DRAFT AMENDMENT
ISO/IEC 18013-3: DAM 1

ISO/IEC JTC **1**/SC **17** Secretariat: **BSI**

Voting begins on:
2015-08-17

Voting terminates on:
2015-11-17

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

Part 3:
Access control, authentication and integrity validation

AMENDMENT 3: PACE

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

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

AMENDEMENT 3: .

ICS: 35.240.15

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC 18013-3:2009/DAM 3:2015(E)

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

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.

Amendment 3 to ISO/IEC 18013-3:2009 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

It describes the optional PACE mechanism enabling 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 ISO-compliant driving licence 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. In the interest of interoperability of cards used for personal identification, this amendment further simplifies the authentication protocols in the IDL Active Authentication is harmonised with other ISO standards, whilst BAP configurations 2, 3 and 4, as well as EAP are no longer supported by this standard.

Information Technology — Personal Identification — ISO Compliant Driving Licence — Part 3: Access control, authentication and integrity validation

AMENDMENT 3:
PACE and simplification of authentication protocols

Page 1, Normative references

Insert the following referenced document:

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

Page 3, Terms and Definitions

In clause 4.7 replace:

“basic access protection“ by “basic access protection or PACE“.

Insert the following definition after clause 4.27:

4.28
PACE
alternative mechanism to BAP to confirm that an inspection system (IS) has physical access to a secure integrated circuit (SIC) 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 As stated in TR-PACE, PACE refers to PACE v2.

NOTE 2 See 8.8 and Annex H

Page 6, Abbreviated terms

Insert the following abbreviation:

MF	master file
PACE	password authenticated connection establishment

Page 11, Table 1

Replace “BAP” by “BAP or PACE”

Page 19, 8.2.4.3 Signature generation using ECC

Replace the text of this clause with the following:

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 [15].

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 [15]. 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.

Page 19, 8.3.1 Applicability

Replace “non-match alert or BAP” by “non-match alert, BAP or PACE”.

Page 19, 8.3.2.1 General

Replace “BAP” by “BAP or PACE”.

AMD1, Page 1, 8.3.2.5 SAI consisting of an IDL MRZ

Replace “BAP” by “BAP or PACE”

AMD1, Page 3, 8.3.2.5.3 Use of the IDL MRZ as a BAP input string

In Table Amd1.1, replace the content of the *Specification* column against the row for *IDL MRZ character position* "2" (*Data element* "Configuration") with the following:

The second character shall designate the configuration as follows:
“1” for IDL SIC protected with BAP configuration 1
"P" for IDL SIC protected with PACE only (i.e. without BAP support).
“N” for IDL SIC protected with non-match alert
“<” for an MRZ does not contain a reference string
Any other characters are reserved for future use.

Note: If the second character of the MRZ is set to 1, PACE may be supported in addition to BAP configuration 1.”

AMD2, page iii, Foreword

Replace the last paragraph by:

“It describes the optional Extended Access Control (EAC) v1 mechanism as a replacement for Extended Access Protection (EAP), enabling access control to sensitive biometric data stored on the integrated circuit.”

AMD2, page 1, clause "Page 6, Terms and Definitions"

Replace in the definition of the EACv1 protocol

"alternative protocol to EAP used to"

by "protocol used to"

AMD2, page 1, clause "Page 11, Table 1"

Delete “EAP or”

AMD2, page 2, 8.7.1 Purpose

Replace "EACv1 is an alternative to EAP and consists of:"

by "EACv1 replaces EAP. This standard no longer supports EAP. EACv1 consists of:"

AMD2, page 2, 8.7.3 Description and mechanism

After the first sentence insert the following sentences:

“This standard only supports EACv1 Chip Authentication with the ECDH mechanism.

This standard only supports EACv1 Terminal Authentication with the ECDSA mechanism.”

Replace b) by:

b) If BAP is performed before EACv1, the driving licence number, as it appears in DG1, shall be used as SIC identifier (ID_{SIC}). If PACE is performed before EACv1, the SIC identifier (ID_{SIC}) is computed from the SIC's ephemeral PACE public key, i.e. ID_{SIC}=Comp(PK_{SIC}).

Delete items e) and f).

AMD2, page 2, clause “Page 32, Table 9”

Delete “Extended access protection or”

AMD2, page 2, clause “Page 32, Figure 15”

Delete “Extended access protection or”

AMD2, page 2, clause “Page 33”

Delete “Extended access protection or”

Delete “in C.3.4 for EAP and”

AMD2, page 3, G.1 Introduction

Replace the last sentence by “The support of EACv1 requires a BAP configuration 1 or PACE configuration for the IDL.”

Insert the following clause after clause 8.7.3 (AMD2):

8.8 PACE

8.8.1 Purpose

The PACE protocol confirms that an IS has physical access to a SIC before the IS is allowed to access to the data stored on the chip. Once access is authorized, PACE protects the subsequent communication by a secure channel between SIC and IS. The PACE protocol can be used as an alternative to BAP and allows various implementation options (mappings, input strings, algorithms).

8.8.2 Applicability

This mechanism is applicable only to SICs.

8.8.3 Description and mechanism

PACE is specified in Annex H. This standard only supports PACE with ECDH generic mapping. The first byte of the input string shall be '50' ("P") if PACE is used as a stand-alone protocol, ie not used in conjunction with BAP configuration 1.

If PACE is used to gain access to the SIC, the SIC shall deny access to the content of the IDL application by its interface unless the IS can prove that it is authorized to access the SIC. This proof is given in a password authenticated Elliptic Curve Diffie Hellman key agreement protocol where the IS proves its knowledge of a SIC-specific key Kπ, which is derived from the input string.

After the IS has been authenticated successfully, the SIC shall enforce encryption and message authentication of the communication channel between the SIC and the IS by Secure Messaging techniques.

PACE shall be performed in the master file (MF) of the SIC. The SIC provides the relevant `SecurityInfos` in a transparent EF.CardAccess contained in the MF (and additionally in DG14 contained in the IDL application). Due to the execution on MF level, PACE provides an application independent authentication between IS and SIC that may also be used to get access to potential other domestic applications on the SIC.

NOTE See TR-PACE sections 2.2 and 3.1.5.

8.8.4 PACE relative to BAP

PACE differs from BAP in the following respects:

a) PACE introduces a mandatory master file (MF) structure.

b) PACE requires an EF.CardAccess file within the MF.

c) Security conditions are established at MF level for PACE.

d) The IDL application is selected by secure messaging using session keys derived in accordance with the PACE procedure.

In relation to BAP, the PACE protocol has the following advantages:

a) Strong session keys are provided independent of the strength of the input string.

b) The entropy of the input string(s) used to authenticate the IS can be very low (e.g. 6 digits are sufficient in general).

c) The binding between PACE and a Terminal Authentication is universal and does not depend on the input string.

The BAP logo in 8.5 may be used to denote the presence of an input string for PACE.