INTERNATIONAL STANDARD

ISO/IEC 18013-3

Second edition
2017-04

Information technology — Personal identification — ISO-compliant driving licence —

Part 3: Access control, authentication and integrity validation

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

Partie 3: Contrôle d'accès, authentification et validation d'intégrité

Reference number
ISO/IEC 18013-3:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 17, *Cards and personal identification*.

This second edition cancels and replaces the first edition (ISO/IEC 18013-3:2009), which has been technically revised. It also incorporates the Amendments ISO/IEC 18013-3:2009/Amd 1:2012 and ISO/IEC 18013-3:2009/Amd 2:2014, and the Technical Corrigenda ISO/IEC 18013-3:2009/Cor 1:2011 and ISO/IEC 18013-3:2009/Cor 2:2013.

The most significant changes are the following:

— In the interest of interoperability of cards used for personal identification, the authentication protocols for the IDL are simplified. Active Authentication is harmonised with other ISO standards and thus BAP configurations 2, 3 and 4, as well as EAP are no longer supported by this document.

— Replacing EAP, the optional EACv1 protocol is defined for the IDL, enabling access control to sensitive biometric data stored on an integrated circuit. EACv1 may be used in conjunction with either BAP configuration 1 or PACE.

— The optional PACE protocol enables access control to the data stored on an integrated circuit. The PACE protocol is a password authenticated Diffie Hellman key agreement protocol based on a (short) input string that provides secure communication between a secure integrated circuit on an IDL and a terminal and allows various implementation options (mappings, input strings, algorithms). The PACE protocol implementation for the IDL is restricted to Elliptic Curve Diffie Hellman (ECDH) generic mapping and can be used as a stand-alone protocol or in combination with the EACv1 protocol.

A list of all the parts in the ISO/IEC 18013 series can be found on the ISO website.

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.

Information technology — 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 1831:1980, *Printing specifications for optical character recognition*

ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 8859-1:1998, *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 9797-1:1999[1)], *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO/IEC 10118-3:2004, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

1) ISO/IEC 9797-1:1999 is withdrawn and replaced by the 2011 version.

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

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, *Information technology — Personal identification — ISO-compliant driving licence — Part 1: Physical characteristics and basic data set*

ISO/IEC 18013-2, *Information technology — Personal identification — ISO-compliant driving licence — Part 2: Machine-readable technologies*

ISO/IEC 18033-3:2005[3], *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

ISO/IEC 18033-3:2005/Cor1:2006, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers — Technical Corrigendum 1*

ISO/IEC 18033-3:2005/Cor2:2007, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers — Technical Corrigendum 2*

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 186-2 (including Change Notice), *Digital Signature Standard (DSS), Federal Information Processing Standards Publication, National Institute of Standards and Technology, 27 January 2000*

ICAO Technical Report – *Supplemental Access Control for Machine Readable Travel Documents, v1.01, 2010 [TR-PACE*]

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*[4]

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* [4]

RFC 3280, *R. Housley et al., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002* [1]

RFC 3369, *R. Housley, Cryptographic Message Syntax, August 2002* [1]

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* [1]

RFC 5639, *M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010* [1]

2) ISO/IEC 11770-2:1996 is withdrawn and replaced by the 2008 version.

3) ISO/IEC 18033-3:2005 is withdrawn and replaced by the 2010 version.

4) http://www.ietf.org/rfc.html

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 terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

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]

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: As stated in TR-PACE, PACE refers to PACE v2.

Note 2 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.

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)

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.

