
**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

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2009

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword.....	iv
Introduction	v
1 Scope	1
2 Conformance	1
3 Normative references	1
4 Terms and definitions.....	3
5 Abbreviated terms	6
6 Functional requirements	7
6.1 Access control	7
6.2 Document authentication.....	7
6.3 Data integrity validation	7
7 Mapping of mechanisms to requirements and technologies.....	10
8 Mechanisms	13
8.1 Passive authentication	13
8.2 Active authentication.....	18
8.3 Scanning area identifier	19
8.4 Non-match alert.....	25
8.5 Basic access protection.....	28
8.6 Extended access protection	30
9 Security mechanism indicator.....	31
10 SIC LDS.....	31
10.1 EF.SOD – Document security object (short EF identifier = '1D', Tag = '77').....	33
10.2 EF.DG12 Non-match alert (short EF identifier= '0C', Tag = '71')	33
10.3 EF.DG13 Active authentication (short EF identifier = '0D', Tag = '6F').....	33
10.4 EF.DG14 Extended access protection (short EF identifier = '0E', Tag = '6E')	33
Annex A (informative) Public key infrastructure (PKI)	34
Annex B (normative) Basic access protection.....	43
Annex C (normative) Extended access protection	82
Annex D (normative) SIC command set.....	106
Annex E (normative) List of tags used.....	108
Annex F (normative) Brainpool curves	109
Bibliography	117

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 18013-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

ISO/IEC 18013 consists of the following parts, under the general title *Information technology — Personal identification — ISO-compliant driving licence*:

- *Part 1: Physical characteristics and basic data set.* Part 1 defines the basic terms for ISO/IEC 18013, including physical characteristics, basic data element set, visual layout, and physical security features.
- *Part 2: Machine-readable technologies.* Part 2 defines the technologies that may be used for ISO/IEC 18013, including the logical data structure and data mapping for each technology.
- *Part 3: Access control, authentication and integrity validation.* Part 3 defines the electronic security features that may be incorporated under ISO/IEC 18013, including mechanisms for controlling access to data, verifying the origin of an ISO-compliant driving licence, and confirming data integrity.

Introduction

This part of ISO/IEC 18013 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. Whilst 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 part of ISO/IEC 18013

- a) is based on the machine-readable data content specified in ISO/IEC 18013-2;
- b) specifies mechanisms and rules available to issuing authorities (IAs) for
 - 1) access control (i.e. limiting access to the machine-readable data recorded on the IDL),
 - 2) document authentication (i.e. confirming that the document was issued by the claimed IA),
 - 3) data integrity validation (i.e. confirming that the data has not been changed since issuing).

This part of ISO/IEC 18013 does not address issues related to the subsequent use of data obtained from the IDL, e.g. privacy issues.

2 Conformance

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

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

3 Normative references

The following referenced documents are indispensable for the application 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 7816-4:2005, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 7816-8:2004, *Identification cards — Integrated circuit cards — Part 8: Commands for security operations*

ISO/IEC 8825-1:2002, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 8859-1:1998, *Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1*

ISO/IEC 9797-1:1999, *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*

ISO/IEC 11770-2:1996, *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 — Corrigendum 1*

ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

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, *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 — Corrigendum 1*

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

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

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

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, <http://www.ietf.org/rfc.html>

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, <http://www.ietf.org/rfc.html>

RFC 3280, R. Housley et al., *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, April 2002, <http://www.ietf.org/rfc.html>

RFC 3369, R. Housley, *Cryptographic Message Syntax*, August 2002, <http://www.ietf.org/rfc.html>

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, <http://www.ietf.org/rfc.html>