DRAFT International Standard

ISO/IEC DIS 18013-3

Personal identification — ISO-compliant driving licence —

Part 3: Access control, authentication and integrity validation

ICS: 35.240.15

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

Secretariat: **BSI**

Voting begins on:
2026-02-23

Voting terminates on:
2026-05-18

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 18013-3:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **2**
4 Abbreviated terms **6**
5 Conformance **7**
6 Functional requirements **7**
6.1 Access control 7
6.2 Document authentication 8
6.3 Data integrity validation 8
7 Mapping of mechanisms to requirements and technologies **10**
8 Mechanisms **12**
8.1 Passive authentication (Ver 02) 12
8.1.1 Purpose 12
8.1.2 Applicability 12
8.1.3 Description 13
8.1.4 Hash function 13
8.1.5 Signing method 14
8.2 Active authentication 17
8.2.1 Purpose 17
8.2.2 Applicability 17
8.2.3 Description 17
8.2.4 Mechanism 17
8.3 Scanning area identifier 19
8.3.1 Applicability 19
8.3.2 Description 19
8.4 Non-match alert 29
8.4.1 Purpose 29
8.4.2 Applicability 30
8.4.3 Description 30
8.4.4 Mechanism 30
8.5 Basic access protection 33
8.5.1 Purpose 33
8.5.2 Applicability 33
8.5.3 Description 33
8.5.4 Mechanism 33
8.6 Extended Access Control v1 35
8.6.1 Purpose 35
8.6.2 Applicability 35
8.6.3 Description and mechanism 35
8.7 PACE 35
8.7.1 Purpose 35
8.7.2 Applicability 35
8.7.3 Description and Mechanism 35
8.7.4 PACE relative to BAP 36
9 Security mechanism indicator **36**
10 SIC LDS **37**
10.1 General 37
10.2 EF.SOD – Document security object (short EF identifier = ‘1D’, Tag = ‘77’) 39
10.3 EF.DG12 Non-match alert (short EF identifier= ‘0C’, Tag = ‘71’) 39

© ISO/IEC 2026 – All rights reserved

10.4 EF.DG13 Active authentication (short EF identifier = '0D', Tag = '6F') 40
10.5 EF.DG14 EACv1 (short EF identifier = '0E', Tag = '6E') 40
10.6 EF.CardAccess if PACE is supported (short EF identifier = '1C') 40
Annex A (informative) **Public key infrastructure (PKI)** **41**
Annex B (normative) **Basic access protection** **53**
Annex C (Normative) **PACE** **69**
Annex D (Normative) **Extended Access Control v1** **79**
Annex E (normative) **SIC Command set** **83**
Annex F (Normative) **List of tags used** **85**
Annex G (informative) **Passive authentication (Version 01)** **87**
Bibliography **92**

© ISO/IEC 2026 – All rights reserved

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 draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes 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 *[had/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. ISO 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 Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and security devices for personal identification*.

This third edition cancels and replaces the second edition (ISO/IEC 18013-3:2017), which has been technically revised.

The main changes are as follows:

— Update ICAO references,

— Incorporate all published amendments

A list of all parts in the ISO/IEC 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.

© ISO/IEC 2026 – All rights reserved

Introduction

This document prescribes requirements for the implementation of mechanisms to control access to data recorded in the machine-readable technology on an ISO-compliant driving licence (IDL), verifying the origin of an IDL, and confirming data integrity.

One of the functions of an IDL is to facilitate international interchange. While storing data in machine-readable form on the IDL supports this function by speeding up data input and eliminating transcription errors, certain machine-readable technologies are vulnerable to being read without the knowledge of the card holder and to other means of unauthorized access by unintended persons that is other than driving licence or law enforcement authorities. Controlling access to IDL data stored in machine- readable form protects the data on the card from being read remotely by electronic means without the knowledge of the card holder.

Identifying falsified driving licences or an alteration to the human-readable data on authentic driving licences present a major problem for driving licence and law enforcement authorities, both domestically and in the context of international interchange. Verifying the authenticity of an IDL and confirming the integrity of the data recorded on an IDL provide driving licence and law enforcement authorities with a means to identify an authentic IDL from a falsified or altered one in the interests of traffic law enforcement and other traffic safety processes.

© ISO/IEC 2026 – All rights reserved

Personal identification — ISO-compliant driving licence —

Part 3:
Access control, authentication and integrity validation

1 Scope

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), machine-readable technologies (ISO/IEC 18013-2), and access control, authentication and integrity validation (ISO/IEC 18013-3). It creates a common basis for international use and mutual recognition of the IDL without impeding individual countries/states to apply their privacy rules and national/community/regional motor vehicle authorities in taking care of their specific needs.

This document

— is based on the machine-readable data content specified in ISO/IEC 18013-2;

— specifies mechanisms and rules available to issuing authorities (IAs) for:

  — access control (i.e. limiting access to the machine-readable data recorded on the IDL),

  — document authentication (i.e. confirming that the document was issued by the claimed IA), and

  — data integrity validation (i.e. confirming that the data has not been changed since issuing).

This document does not address issues related to the subsequent use of data obtained from the IDL, e.g. privacy issues.

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 1831, *Printing specifications for optical character recognition*

ISO/IEC 7816-4, *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 9796-2, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

ISO/IEC 9797-1, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO/IEC 10118-3, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

ISO/IEC 11770-2:1996, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*

© ISO/IEC 2026 – All rights reserved

ISO/IEC 11770-2:1996/Cor.1:2005, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques — Technical Corrigendum 1*

ISO/IEC 18013-1, *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 18033-3:2010, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

ANSI X9.62:2005, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*

BSI Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents — Part 1 — eMRTDs with BAC/PACEv2 and EACv1 — Version 2.10 — 2012-03-20

BSI Technical Guideline TR-03110-3: Advanced Security Mechanisms for Machine Readable Travel Documents — Part 3 — Common Specifications — Version 2.10 — 2012-03-20

FIPS 186-4, *(including Change Notice), Digital Signature Standard (DSS), Federal Information Processing Standards Publication, National Institute of Standards and Technology, July 2013*

ICAO Doc 9303 – Machine Readable Travel Documents, Eighth Edition, 2021, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC) [Doc 9303-10]

ICAO Doc 9303 – Machine Readable Travel Documents, Eighth Edition, 2021, Part 11: Security Mechanisms for MRTDs [Doc 9303-11]"

NIST/SP 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005*

RFC 2631, *E. Rescorla, Diffie-Hellman Key Agreement Method, June 1999*

RFC 3279, *W. Polk et al., Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002*

RFC 3280, *R. Housley et al., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002*

RFC 3369, *R. Housley, Cryptographic Message Syntax, August 2002*

RFC 4055, *J. Schaad, B. Kaliski, R. Housley, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, June 2005*

RFC 5639, *M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010*

RFC 8422, *Y. Nir, S. Josefsson, M. Pegourie-Gonnard, Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier, August 2018*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 18013-1, ISO/IEC 18013-2 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/

© ISO/IEC 2026 – All rights reserved

3.1
active authentication
mechanism that uses information stored in a secure area of a *secure integrated circuit (SIC)* (3.17) to confirm that the SIC and the other machine-readable data were issued together

Note 1 to entry: See 8.2.

3.2
basic access protection
BAP
mechanism to confirm that an inspection system (IS) has physical access to a proximity integrated circuit card (PICC) before the IS is allowed access to the data stored on the PICC and to ensure that communication between the IS and the PICC (once access is authorized) is protected

Note 1 to entry: See 8.5 and Annex B.

3.3
chip authentication
ephemeral-static key agreement protocol that provides authentication of the *secure integrated circuit* (3.17) and strong secure messaging

Note 1 to entry: See 8.6.

3.4
clone
unauthorized exact copy of a document that has the same security characteristics as the original document and that cannot be distinguished from the legitimate one

3.5
eavesdropping
unauthorized interception and interpretation of information-bearing emanations

[SOURCE: ISO/IEC 2382-8:2015, 08.05.25, modified]

3.6
extended access control v1
EACv1
protocol used to limit access to optional signature and biometric data groups

Note 1 to entry: See 8.6 and Annex D.

3.7
input string
string of characters printed on an ISO-compliant driving licence [as human-readable text, optionally (or by specification) accompanied by or consisting of a machine-readable rendering thereof] used as input (either manually or automatically through the use of suitable equipment) for the non-match alert and *BAP* (3.2) or *PACE* (3.10) mechanisms

3.8
issuing authority
IA
licensing authority (or issuing country if separate licensing authorities have not been authorized) which applies a digital signature to an ISO-compliant driving licence and is responsible for the associated key management

[SOURCE: ISO/IEC 18013-1]

© ISO/IEC 2026 – All rights reserved

3.9
non-match alert
mechanism to detect any differences between the machine-readable information and (some of) the human-readable information on an ISO-compliant driving licence

Note 1 to entry: See 8.4.

3.10
PACE
alternative mechanism to BAP to confirm that an inspection system (IS) has physical access to a *secure integrated circuit (SIC)* (3.17) on a driving licence card before the IS is allowed to access to the data stored on the SIC and to establish a secure communication channel between the IS and SIC once access is authorised

Note 1 to entry: See 8.7 and Annex C.

