



BSI Standards Publication

Information technology — Personal identification — ISO-compliant driving licence

Part 3: Access control, authentication and integrity validation

National foreword

This British Standard is the UK implementation of ISO/IEC 18013-3:2017+A2:2023. It supersedes BS ISO/IEC 18013-3:2017+A1:2022, which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to ISO/IEC text carry the number of the ISO/IEC amendment. For example, text altered by ISO/IEC amendment 1 is indicated by A1 A1.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and security devices for personal identification.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient’s own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 19703 7

ICS 35.240.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2017.

Amendments/corrigenda issued since publication

Date	Text affected
31 July 2022	Implementation of ISO/IEC amendment 1:2022
31 May 2023	Implementation of ISO/IEC amendment 2:2023

**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





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	33
8.5.1 Purpose	33
8.5.2 Applicability	33
8.5.3 Description	33
8.5.4 Mechanism	34
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	36
8.7.1 Purpose	36
8.7.2 Applicability	36
8.7.3 Description and mechanism	36
8.7.4 PACE relative to BAP	36
9 Security mechanism indicator	37
10 SIC LDS	38
10.1 General	38
10.2 EFSOD – Document security object (short EF identifier = ‘1D’, Tag = ‘77’)	40

ISO/IEC 18013-3:2017+A2:2023(E)

10.3	EF.DG12 Non-match alert (short EF identifier= '0C', Tag = '71')	40
10.4	EF.DG13 Active authentication (short EF identifier = '0D', Tag = '6F')	40
10.5	EF.DG14 EACv1 (short EF identifier = '0E', Tag = '6E')	41
10.6	EF.CardAccess if PACE is supported (short EF identifier = '1C')	41
Annex A (informative) Public key infrastructure (PKI)		42
Annex B (normative) Basic access protection		52
Annex C (normative) PACE		68
Annex D (normative) Extended Access Control v1		79
Annex E (normative) SIC command set		83
Annex F (normative) List of tags used		85
Bibliography		87

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/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*

A₂ FIPS 186-4 (including Change Notice), *Digital Signature Standard (DSS), Federal Information Processing Standards Publication, National Institute of Standards and Technology, July 2013* **A₂**

A₁ ICAO Doc 9303-10, *Machine Readable Travel Documents, Seventh Edition, 2015, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)*

ICAO Doc 9303-11, *Machine Readable Travel Documents, Seventh Edition, 2015, Part 11: Security Mechanisms for MRTDs* **A₁**

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

A1 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](#). **A1**

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

A2 Note 1 to entry: See [8.1](#) and Annex G (informative). **A2**

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](#).

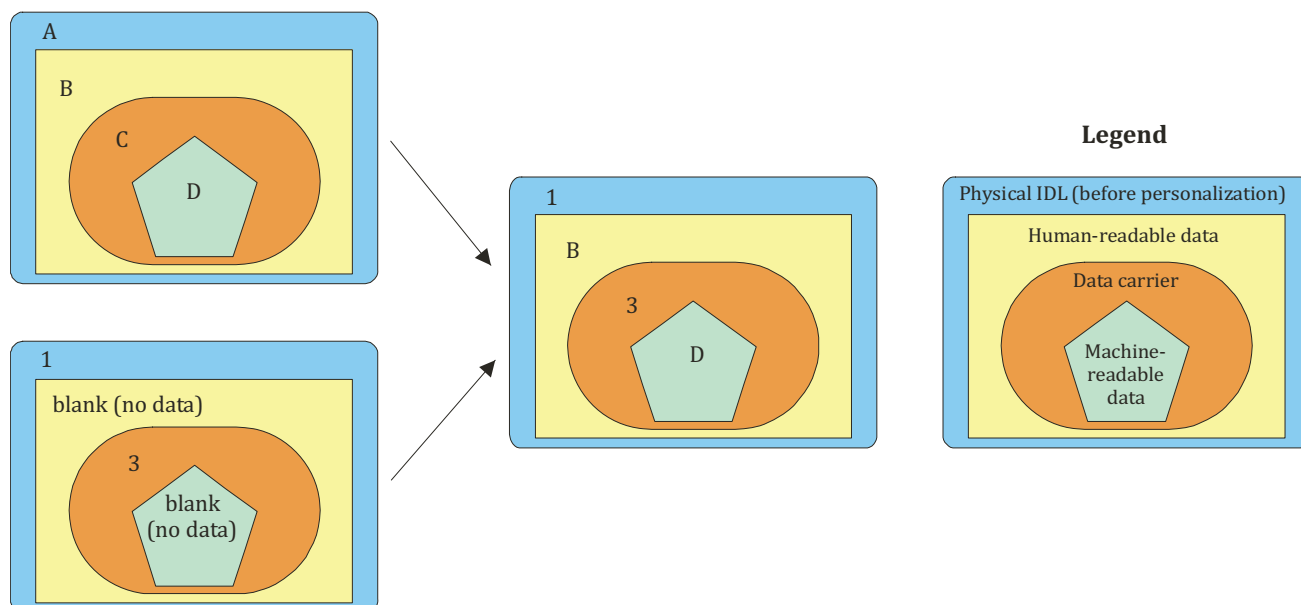


Figure 1 — Data integrity validation: IDL cloning

- 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.

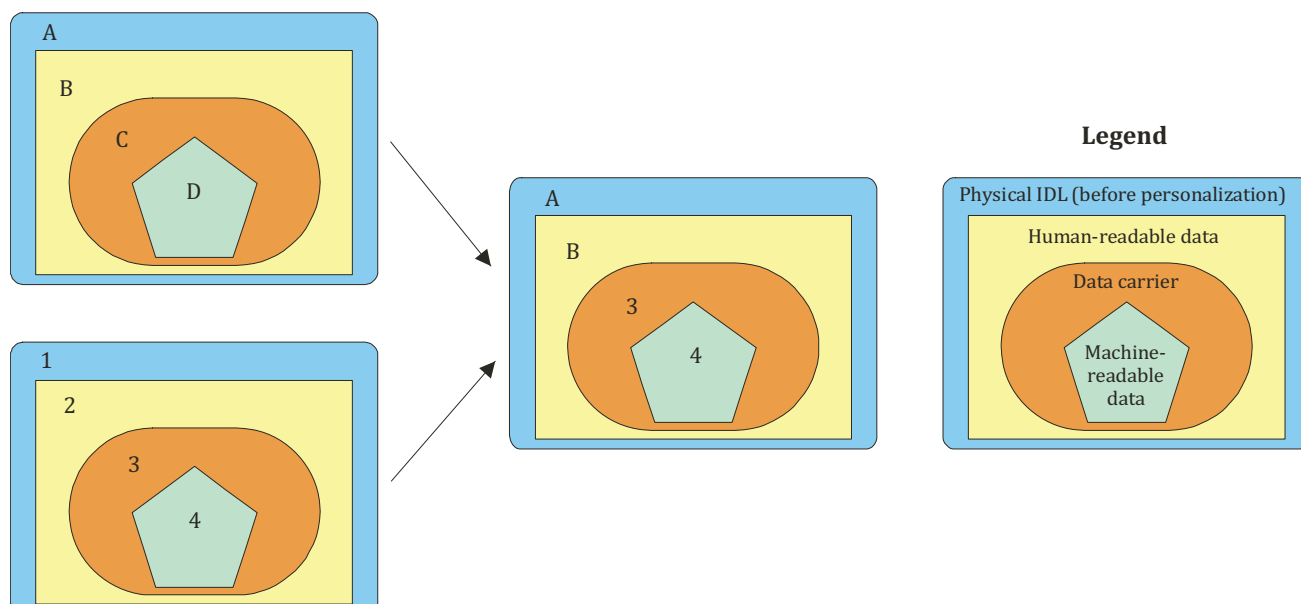


Figure 2 — Data integrity validation: Data carrier exchange or twinning

- 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](#).

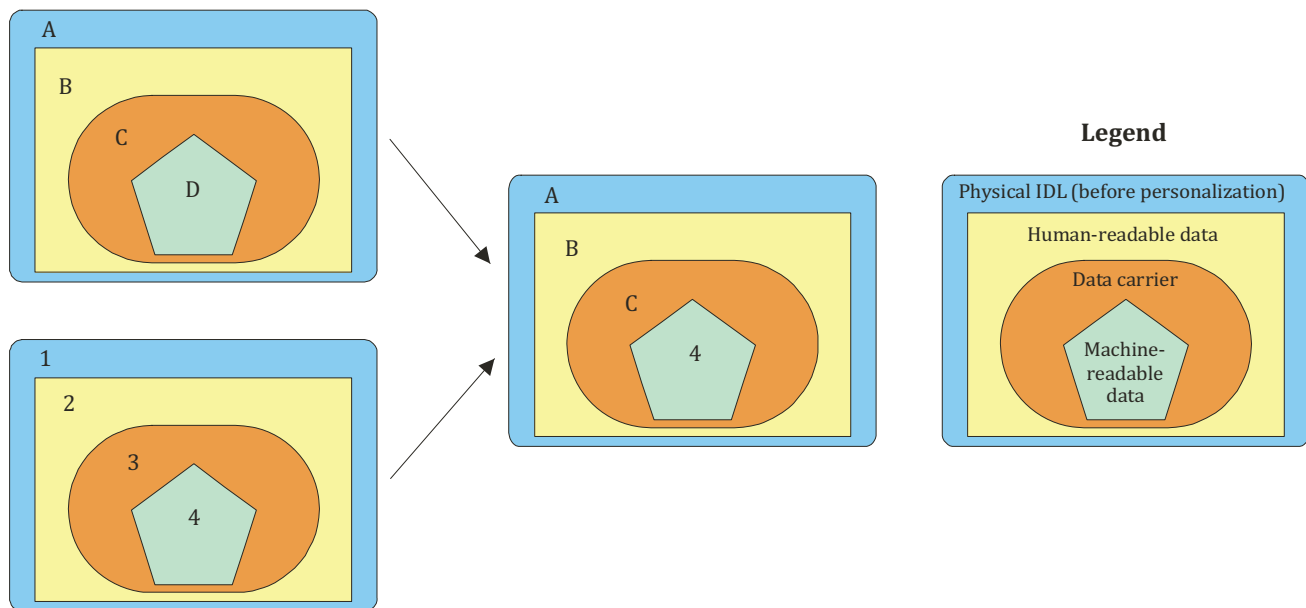


Figure 3 — Data integrity validation: Machine-readable data exchange

- d) Validate the integrity of the human readable data (i.e. confirm that the human-readable data has not changed since issuing). This type of attack can schematically be illustrated as shown in [Figure 4](#).

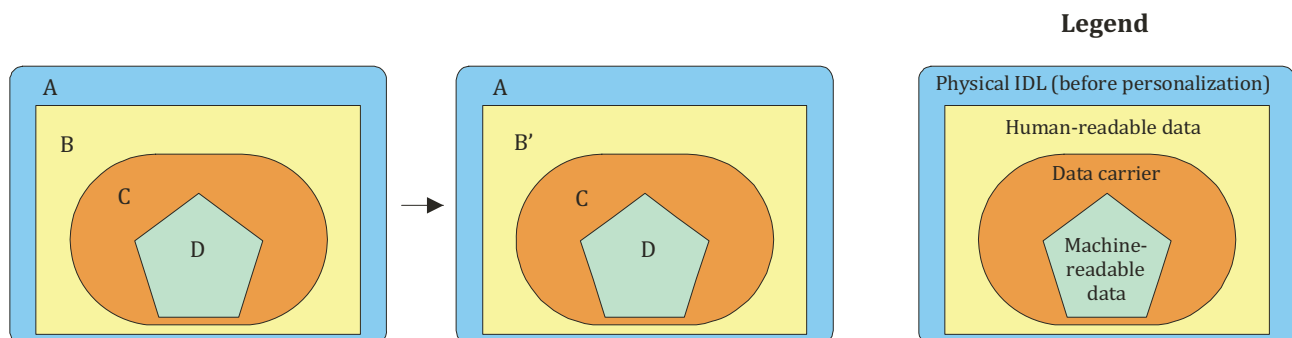


Figure 4 — Data integrity validation: Human-readable data alteration

- e) Validate the integrity of the machine-readable data (i.e. confirm that the machine-readable data has not changed since issuing). This can schematically be illustrated as shown in [Figure 5](#).

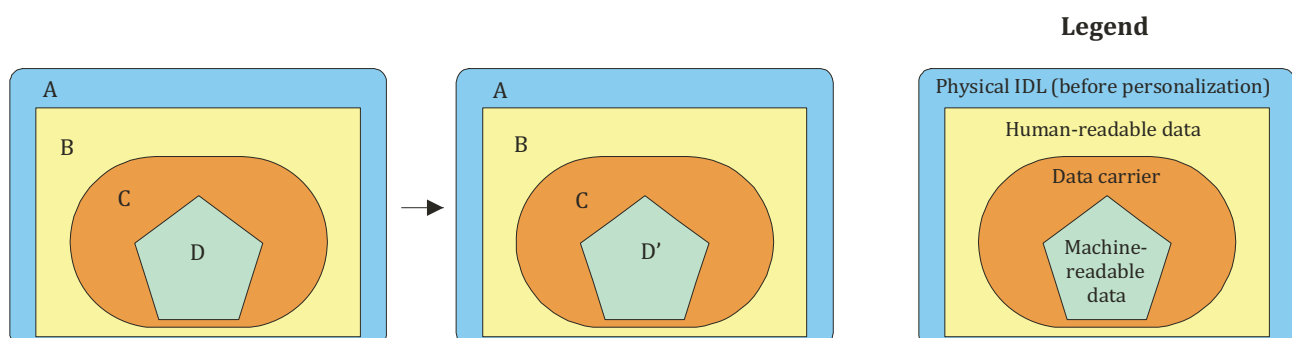


Figure 5 — Data integrity validation: Machine-readable data alteration

7 Mapping of mechanisms to requirements and technologies

Mechanisms that, when used individually, can address specific functional requirements are specified in [Clause 8](#). Mechanisms can also be used together to address a broader range of functional requirements. Not all machine-readable technologies have the same functional requirements, and some mechanisms are applicable only to specific machine-readable technologies. [Table 1](#) specifies the relationships between the mechanisms, machine-readable technologies, and functional requirements.

Table 1 — Applicable mechanisms

Functional requirement	Mechanisms		
	2D bar code	ICC with contacts	PICC
Prevent skimming	Physical access to the IDL is required to read the machine-readable data	Physical access to the IDL is required to read the machine-readable data	BAP or PACE
Prevent unnoticed alteration of communication between a reader and an IDL	N/A	Chip authentication (EACv1) in combination with BAP or PACE secure messaging	BAP or PACE Chip authentication (EACv1) in combination with BAP or PACE secure messaging
Prevent eavesdropping	N/A	Chip authentication (EACv1) in combination with BAP or PACE secure messaging	BAP ^a or PACE Chip authentication (EACv1) in combination with BAP or PACE secure messaging
Selectively restrict access to specific optional machine-readable data groups for specific reading authorities	N/A	Terminal authentication (EACv1)	Terminal authentication (EACv1)
Allow for verification of the origin of an IDL	Step 1: Verify trustworthiness of/obtain a trustworthy asymmetric/public key (via a PKI and a protected distribution communication channel, or via alternative trust building methods) Step 2: Use trusted key to perform passive authentication, followed by use of the non-match alert mechanism, or followed by visual comparison of the human-readable data printed on the document with the authenticated machine-readable data	Step 1: Verify trustworthiness of/obtain a trustworthy asymmetric/public key (via a PKI and a protected distribution communication channel, or via alternative trust building methods) Step 2: Use trusted key to perform passive authentication; if the passive authentication was preceded by BAP or PACE, the IDL is authentic while if BAP or PACE is not implemented, passive authentication can be followed by use of the non-match alert mechanism, or followed by visual comparison of the human-readable data printed on the document with the authenticated machine-readable data	Step 1: Verify trustworthiness of/obtain a trustworthy asymmetric/public key (via a PKI and a protected distribution communication channel, or via alternative trust building methods) Step 2: Use trusted key to perform passive authentication; if the passive authentication was preceded by BAP or PACE, the IDL is authentic while if BAP or PACE is not implemented, passive authentication can be followed by use of the non-match alert mechanism, or followed by visual comparison of the human-readable data printed on the document with the authenticated machine-readable data
Verify that the IDL (including the machine-readable data) is not a clone of another IDL	2D bar code: Cannot be verified through available international standards	Active authentication via challenge response Chip authentication (EACv1)	Active authentication via challenge response Chip authentication (EACv1)
Protect against the exchange of machine readable data carriers between otherwise authentic IDLs	Non-match alert Passive authentication followed by a visual comparison of the human-readable data printed on the document with the authenticated machine-readable data	Non-match alert BAP or PACE Passive authentication followed by a visual comparison of the human-readable data printed on the document with the authenticated machine-readable data	Non-match alert BAP or PACE Passive authentication followed by a visual comparison of the human-readable data printed on the document with the authenticated machine-readable data

Table 1 (continued)

