

STN	Osobná identifikácia Vodičský preukaz v súlade s ISO Časť 5: Aplikácia mobilného vodičského preukazu (mDL)	STN ISO/IEC 18013-5 97 4158
------------	---	--

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

Informationstechnik
Persönliche Identifikation
ISO-konformer Führerschein
Teil 5: Mobile Führerscheinanwendung (mDL)

Táto slovenská technická norma obsahuje anglickú verziu medzinárodnej normy ISO/IEC 18013-5: 2021 a má postavenie oficiálnej verzie.

This Slovak standard includes the English version of the International standard ISO/IEC 18013-5: 2021 and has the status of the official version.

136988

Anotácia

Tento dokument stanovuje špecifikácie rozhrania na implementáciu vodičského preukazu v spojení s mobilným zariadením. Tento dokument špecifikuje rozhranie medzi mDL a mDL čítačkou a rozhranie medzi čítačkou mDL a infraštruktúrou vydávajúceho orgánu. Tento dokument umožňuje aj iným stranám, ako je vydávajúci orgán (napr. iné vydávajúce orgány alebo mDL overovatelia v iných krajinách):

- použiť strojové čítanie na získanie údajov mDL;
- prepojiť mDL voči držiteľovi mDL;
- overiť pôvod údajov mDL;
- overiť integritu údajov mDL.

Nasledujúce je mimo rozsahu tohto dokumentu:

- ako sa získava súhlas držiteľa mDL na zdieľanie údajov;
- požiadavky na uchovávanie údajov mDL a súkromných kľúčov mDL.

Národný predhovor

Obrázky v tejto norme sú prevzaté z elektronických podkladov dodaných z ISO, © 2021 ISO, ref. č. ISO/IEC 18013-5 E: 2021.

Normatívne referenčné dokumenty

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN a TNI možno získať na webovom sídle www.unms.sk.

ISO 3166-1 prijatá ako STN EN ISO 3166-1 Kódy názvov krajín a ich častí. Časť 1: Kódy krajín (ISO 3166-1) (01 0190)

ISO 3166-2: 2020 dosiaľ neprijatá

ISO/IEC 5218 dosiaľ neprijatá

ISO/IEC 7816-4: 2020 dosiaľ neprijatá

ISO/IEC 8859-1 dosiaľ neprijatá

ISO/IEC 18004 dosiaľ neprijatá

ISO/IEC 18013-1: 2018 dosiaľ neprijatá

ISO/IEC 18013-2: 2020 dosiaľ neprijatá

ISO/IEC 19785-3: 2020 dosiaľ neprijatá

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

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

NFC Forum, Connection Handover (CH) Technical Specification, Version 1.5

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

OpenID Foundation OpenID Connect Core 1.0 incorporating errata set 1

OpenID Foundation OpenID Connect Discovery 1.0 incorporating errata set 1

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

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

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

RFC 6066, D. Eastlake 3rd, Transport Layer Security (TLS) Extensions: Extension Definitions, January 2011

RFC 7049, C. Bormann et al., Concise Binary Object Representation (CBOR), October 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, January 2016

RFC 7905, A. Langley et al., ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS), June 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 8252, W. Denniss et al., OAuth 2.0 for Native Apps, October 2017

RFC 8259, T. Bray, The JavaScript Object Notation (JSON) Data Interchange Format, December 2017

RFC 8410, S. Josefsson et al., Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure, August 2018

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

RFC 8943, M. Jones et al., Concise Binary Object Representation (CBOR) Tags for Date, November 2020

RFC, CBOR Object Signing and Encryption (COSE): Headers for carrying and referencing X.509 certificates Wi-Fi Alliance, Neighbor Awareness Networking Specification, Version 3.1

Vypracovanie slovenskej technickej normy

Spracovateľ: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

Contents

Page

Foreword.....	v
Introduction.....	vi
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions.....	3
4 Abbreviated terms.....	5
5 Conformance requirement.....	6
6 mDL overview.....	6
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
7 mDL data model.....	15
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
8 Transaction.....	23
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
9 Security mechanisms.....	47
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

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

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).

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) 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. 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*.

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 and 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.

Personal identification — ISO-compliant driving licence —

Part 5: Mobile driving licence (mDL) application

1 Scope

This document establishes interface specifications for the implementation of a driving licence in association with a mobile device. This document specifies the interface between the mDL and mDL reader and the interface between the mDL reader and the issuing authority infrastructure. This document also enables parties other than the issuing authority (e.g. other issuing authorities, or mDL verifiers in other countries) to:

- use a machine to obtain the mDL data;
- tie the mDL to the mDL holder;
- authenticate the origin of the mDL data;
- verify the integrity of the mDL data.

The following items are out of scope for this document:

- how mDL holder consent to share data is obtained;
- requirements on storage of mDL data and mDL private keys.

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

ISO 3166-2:2020, *Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code*

ISO/IEC 5218, *Information technology — Codes for the representation of human sexes*

ISO/IEC 7816-4:2020, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 8859-1, *Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1*

ISO/IEC 18004, *Information technology — Automatic identification and data capture techniques — QR Code 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 18013-2:2020, *Personal identification — ISO-compliant driving licence — Part 2: Machine-readable technologies*

ISO/IEC 18013-5:2021(E)

ISO/IEC 19785-3:2020, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

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

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

NFC Forum, *Connection Handover (CH) Technical Specification, Version 1.5*

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

OpenID Foundation *OpenID Connect Core 1.0 incorporating errata set 1*

OpenID Foundation *OpenID Connect Discovery 1.0 incorporating errata set 1*

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

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

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

RFC 6066, *D. Eastlake 3rd, Transport Layer Security (TLS) Extensions: Extension Definitions, January 2011*

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

RFC 7905, *A. Langley et al., ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS), June 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 8252, *W. Denniss et al., OAuth 2.0 for Native Apps, October 2017*

RFC 8259, *T. Bray, The JavaScript Object Notation (JSON) Data Interchange Format, December 2017*

RFC 8410, *S. Josefsson et al., Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure, August 2018*

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

RFC 8943, *M. Jones et al., Concise Binary Object Representation (CBOR) Tags for Date, November 2020*

RFC, *CBOR Object Signing and Encryption (COSE): Headers for carrying and referencing X.509 certificates*

Wi-Fi Alliance, *Neighbor Awareness Networking Specification, Version 3.1*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN