TR 25219

Personal identification — ISO-compliant driving licence — Considerations for early adopters of ISO/IEC 18013-7

Identification des personnes — Permis de conduire conforme à l'ISO — Éléments à prendre en compte pour les premiers utilisateurs de l'ISO/IEC 18013-7

First edition
2024-10

Reference number
ISO/IEC TR 25219:2024(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

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 or www.iec.ch/members_experts/refdocs).

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. In the IEC, see 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*.

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-committees.

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.

ISO/IEC TS 18013-7 augments the capabilities of the mDL by describing the interface and related requirements for presentation to an mDL reader over the internet.

This document lists considerations for early adopters of ISO/IEC TS 18013-7, to the extent they are important to an early adopter. The protocols defined in ISO/IEC TS 18013-7 continue to be improved. This means that early adopters of ISO/IEC TS 18013-7 can expect to see updates in the future.

Personal identification — ISO-compliant driving licence — Considerations for early adopters of ISO/IEC 18013-7

1 Scope

This document specifies considerations that can be of use to implementers and developers that elect to participate in work around updates to ISO/IEC TS 18013-7. These considerations are intended to support the improvements, to maximize backward compatibility and to, at minimum, maintain the security and privacy properties already embodied in ISO/IEC TS 18013-7.

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 TS 18013-7, *Personal identification — ISO-compliant driving licence — Part 7: Mobile driving licence (mDL) add-on functions*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC TS 18013-7 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/

4 Considerations

Unless specifically indicated otherwise, the considerations that follow apply equally to the existing protocols described in ISO/IEC TS 18013-7 as well as to the digital credentials API initiative of the World Wide Web Consortium (W3C) Web Platform Incubator Community Group (WIGC).

1. Works with the wallet/app of choice of the issuing authority, within reason. The intent of this consideration is not to ensure support for esoteric wallets/apps. The intent with this consideration is to prevent a situation where an issuing authority prefers a generally available or mainstream wallet/app, such as a mature implementation available from the OpenWallet Foundation, but the digital credentials API/operating system combination does not support the wallet/app. Discretion is needed when applying this consideration.

2. Provides protection against engagement/request information being forwarded by an attacker to an mdoc by binding the presentment to the originating request channel. See Clause 6.5 in ISO/IEC TS 18013-7.

3. Minimizes the information an mDL reader has to provide to the digital credentials API in order to ultimately retrieve information (upon user consent) from the mdoc.

4. Provides for the following independent items:

    a. Allows the mdoc reader to convey identifying and attestation information about the mDL verifier to the mdoc, functionally similar in terms of content and authentication to what can be conveyed via the mdoc reader authentication certificate in ISO/IEC 18013-5. For example, the mdoc reader

authentication certificate could be used to convey that the verifier has obtained a privacy certification from a certification body, or that the verifier has been authorized to receive certain data elements. “Authentication” as used here refers to the ability of the mdoc to confirm the authenticity of the identity and attestations received from the mdoc reader with the same level of trust possible in ISO/IEC 18013-5.

b. Specifically for the digital credentials API, allows wallet selection and delivery of payload that will allow subsequent use of the existing mechanisms in ISO/IEC TS 18013-7 and ISO/IEC 18013-5 with minimal change.

c. Delivers a message equivalent in function to the DeviceRequest message (maintaining the concepts of the doctype(s), namespace(s) and field identifiers as described in ISO/IEC 18013-5) to the mdoc.

d. Accepts a DeviceResponse message, as described in ISO/IEC 18013-5, as part of the response from the mdoc.

e. Implements application layer encryption for the response from the mdoc, where the encryption complies with the following:

   — The encryption scheme uses an asymmetric key algorithm to derive an ephemeral symmetric key that is used to encrypt the response.

   — The session transcript as defined in ISO/IEC TS 18013-7 and ISO/IEC 18013-5 is used as part of key derivation.

Bibliography

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

ICS 35.240.15
Price based on 3 pages

iso.org