Functional requirement	Mechanisms		
	2D bar code	ICC with contacts	PICC
Verify that the physical IDL and the machine-readable data thereon were issued (belong) together (i.e. that the machine-readable data has not been copied from another IDL)	Non-match alert Passive authentication followed by a visual comparison of the human-readable data printed on the document with the authenticated machine-readable data	Non-match alert BAP or PACE Passive authentication followed by a visual comparison of the human-readable data printed on the document with the authenticated machine-readable data Active authentication via challenge response ^a	Non-match alert BAP or PACE Passive authentication followed by a visual comparison of the human-readable data printed on the document with the authenticated machine-readable data Active authentication via challenge response ^a
Validate the integrity of the human readable data (i.e. confirm that the human-readable data has not changed since issuing)	Non-match alert Passive authentication followed by a visual comparison of the human-readable data printed on the document with the authenticated machine-readable data Visual inspection of the security features incorporated into the IDL (see ISO/IEC 18013-1)	Non-match alert BAP or PACE Passive authentication followed by a visual comparison of the human-readable data printed on the document with the authenticated machine-readable data Visual inspection of the security features incorporated into the IDL (see ISO/IEC 18013-1)	Non-match alert BAP or PACE Passive authentication followed by a visual comparison of the human-readable data printed on the document with the authenticated machine-readable data Visual inspection of the security features incorporated into the IDL (see ISO/IEC 18013-1)
Validate the integrity of the machine-readable data (i.e. confirm that the machine-readable data has not changed since issuing)	Passive authentication	Passive authentication	Passive authentication
NOTE Visual comparison of human-readable information printed on an IDL with machine-readable information obtained from the same IDL is not formally specified as a mechanism in this document; it is assumed that such comparison can be implemented by any RA in a manner that meets local needs.			
^a The entropy of the reference string used has to be commensurate with the IA's assessment of the threat.			

IA's may selectively implement the mechanisms identified above, subject to any dependencies noted in [Clause 8](#).

8 Mechanisms

8.1 Passive authentication (ver 02)

8.1.1 Purpose

The purpose of passive authentication is to confirm that machine-readable data has not been changed since the IDL was issued.

 This version 02 of passive authentication supersedes the deprecated version 01 included in Annex G (informative) for the information of manufacturers of readers that must be able to read IDL cards issued in accordance with this version that have not yet expired. 

8.1.2 Applicability

Passive authentication is applicable to all machine-readable technologies.

8.1.3 Description

Passive authentication is implemented by way of a digital signature over specified machine-readable data on the IDL, using a public-private (asymmetric) key pair.

In the case of standard encoding, a separate message digest is calculated for each data group and included in the machine-readable data. The collection of message digests is then digitally signed (using a private key that is kept secret by the IA) and the digital signature is added to the machine-readable data.

In the case of compact encoding, no message digests are calculated separately. The contents of the data groups present is directly signed (using a private key that is kept secret by the IA) and the digital signature is added to the machine-readable data.

NOTE A message digest has the following properties:

- a) It is very small in size compared to the IDL data.
- b) The probability of finding any two (different) IDL data sets that lead to the same message digest is negligible. This has the following implications:
 - 1) The probability of finding an IDL data set A that produces the same message digest as a given IDL data set B is negligible.
 - 2) The probability that a message digest (for the data on an IDL) remains the same upon a change in the data is negligible.

When the IDL is presented to a RA, the RA uses the IA's public key to verify the digital signature. The RA also computes the message digests of each of the data groups that it is interested in and compares them to the corresponding message digests stored in the machine-readable data. If the following conditions are met, the RA can consider the data groups that it is interested in to be authentic:

- a) the digital signature verifies;
- b) the calculated message digests are the same as the message digests stored in the machine-readable data;
- c) the RA is confident that the public key used to verify the digital signature belongs to the claimed IA.

If the digital signature does not verify, either an incorrect public key was used or the data on the IDL has been changed. ^{A2} Depending on the digital signature method used, it can be possible to further narrow down the cause of the non-verification. ^{A2}

This document does not prescribe methods to obtain and/or to establish trust in public keys. It is the responsibility of each RA to obtain and/or to establish trust in the public keys used to verify a digital signature on an IDL. However, informative methods and approaches to establish such trust are provided in [Annex A](#), which describes the principles for a PKI that may be used for public key distribution in the absence of one global certification authority.

This document does not prescribe methods for the generation, administration and safekeeping of key pairs. It is the responsibility of each issuing jurisdiction to ensure that keys are generated, administered and protected as necessary.

8.1.4 Hash function

8.1.4.1 Standard encoding

^{A2} For standard encoding, IA's shall choose the SHA-256, SHA-384 or the SHA-512 hash function.

SHA-256 is recommended. ^{A2}

A message digest is calculated separately for each data group present and stored in the machine-readable data (see [8.1.5.1](#)). The same hash function is used for all data groups. A message digest for a data group is calculated on the concatenation of those data elements present in the data group in the order specified in ISO/IEC 18013-2.

NOTE This approach allows reading authorities to read only those data groups it is interested in.

8.1.4.2 Compact encoding

For compact encoding, IA's shall not calculate separate message digests for each data group. Therefore, no hash function is specified for compact encoding (except as required as part of any digital signature mechanism; see [8.1.5.2](#)).

8.1.5 Signing method

8.1.5.1 Standard encoding

An IDL digital signature is generated over the concatenation of the message digests of the data groups present.

IA's may use either ECDSA or RSA as digital signature methods for standard encoding.

IA's using RSA shall use RFC 4055. RFC 4055 specifies two signature mechanisms, RSASSA-PSS and RSASSA-PKCS1-v1_5. It is recommended to generate signatures according to RSASSA-PSS, but reading authorities shall also be prepared to verify signatures according to RSASSA-PKCS1-v1_5. The minimum size of the modulus, n , shall be 1024 bits.

IA's implementing ECDSA shall use ANSI X9.62. The elliptic curve domain parameters used to generate the ECDSA key pair shall be described explicitly in the parameters of the public key, i.e. parameters shall be of type ECParameters (no named curves, no implicit parameters) and shall include the optional cofactor. ECPoints shall be in uncompressed format. The minimum size for the base point order shall be 160 bits.

