
**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

This document is a preview generated by ERS



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
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	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	3
4 Abbreviated terms	6
5 Conformance	8
6 Functional requirements	8
6.1 Access control	8
6.2 Document authentication	8
6.3 Data integrity validation	8
7 Mapping of mechanisms to requirements and technologies	11
8 Mechanisms	12
8.1 Passive authentication	12
8.1.1 Purpose	12
8.1.2 Applicability	12
8.1.3 Description	12
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	30
8.4.1 Purpose	30
8.4.2 Applicability	30
8.4.3 Description	30
8.4.4 Mechanism	31
8.5 Basic access protection	32
8.5.1 Purpose	32
8.5.2 Applicability	32
8.5.3 Description	32
8.5.4 Mechanism	33
8.6 Extended Access Control v1	34
8.6.1 Purpose	34
8.6.2 Applicability	34
8.6.3 Description and mechanism	34
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	35
9 Security mechanism indicator	36
10 SIC LDS	37
10.1 General	37
10.2 EFSOD – Document security object (short EF identifier = ‘1D’, Tag = ‘77’)	39

10.3	EF.DG12 Non-match alert (short EF identifier= '0C', Tag = '71')	39
10.4	EF.DG13 Active authentication (short EF identifier = '0D', Tag = '6F')	39
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		51
Annex C (normative) PACE		67
Annex D (normative) Extended Access Control v1		72
Annex E (normative) SIC command set		76
Annex F (normative) List of tags used		78
Bibliography		80

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 9797-1:1999¹⁾, *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 11770-2:1996²⁾, *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 18033-3:2005³⁾, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

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

ISO/IEC 18033-3:2005/Cor.2:2007, *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 1999⁴⁾*

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 2002⁴*

RFC 3280, R. Housley et al., *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002¹*

RFC 3369, R. Housley, *Cryptographic Message Syntax, August 2002¹*

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 2005¹*

RFC 5639, M. Lochter, J. Merkle, *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010¹*

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>