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
BAP	basic access protection
BCD	binary coded decimal
BER-TLV	basic encoding rules – tag-length-value (see ISO/IEC 8825-1:2002[a])
CA	certification authority
CBC	cipher block chaining
DER	distinguished encoding rules (see ISO/IEC 8825-1:2002)
DF	dedicated file
DG	data group
DO	data object
DST	control reference template for digital signature (see ISO/IEC 7816-4:2013)
EACv1	extended access control v1
EAP	extended access protection
EF	elementary file
IA	issuing authority
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 7816-4:2013)
LDS	logical data structure
MAC	message authentication code
MF	master file
MRTD	machine readable travel document
MRZ	machine readable zone
MSE	manage security environment (see ISO/IEC 7816-4:2013)
OCR	optical character recognition
OID	object identifier
PACE	password authenticated connection establishment
PIA	pseudo issuing authority
PIC	proximity integrated circuit
PICC	proximity integrated circuit card
PKI	public key infrastructure
PSO	perform security operation (see ISO/IEC 7816-4:2013)
RA	reading authority
RFU	reserved for future use
SAI	scanning area identifier
SIC	secure integrated circuit
SM	secure messaging
SOD	document security object
SSC	send sequence counter
TRCA	trust root certificate authority
UTC	coordinated universal time

VA verifying authority

2D two-dimensional

[a] ISO/IEC 8825-1:2002 is withdrawn and replaced by the 2015 version.

5 Conformance

A driving licence is in conformance with this document if it meets all mandatory requirements specified directly or by reference herein. Compliance with ISO/IEC 18013-2 is required for compliance with this document.

Compliance with ISO/IEC 18013-1 is not required for compliance with this document. Conversely, the incorporation of a machine-readable technology which is not compliant with this document does not render the IDL non-compliant with ISO/IEC 18013-1.

6 Functional requirements

6.1 Access control

Access control can be broken down into the following functional requirements:

a) prevent skimming of machine-readable data on a PICC by ensuring that physical access to the IDL is acquired prior to reading;

b) prevent unnoticed alteration of communication between a reader and a SIC;

c) prevent eavesdropping between a reader and a SIC;

d) selectively restrict access to specific optional machine-readable data groups for specific reading authorities.

6.2 Document authentication

Document authentication can functionally be established by allowing for verification of the origin of an IDL.

6.3 Data integrity validation

Data integrity validation can be broken down into the following functional requirements:

a) Verify that the IDL (including the machine-readable data) is not a clone of another IDL. A cloning attempt can schematically be illustrated as shown in Figure 1.