In addition to EF.COM and the data groups specified in ISO/IEC 18013-2, IA's shall add the SOD to accommodate the hashes of the individual data groups (see [8.1.4.1](#)) and the digital signature of the data on the IDL. The SOD is implemented as a SignedData Type, as specified in RFC 3369 (including processing rules). The SOD shall be produced in DER format.

Table 2 — SignedData Type

Value	Type	Comments
SignedData	m	
Version	m	
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-ldsSecurityObject
eContent	m	The encoded contents of an ldsSecurityObject
certificates	o	
Crls	x	
signerInfos	m	
SignerInfo	m	
version	m	
Sid	m	
issuerandSerialNumber	c	It is recommended that IA's support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	
m = mandatory (the field shall be present); x = do not use (the field shall not be populated); o = optional (the field may be present); c = choice (the field contents is a choice from alternatives)		

Table 2 (continued)

Value	Type	Comments
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	IA's may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by a RA except to verify the signature value.
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value and any associated parameters.
signature	m	The result of the signature generation process.
unsignedAttrs	o	IA's may wish to use this field, but it is not recommended and reading authorities may choose to ignore them.
m = mandatory (the field shall be present); x = do not use (the field shall not be populated); o = optional (the field may be present); c = choice (the field contents is a choice from alternatives)		

ASN.1 sequence

```
LDSecurityObject { joint-iso-itu-t(2) international-organizations(23) icao(136) mrttd(1)
security(1) ldsSecurityObject(1) }
```

```
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
-- Imports from RFC 3280 [PROFILE], Appendix A.1
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
id-mod(0) id-pkix1-explicit(18) }

-- Constants
ub-DataGroups INTEGER ::= 16

-- Object Identifiers
id-icao OBJECT IDENTIFIER ::= {2.23.136}
id-icao-mrttd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrttd-security OBJECT IDENTIFIER ::= {id-icao-mrttd 1}
id-icao-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrttd-security 1}

-- LDS Security Object
LDSecurityObjectVersion ::= INTEGER {V0(0)}
DigestAlgorithmIdentifier ::= AlgorithmIdentifier
LDSecurityObject ::= SEQUENCE {
    version LDSecurityObjectVersion,
    hashAlgorithm DigestAlgorithmIdentifier,
    dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF DataGroupHash }

DataGroupHash ::= SEQUENCE {
    dataGroupNumber DataGroupNumber,
    dataGroupHashValue OCTET STRING }
DataGroupNumber ::= INTEGER {
    dataGroup1 (1),
    dataGroup2 (2),
    dataGroup3 (3),
    dataGroup4 (4),
    dataGroup5 (5),
    dataGroup6 (6),
    dataGroup7 (7),
    dataGroup8 (8),
    dataGroup9 (9),
    dataGroup10 (10),
```

```

dataGroup11 (11),
dataGroup12 (12),
dataGroup13 (13),
dataGroup14 (14),
dataGroup15 (15),
dataGroup16 (16) }
END

```

NOTE 1 The field `dataGroupHashValue` contains the calculated hash over the complete contents of the Data Group EF, specified by `dataGroupNumber`.

A2 NOTE 2 Data Groups 15 and 16 can be defined in future. **A2**

8.1.5.2 Compact encoding

An IDL digital signature is generated over the full data stream from the start of DG1 (including the data group delimiter between DG1 and the header) to the end of DG12 (including the data group delimiter that terminates DG12, but excluding DG.SOD, if present). The digital signature is stored in DG.SOD.

NOTE The header is not included in the information to be signed as the length information in the header pertains to **A2** DG.SOD.1 and DG.SOD.H **A2** as well.

IA's shall use ECDSA (as defined in ANSI X9.62) as a signing method for compact encoding, and in order to reduce the storage requirements for the domain parameters, shall use one of the curves specified in **A2** Table 3. **A2**

A2 DG.SOD shall consist of a concatenation of two Type 2 data groups, storing the following information: **A2**

a) DG.SOD.1: digital signature, shall be the DER encoded ASN.1 sequence of two integers, r and s :

$$\text{SEQUENCE} ::= \{ r \text{ INTEGER}, s \text{ INTEGER} \};$$

A2 b) DG.SOD.H: SHA-256 hash of IA public key certificate that contains the public key for the verification of the DG.SOD.1 signature; the hash value shall be calculated over the entire DER-encoded certificate (including the signature). **A2**

DG.SOD shall be added after DG12, as follows:

A2 [header] × [Data Group 1] × [Data Group 2] × [Data Group 3] × [Data Group 4] × [Data Group 7] × [Data Group 11] × [Data Group 12] × [DG.SOD.1 length] [digital signature] × [DG.SOD.H length] [hash value] **A2**

A2 DG.SOD.1 and DG.SOD.H shall be included. **A2** Length information is encoded using ASN.1 rules.

NOTE Reading authorities should be able to verify (or obtain) a public key (and domain parameters) from the IA using the data in other data groups **A2** (specifically the ISO issuer ID number from ISO/IEC 7812-1, and document discriminator in DG3 and the licence number and date of issue in DG1). **A2**

The curve identifier shall consist of one byte, as shown in [Table 3](#).

Table 3 — Curve identifiers

A2

Curve name in FIPS 186-4	Curve name in RFC 5639
P-224	brainpoolP224r1
P-256	brainpoolP224t1
P-384	brainpoolP256r1
P-521	brainpoolP256t1
	brainpoolP320r1

Table 3 (continued)

Curve name in FIPS 186-4	Curve name in RFC 5639
	brainpoolP320t1
	brainpoolP384r1
	brainpoolP384t1
	brainpoolP512r1
	brainpoolP512t1

A2

EXAMPLE Suppose that a compact encoded data string contains the following data groups: DG1, DG2, DG7, DG.SOD.1 and DG.SOD.H. A digital signature and public key certificate hash is included. The sequence of data groups and data group delimiters will be as follows:

[header] × [DG1] × [DG2] × × × [DG7] × × × [DG.SOD.1] × [DG.SOD.H] ¶ A2

8.2 Active authentication

8.2.1 Purpose

Active authentication uses information stored in a secure area of an SIC to confirm that the SIC and the other machine-readable data were issued together.