3.11
passive authentication
mechanism to confirm that machine-readable data on an ISO-compliant driving licence (IDL) has not been changed since the IDL was issued

Note 1 to entry: See 8.1 and Annex G (informative)..

3.12
pseudo issuing authority
PIA
authority that does not issue ISO-compliant driving licences [but that is similar to an *issuing authority (IA)* (3.8) in all other respects] and which does not issue document keys, but which does have a root key pair with which it can sign documents of other IAs or PIAs that it trusts

3.13
public key infrastructure
PKI
technologies and products using public key (asymmetric) cryptography

Note 1 to entry: Both *passive authentication* (3.11) and extended access protection use this technology.

3.14
reading authority
RA
authorized entity reading the machine-readable data on an ISO-compliant driving licence (IDL)

Note 1 to entry: Driving licence authorities other than the authority that issued the IDL and law enforcement authorities are examples of reading authorities.

3.15
reference string
string of characters used as a reference against which to compare the *input string* (3.7) when using the *non-match alert* (3.9) mechanism, and used for session key calculation purposes by the *secure integrated circuit* (3.17) during execution of the *basic access protection* (3.2) mechanism

3.16
scanning area identifier
SAI
one or more graphical elements that demarcate an *input string* (3.7)

© ISO/IEC 2026 – All rights reserved

3.17
secure integrated circuit
SIC
integrated circuit that includes both a security feature (or security features), and memory and/or a central processing unit

Note 1 to entry: An integrated circuit card with contacts and a proximity integrated circuit card (PICC) are examples of a SIC.

Note 2 to entry: A SIC can be embedded in different solutions, for example in ID-1 sized cards (as used for the ISO-compliant driving licence) and in a booklet (as found in passports).

3.18
secure memory
integrated circuit (IC) memory of which the content [once populated by an *issuing authority* (3.8) during the personalization process] is accessible only by the IC operating system for internal use, and cannot be made available by the operating system to any reading device

3.19
skimming
reading data from a proximity integrated circuit card (PICC) without the card holder's awareness

3.20
trust chain
sequential set of *trust points* (3.23) that a *verifying authority* (3.26) references to verify a specific *issuing authority's* (3.8) public root key

3.21
trust model
description of the functional and logical aspects of a traditional *public key infrastructure* (3.13), specifically excluding technical implementation details

3.22
trust network
component of a *trust model* (3.21) that describes the trust relationships and chains between issuing authorities

3.23
trust point
issuing authority (3.8) or *pseudo issuing authority* (3.12) that publishes a trust list (and the related public root keys) that verifying entities can reference

3.24
twinning
copying the data and/or integrated circuit of a physically and/or biometrically similar driver to the attacker's integrated circuit or ISO-compliant driving licence

3.25
unpacked BCD
binary coding of a sequence of integers using 4 bits for each integer (where the bit weights are 8421) and encoding one integer in the least significant bits of each byte

Note 1 to entry: Only unsigned BCD is used in this document.

3.26
verifying authority
VA
verifying entity (3.27) that is part of a *trust network* (3.22), i.e. that also is an *issuing authority* (3.8) or a *pseudo issuing authority* (3.12)

Note 1 to entry: Not all verifying entities are VAs. A car rental company can be a verifying entity, but is not a VA as it is not part of the trust network.

© ISO/IEC 2026 – All rights reserved

Note 2 to entry: VAs can be divided into *immediate VAs* (3.26.1) and *non-immediate VAs* (3.26.2).

3.26.1
immediate VA
VA (3.26) that acquired the public root key of the *issuing authority* (3.8) via out-of-band means

3.26.2
non-immediate VA
VA (3.26) that acquired the public root key of the *issuing authority* (3.8) from another VA

3.27
verifying entity
entity that tries to determine if a digital signature is valid (i.e. if the data to which a certificate has been applied has not been changed, and if the signature was generated by the *issuing authority* (3.8) the verifying entity expects)

4 Abbreviated terms

APDU	application protocol data unit
BAC	basic access control
BCD	binary coded decimal
BER-TLV	basic encoding rules – tag-length-value (see ISO/IEC 8825-1)
CA	certification authority
CBC	cipher block chaining
DER	distinguished encoding rules (see ISO/IEC 8825-1)
DF	dedicated file
DG	data group
DO	data object
DST	control reference template for digital signature (see ISO/IEC 7816-4)
EAP	extended access protection
EF	elementary file
IC	integrated circuit
ICC	integrated circuit card
IDL	ISO-compliant driving licence
IFD	interface device
IS	inspection system
IV	initialization vector
KAT	control reference template for key agreement (see ISO/IEC 7816-4)
LDS	logical data structure
MAC	message authentication code

© ISO/IEC 2026 – All rights reserved