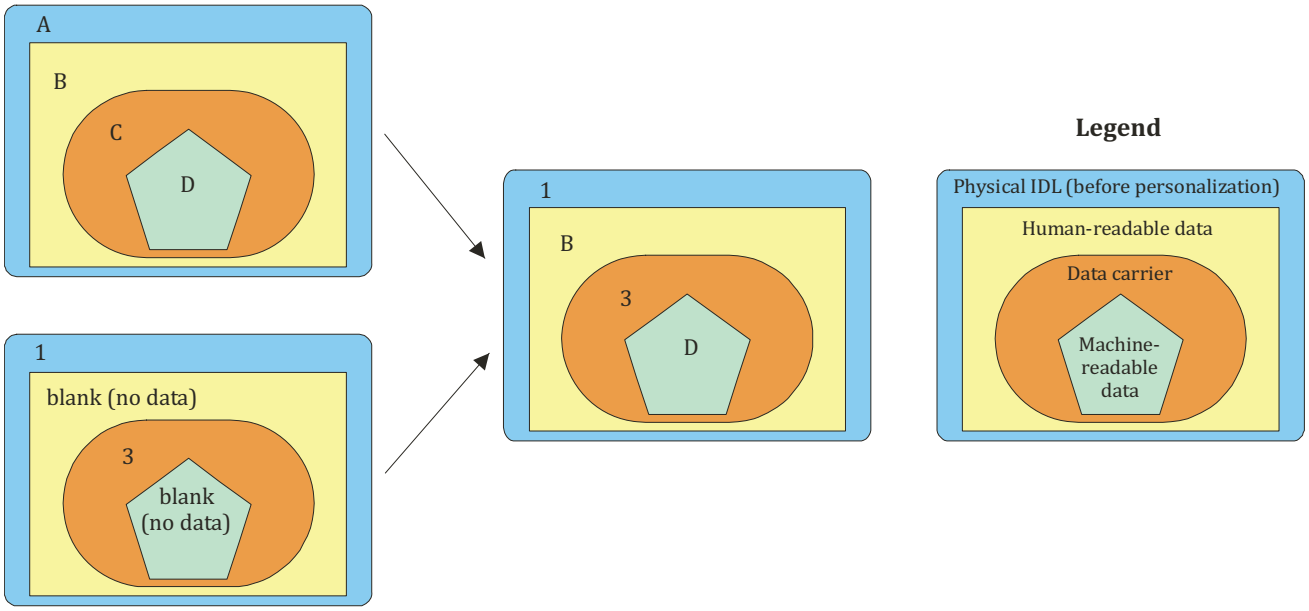

Figure 1 — Data integrity validation: IDL cloning

b) Protect against the exchange of machine-readable data carriers between otherwise authentic IDLs. This type of attack can schematically be illustrated as shown in Figure 2.

NOTE This guards (among others) against an IC "twinning" attack. This type of attack is of particular concern in inspection environments where machine-readable data and human-readable data is not compared (or only cursorily compared by an operator using, for example, a portrait image). Finding a biometrically similar driver is possible by skimming the data of a few thousand IDL PICs.

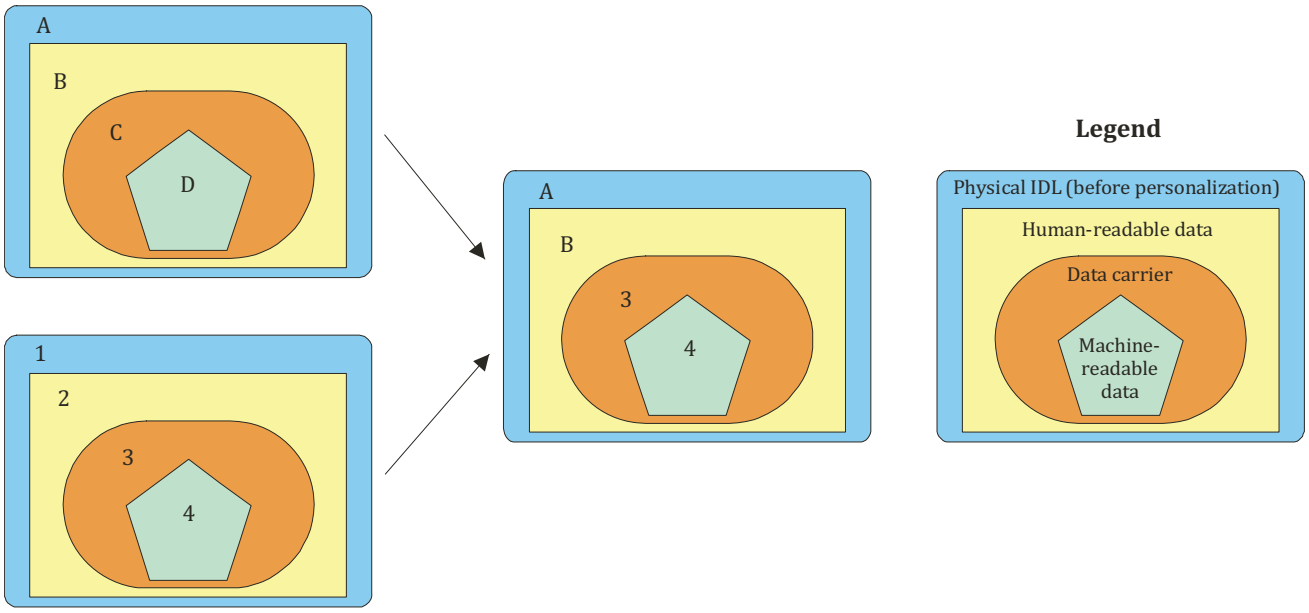

Figure 2 — Data integrity validation: Data carrier exchange or twinning

c) Verify that the physical IDL and the machine-readable data thereon were issued (belong) together. This type of attack can schematically be illustrated as shown in Figure 3.