8.2.2 Applicability

This mechanism is limited to SICs.

8.2.3 Description

A challenge-response protocol matches the private and public keys of an SIC-individual key pair. The private key is stored in the SIC's secure memory and cannot be copied. The public key is stored as part of the signed data on the SIC (the challenge-response protocol thus has to be preceded by passive authentication). The SIC (or more specifically, the SIC operating system) can prove knowledge of the SIC-individual private key in a challenge-response protocol. In this protocol, the SIC digitally signs a challenge randomly chosen by the IS. The IS is convinced that the SIC is genuine if and only if the returned signature is correct.

NOTE Active authentication using a challenge-response protocol is open to a "traceability" attack. The challenge-response protocol does not place any limitation on the format or content of the challenge. If the challenge includes time, date, location, and a secret key, a log of challenge responses can be used to track IDLs and to prove presence (due to the inclusion of the secret key). The counterargument is that basic access protection would safeguard against unknown read attempts and that a driver's location is known in any case in those instances where an IDL is handed over for inspection.

8.2.4 Mechanism

8.2.4.1 General

The SIC-individual public key shall be stored in DG13, an additional data group specifically intended for use with the active authentication mechanism. The format of the structure (SubjectPublicKeyInfo) is specified in RFC 3280. SubjectPublicKeyInfo shall be produced in DER format as follows:

```
ActiveAuthenticationPublicKeyInfo ::= SubjectPublicKeyInfo
```

```
SubjectPublicKeyInfo ::= SEQUENCE {  
    algorithm AlgorithmIdentifier,  
    subjectPublicKey BIT STRING }
```

```
AlgorithmIdentifier ::= SEQUENCE {  
    algorithm OBJECT IDENTIFIER,  
    parameters ANY DEFINED BY algorithm OPTIONAL }
```

Allowed algorithm object identifiers and parameters are specified in RFC 3279.

Active authentication shall be performed using the ISO/IEC 7816 INTERNAL AUTHENTICATE command as defined by ISO/IEC 7816-4:2013. The input shall be a terminal-generated nonce (RND.IFD) that shall be 8 bytes in length. The SIC computes a signature which shall be sent back to the IS. The IS shall check the response and verify the signature.

8.2.4.2 Signature generation using RSA

The signature shall be computed according to ISO/IEC 9796-2 Digital Signature Scheme 1. M shall consist of M1 and M2, where M1 is an SIC-generated nonce of c-4 bits and M2 is RND.IFD. The result of the signature generation shall be the signature Σ without the recoverable message part M2.

8.2.4.3 Signature generation using ECC

An IDL supporting ECDSA shall use a prime curve with uncompressed points for this computation. In this case the output of the computation shall be the concatenation of the values r and s (r||s). The input for this computation shall be compressed with a hash algorithm with an output length shorter or equal to the length of the signature key.

NOTE The plain signature format (r||s) for the ECDSA is according to TR-03111[6].

Based on a suitable algorithm catalogue, the length of the key for ECDSA should be chosen to provide the desired security level for the physical life of the IDL.

If ECDSA based signature algorithm is used for Active Authentication by the SIC, the SecurityInfos in LDS Data Group 14 of the IDL application shall contain following SecurityInfo entry:

```
ActiveAuthenticationInfo ::= SEQUENCE {  
    protocol id-icao-mrtd-security-aaProtocolObject,  
    version INTEGER, -- MUST be 1  
    signatureAlgorithm OBJECT IDENTIFIER  
}
```

```
id-icao-mrtd-security-aaProtocolObject OBJECT IDENTIFIER ::= {  
    id-icao-mrtd-security 5 }
```

The object identifiers for signatureAlgorithm are defined in TR-03111[6]. ecdsa-plain-SHA1 and ecdsa-plain-RIPEMD160 shall not be used.

NOTE 1 See 8.1.5.1 for the definition of the Object Identifier id-icao-mrtd-security.

NOTE 2 SecurityInfos may contain entries for other protocols, e.g. Chip Authentication, Terminal Authentication, PACE.

8.2.4.4 Security mechanism indicator

SICs which implement active authentication may optionally indicate this in the security mechanism indicator (see Clause 9). The object identifier shall be id-sm-AA.

```
id-sm-AA OBJECT IDENTIFIER ::= {  
    iso(1) standard(0) driving-licence(18013) part-3(3)  
    security-mechanisms(2) 3}
```

The parameters are mandatory and shall be of type param-AA.

```
param-AA ::= SEQUENCE {
    version INTEGER,
    publicKeyDG INTEGER}
```

The version shall be set to v1(0) for this version of active authentication. The `publicKeyDG` field shall be set to the number of the data group of the active authentication public key, i.e. 13.

8.3 Scanning area identifier

8.3.1 Applicability

This mechanism is used with the non-match alert, BAP or PACE mechanisms, which collectively are applicable to SICs and 2D barcode (see [8.4](#) and [8.5](#)).

8.3.2 Description

8.3.2.1 General

The primary purpose of this mechanism is to facilitate machine assisted automatic or interactive verification procedures that match machine-readable data to human-readable data. This mechanism is not a solution on its own, but is intended for use as a component of either of the following mechanisms:

- a) non-match alert (see [8.4](#)), which checks if the machine-readable and human-readable data belong together;
- b) BAP (see [8.5](#)) or PACE (see [8.7](#)), which ensures that a PICC cannot be read without physical access to the IDL.

NOTE The BAP mechanism also performs the function of the non-match alert mechanism, but potentially at a different level of security.

