INTERNATIONAL STANDARD

ISO/IEC 18013-3

Second edition
2017-04

AMENDMENT 2
2023-04

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

Part 3: **Access control, authentication and integrity validation**

AMENDMENT 2: Updates for passive authentication

Reference number
ISO/IEC 18013-3:2017/Amd. 2:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, SC 17, *Cards and security devices for personal identification*.

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

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

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

Part 3: **Access control, authentication and integrity validation**

AMENDMENT 2: Updates for passive authentication

Page 2, Clause 2 Normative references

Replace

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

with

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

Page 4, subclause 3.11

Replace

Note 1 to entry See 8.1.

with

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

Page 12, subclause 8.1

Replace

8.1 Passive authentication

with

8.1 Passive authentication (ver 02)

Page 12, subclause 8.1.1

Add the following paragraph at the end of the subclause:

> 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.

Page 13, subclause 8.1.3

In the third to last paragraph, second sentence, replace

“...it may be possible to further narrow down the cause of the non-verification.”

with

“...it can be possible to further narrow down the cause of the non-verification.”

Page 13, subclause 8.1.4.1

In the first paragraph, delete “SHA-1, SHA-224,”.

In the second paragraph, delete "SHA-1 remains for compatibility with ICAO Doc 9303-1."

Page 16, subclause 8.1.5.1

In NOTE 2 replace

“Data Groups 15 and 16 may be defined in future.”

with

“Data Groups 15 and 16 can be defined in future.”

Page 16, subclause 8.1.5.2

In the first NOTE replace "DG11" with "DG.SOD.1 and DG.SOD.H".

In the second paragraph, replace "FIPS 186-2, Appendix 6” with "Table 3".

In the third paragraph, delete “and one Type 1 data group”.

In the lettered list, replace b) with:

> “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);”

In the lettered list, delete c).

Under "DG.SOD shall be added after DG12, as follows:", replace with:

> “[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]”

Under the content of DG.SOD, replace “The inclusion of DG.SOD.2 and DG.SOD.3 (as a pair) is optional.” with "DG.SOD.1 and DG.SOD.H shall be included."

In the second NOTE replace “specifically the ISO issuer ID number and document discriminator in DG3 and the licence number and date of issue in DG1” with “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”.

Replace Table 3 with:

Curve name in FIPS 186-4	Curve name in RFC 5639
P-224	brainpoolP224r1
P-256	brainpoolP224t1
P-384	brainpoolP256r1
P-521	brainpoolP256t1
	brainpoolP320r1
	brainpoolP320t1
	brainpoolP384r1
	brainpoolP384t1
	brainpoolP512r1
	brainpoolP512t1

Replace the EXAMPLE with:

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] ¶

Page 46, A.5.1, second list b) second paragraph

Replace

"For compact encoding, the appropriate public document key is identified by comparing the issue date of the IDL with the “valid for signing from” and “valid for signing until” dates of the available public document keys of the IA."

with

"For compact encoding, the appropriate public document key can be identified using the hash value of the signer certificate."

Bibliography

Add new entry

[13] ISO/IEC 7812-1, *Identification cards — Identification of issuers — Part 1: Numbering system*

After Annex F

Add new Annex G.

Annex G
(informative)

Passive authentication (version 01)

G.1 General

This annex defines the deprecated passive authentication (ver 01) 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.

G.2 Purpose

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

G.3 Applicability

Passive authentication is applicable to all machine-readable technologies.

G.4 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. Depending on the digital signature method used, it can be possible to further narrow down the cause of the non-verification.

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.

G.5 Hash function

G.5.1 Standard encoding

For standard encoding, IAs shall choose the SHA-1, SHA-224, SHA-256, SHA-384 or the SHA-512 hash function.

SHA-256 is recommended. SHA-1 remains for compatibility with ICAO Doc 9303-11.

A message digest is calculated separately for each data group present and stored in the machine-readable data (see G.6.1). 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.

G.5.2 Compact encoding

For compact encoding, IAs 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 G.6.2).

G.6 Signing method

G.6.1 Standard encoding

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

IAs may use either ECDSA or RSA as digital signature methods for standard encoding.

IAs 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.

IAs 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, IAs shall add the SOD to accommodate the hashes of the individual data groups (see G.5.1) and the digital signature of the data on the IDL. The SOD is implemented as a SignedData Type in Table G.1, as specified in RFC 3369 (including processing rules). The SOD shall be produced in DER format.

Table G.1 — 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 IAs support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	IAs can 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	IAs can use this field, but it is not recommended and reading authorities can 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

```
LDSSecurityObject { joint-iso-itu-t(2) international-organizations(23) icao(136) mrtd(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-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 1}

-- LDS Security Object
LDSSecurityObjectVersion ::= INTEGER {V0(0)}
DigestAlgorithmIdentifier ::= AlgorithmIdentifier
LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   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`.

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

G.6.2 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 1 The header is not included in the information to be signed as the length information in the header pertains to DG11 as well.

IAs 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 FIPS 186-2:2000, Appendix 6.

DG.SOD shall consist of a concatenation of two Type 2 data groups and one Type 1 data group, storing the following information:

a) DG.SOD.1: digital signature, shall be the DER encoded ASN.1 sequence of two integers, r and s: SEQUENCE ::= { r INTEGER, s INTEGER };

b) DG.SOD.2: public key; octet string representation of the public point in uncompressed form according to X9.62;