The SAI demarcates the input string. The input string can be entered manually by an operator or can be read automatically using machine-readable technologies.

The SAI and any machine-readable information demarcated by it shall be adapted for reading in the B900 infrared band defined in ISO 1831:1980. Under such illumination, the printing background and any overlays within the SAI will backscatter light in a homogeneous way (i.e. the SAI shall contain no optically variable device, local deviations in properties, security features, or surface gloss exceeding natural transparent overlay gloss, which will interfere with readability). In addition, machine-readable printed information (e.g. bar codes and OCR characters) shall comply with the associated standards. The brightness of the printing background (including the effects of overlays) will not be less than 40 % compared to an ideal white surface under the same illumination. Human-readable information inside the SAI shall be rendered such that it can be read without difficulty.

The contrast ratio between character lines and the background shall be a minimum of 4:1. Any reflective layer covering the SAI area shall not further deteriorate this contrast value when illuminated under angles of incidence up to 45° and looked at under angles more than 10° outside of the nominal glance angle.

The presence of the SAI is identified as follows:

- a) If PICC access is required and the access conditions are unsatisfied (i.e. BAP or PACE is in place), the reader searches for a SAI on the IDL.
- b) If access to DG12 is available, BAP or PACE is not applicable and the non-match alert mechanism is present. DG12 may indicate the location of the SAI, alternatively, the reader searches for a SAI on the IDL.

Not more than one SAI shall be present on a single IDL.

The reference string (and the input string, when stored in a barcode) shall be encoded in accordance with ISO/IEC 8859-1:1998.

The content of the SAI can follow one of three standards, i.e. based on an existing text field, containing a dedicated text field, or containing a barcode.

8.3.2.2 SAI content based on existing text field

The SAI may be constructed around an existing field on an IDL. In this case, the SAI shall consist of a double lined rectangle as illustrated by the example in [Figure 6](#).



Figure 6 — SAI around an existing field (not to scale)

Each line shall have a thickness of $0,2 \text{ mm} \pm 0,1 \text{ mm}$, and the distance between the centre of each line shall be $0,6 \text{ mm} \pm 0,1 \text{ mm}$. The lines shall be black in colour. The clear distance between the inside line and the extremities of the input string shall be at least 1 mm.

The input string shall be printed using OCR-B size 1 or a character set with the same symbols and character shapes but using a reduced size of either 25 % or 50 % reduction of all linear dimensions compared to OCR-B size 1.

To prevent confusion about the input sequence of the characters, text within the rectangle shall be limited to one line. The data element name (if reflected on the IDL) and/or the data field reference code shall not be included within the rectangle.

In order to facilitate manual entry of the input string when needed, the input string may contain only Latin capital letters (hexadecimal range 41 to 5A of ISO/IEC 8859-1:1998), Latin small letters (hexadecimal range 61 to 7A of ISO/IEC 8859-1:1998), N characters, and the S characters shown in [Table 4](#).

NOTE 1 Latin capital letters (hexadecimal range 41 to 5A of ISO/IEC 8859-1:1998) are recommended.

NOTE 2 References to ISO/IEC 8859-1:1998 are only for purposes of identifying the characters. Encoding methods are specified elsewhere.

Table 4 — S characters allowed for SAI content based on existing field

S character	Hexadecimal number in ISO/IEC 8859-1:1998 ^a
<space>	20
–	2D
<	3C
^a Reference to ISO/IEC 8859-1:1998 is only for the purpose of identifying the characters. Encoding methods are specified elsewhere.	

The reference string shall not contain any space characters (i.e. hexadecimal character '20' of ISO/IEC 8859-1:1998). Thus, the IS shall delete all space characters (hexadecimal code 20 of ISO/IEC 8859-1:1998) from the input string before further processing.

IA's should carefully consider the level of entropy of existing fields before use within the SAI. Any rules followed in the construction of the field will decrease the entropy.

IA's considering the use of an SAI based on an existing field should keep in mind that a check digit is not provided for in this case.

EXAMPLE See [Figure 7](#).

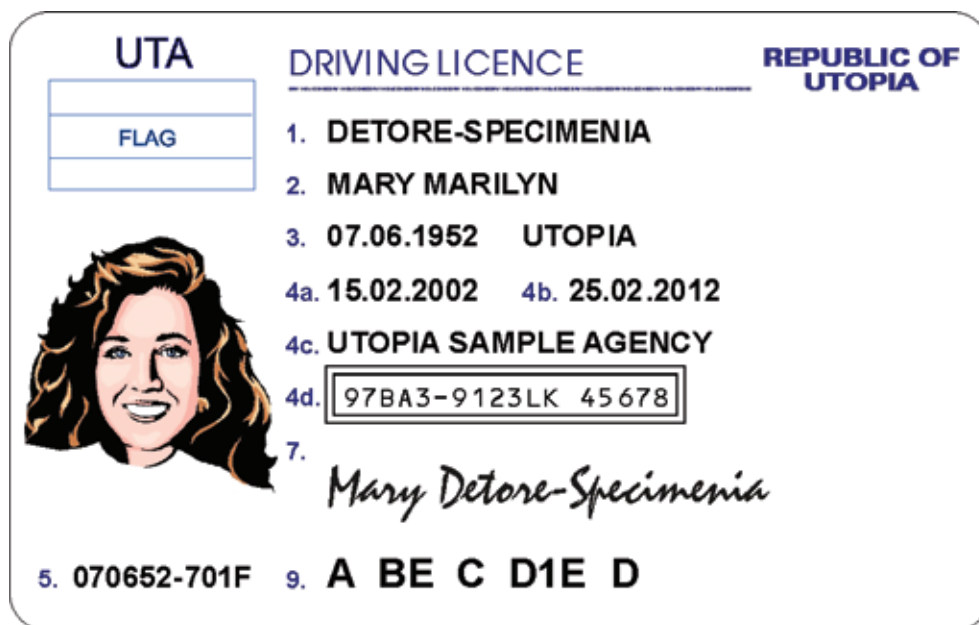


Figure 7 — Existing data field on portrait side of IDL designated as input string (not to scale)

8.3.2.3 SAI content consisting of a dedicated text field

A dedicated field (i.e. a field designed specifically for this purpose) may be used within a SAI. In this case, the SAI shall consist of a rectangle constructed by a black single line with a thickness of $0,65 \text{ mm} \pm 0,1 \text{ mm}$. The clear distance between the line and the extremities of the printed input string shall be at least 1 mm.

EXAMPLE See [Figure 8](#).

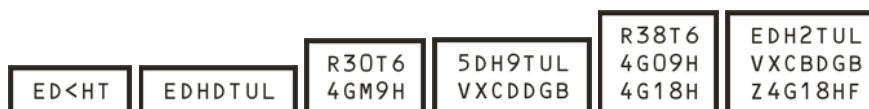


Figure 8 — SAI around a dedicated field (not to scale)

The content of the SAI shall comply with the following requirements:

- the text shall be limited to the set of ICAO MRZ characters, i.e. 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z <;
- an odd number of characters per line shall be used;
- if characters are printed in more than one line, each line shall have the same number of characters;
- a line shall not have more than seven characters;
- no more than three lines shall be used;
- the text shall be printed using OCR-B font at 100 % of OCR-B size 1;
- the middle character of each line shall be reserved for a check digit. Before adding the check digit(s), the input string may have the following lengths:
 - for one line only, string lengths of 4 or 6 characters are permitted;
 - for two lines, string lengths of 8 or 12 characters are permitted;

- 3) for three lines 12 or 18 characters are permitted.

To construct an input string (with check digits) consisting of i lines, the input string (before check digits are added) is parsed into i parts of equal length. The leftmost part is used to form line 1, the following parts each to form an additional line. Each part is split in the middle into a left and a right subsection. The left subsection forms the leftmost part of the corresponding line, the right subsection forms the rightmost part of the line. An additional character position is inserted in the middle of each line (for the check digit). The value of the check digit of each line will be calculated as explained further below.

For the purpose of check digit calculation, each character in the input string (before the check digits are added) represents a numerical value V_C defined by the formula $V_C = E_C$, where E_C is a unique number allotted to each character value, as defined in [Table 5](#).

Table 5 — Character numerical equivalents

Char	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	I
E_C	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Char	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	<	
E_C	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	

If line 1 is the only line, then the unique check digit will be calculated as follows:

- A check sum S is calculated as $S = \sum V_{Ci}$, where i runs from 0 to $n-1$ and V_{Ci} indicates the respective value V_C for the character in the i -th position in the input string of length n , counted from right to left, starting with position 0 for the rightmost character.
- From S , the corresponding check digit c is calculated as $c = S$ modulo 37; (integer remainder when dividing S by 37).

If there are two or three lines, then the check digits c_1 for line one and c_2 for line two will be calculated as follows:

- A check sum S_V is calculated over the entire input string (before it is split into lines and before adding the check digits) as $S_V = \sum V_{Ci}$, where i runs from 0 to $n-1$ and indicates the character in the i -th position in the input string of length n , counted from right to left, starting with position 0 for the rightmost character.
- A check sum S_P is calculated over the entire input string (before it is split into lines, and before adding the check digits) as $S_P = \sum (V_{Ci} * i)$, where i runs from 0 to $n-1$ and i indicates the i -th position number in the input string of length n , counted from right to left, starting with position 0 for the rightmost character, and V_{Ci} indicates the respective value for the character in the i -th position.
- Check digits c_1 and c_2 are calculated as $c_1 = (S_V \text{ modulo } 37)$ and $c_2 = (S_P \text{ modulo } 37)$, respectively.

In the case of exactly three lines, the inserted character c_3 in the centre of line three will represent the version number and will be set to "1" for this version of the standard. Version numbers are not supported for less than three lines.

When printed on an IDL, lines are numbered from top to bottom, as shown in [Figure 9](#).



Figure 9 — Line configuration (not to scale)

EXAMPLE Input string for [Figure 9](#) is EDHTULVXCDGBZ4G8HF.

Input string	E	D	H	T	U	L	V	X	C	D	G	B	Z	4	G	8	H	F
E_C	14	13	17	29	30	21	31	33	12	13	16	11	35	4	16	8	17	15
i	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
$V_{Ci} * i$	238	208	255	406	390	252	341	330	108	104	112	66	175	16	48	16	17	0

$$S_V = 335$$

$$S_P = 3082$$

Check digit	Numeric value	Code value
c1	2	2
c2	11	B

$$c3 = 1$$

The input string submitted as input to the non-match alert or BAP mechanisms is the input string inclusive of the check digit, i.e. the concatenation $s_1 + s_2 + s_3$ where s_i is the string in line i of the corresponding input string, including the respective check digit and read from the left to the right, with i ranging from 1 to a maximum of 3.

NOTE Mathematically, the check digit scheme allows identifying any single digit reading error in the case of a one-line input string and to correct any single digit reading error, as well as identifying any double error in the case of a two-line or three-line input string. Less than 3 % of any other statistical reading error may pass inadvertently. This is only true if adequate measures are taken on the side of the reading equipment to make use of the information offered by the check digit scheme.

It is recommended that the minimum entropy of the input string be 40 bits or more (before addition of the check digits). The use of random data is recommended.

NOTE IA's may consider imposing restrictions on allowable content of input strings to meet local requirements, e.g. to address the "nasty word" problem, or to limit the value range of practically existing check digits (i.e. numerical characters only). Methods exist that allow enforcement of such restrictions without violation of the rules set out above. The use of such methods is left to the discretion of the IA's. Attention is drawn to the fact that such restrictions will reduce the entropy of the input string.

EXAMPLE See [Figure 10](#).