INTERNATIONAL STANDARD

ISO/IEC 18013-3

First edition
2009-03-01

AMENDMENT 2
2014-12-01

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

Part 3: Access control, authentication and integrity validation

AMENDMENT 2: Extended Access Control v1

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 2: Extended Access Control v1

Reference number
ISO/IEC 18013-3:2009/Amd.2:2014(E)

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

Published in Switzerland

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 2 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 Extended Access Control (EAC) v1 mechanism as an alternative and further option in addition to Extended Access Protection (EAP), enabling access control to sensitive biometric data stored on an integrated circuit.

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

Part 3:
Access control, authentication and integrity validation

AMENDMENT 2: Extended Access Control v1

Page 1, Normative references

Insert the following referenced documents:

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.

Page 6, Terms and Definitions

Insert the following definition after 4.26:

4.27

Extended Access Control v1

EACv1

alternative protocol to EAP used to limit access to optional signature and biometric data groups

Note 1 to entry: See 8.7 and Annex G.

Page 6, Abbreviated terms

Insert the following abbreviations:

EACv1 extended access control v1

IFD interface device

RFU reserved for future use

Page 11, Table 1

Replace "EAP" by "EAP or EACv1"

Page 30

Insert the following clause after 8.6.3:

8.7 Extended Access Control v1

8.7.1 Purpose

EACv1 is an alternative to EAP and consists of:

a) Chip authentication, which provides for authentication of the SIC and strong secure messaging.

b) Terminal authentication, which provides for conditional authenticated access to data groups.

8.7.2 Applicability

This mechanism is applicable only to SICs.

8.7.3 Description and mechanism

EACv1 is specified in Annex G. The following rules shall be used in the application of EACv1 for an IDL:

a) The SIC's key agreement public key(s) shall be stored in DG14, formatted in accordance with BSI/TR 03110-3.

b) When EACv1 is used in combination with BAP, the input string shall be used as the SIC identifier.

c) Strong secure messaging (established using chip authentication as described in BSI/TR 03110) shall be active before terminal authentication can take place.

d) DG14 shall be accessible without terminal authentication.

e) Only BAP-1 is allowed as possible preceding authentication for EACv1.

f) EAP and EACv1 shall not be supported simultaneously.

Page 32, Table 9

Replace "Extended access protection" by "Extended access protection or EACv1"

Page 32, Figure 15

Replace "Extended access protection" by "Extended access protection or EACv1"

Page 33

Replace 10.4 with the following:

10.4 EF.DG14 Extended access protection or EACv1 (short EF identifier = '0E', Tag = '6E')

DG14 is defined in C.3.4 for EAP and in Annex G for EACv1.

Annex G
(normative)

Extended Access Control v1

G.1 Introduction

This annex describes an additional protocol for conditional access to an application that stores data in data groups according to a LDS.

EACv1 is specified by the BSI in the Technical Guidelines TR-03110-1 v2.10 and in TR-03110-3 v2.10.

The support of EACv1 requires a BAP-1 configuration for the IDL.

G.2 Changes to TR-03110-1 v2.10

This section describes the changes that apply to TR-03110-1 v2.10 to support the IDL.

G.2.1 General

For BAC, read BAP.

For DG2, read DG6.

For DG3, read DG7.

For DG4, read DG8.

For DG15, read DG13.

For ePassport, read Driving Licence.

For ePassport Application, read Driving Licence Application.

For ICAO compliant ePassport Application, read Driving Licence Application.

For ICAO/EAC1-compliant ePassport Application, read Driving Licence Application.

For ICAO Active Authentication, read Active Authentication.

For MRTD, read IDL.

For MRTD chip, read SIC.

For MRZ, read input string.

For PCD, read IS/IFD.

For PICC, read SIC.

G.2.2 Clauses not applicable to IDL

The following clauses of TR-03110-1 v2.10 are not applicable to the IDL:

a) Clause 1: Introduction, with the exception of clause 1.5 (Requirements for IDL Chips and Terminals) and clause 1.6 (Terminology) that are applicable to the IDL.

b) Clause 2.4.2: Standard Inspection Procedure

c) Clause 3.2: BAC

d) Clause 3.3: PACE

e) Annex A: Basic Access Control (Informative)

G.2.3 Clause 2.1: Driving Licence Application

The Driving Licence Application is defined by ISO/IEC 18013.

G.2.4 Clause 2.2: Inspection System

For the entire clause, read:

The Standard Inspection Procedure is not applicable to the IDL and only one inspection procedure is supported, namely the Advanced Inspection Procedure. Consequently the Basic Inspection System is not applicable to the IDL, only the Extended Inspection System is supported.

For Table 3, read the following table:

Table 3 — Data Groups of the Driving Licence Application

DG	Content	Read/ Write	Mandatory/ OptionalText a	Access Control	
				BAP	EACv1
DG1	Text data elements	R	m	m	x
DG2	Licence Holder details	R	o	m	x

a As defined in ISO/IEC 18013-2 and ISO/IEC 18013-3

b Although named Extended Access Control, the content in this annex is defined as EACv1 in 10.4

Table 3 *(continued)*

DG	Content	Read/ Write	Mandatory/ OptionalText a	Access Control	
				BAP	EACv1
DG3	Issuing Authority details	R	o	m	x
DG4	Portrait Image of licence holder	R	o	m	x
DG5	Signature	R	o	m	r
DG6	Facial biometric template	R	o	m	o
DG7	Finger biometric template	R	o	m	r
DG8	Iris biometric template	R	o	m	r
DG9	Other biometric template	R	o	m	o
DG10	Reserved for future use	R	o	m	o
DG11	Domestic application data	R	o	m	o
DG12	Non-Match Alert	R	o	m	x
DG13	Active Authentication	R	o	m	x
DG14	Extended Access ControlText b	R	o	m	x
SOD	Security Object	R	m	m	x

a As defined in ISO/IEC 18013-2 and ISO/IEC 18013-3

b Although named Extended Access Control, the content in this annex is defined as EACv1 in 10.4

G.2.5 Clause 2.3: Passwords

For the entire clause, read:

The Driving Licence Application does not support PACE. Consequently only one "password" is supported for BAP, namely the input string, and the Card Access Number (CAN) is not applicable.

G.2.6 Clause 2.4: Inspection Procedures

For the entire clause, read:

The Standard Inspection Procedure is not applicable to the IDL and only one inspection procedure is supported, namely the Advanced Inspection Procedure.

G.2.7 Clause 2.4.1: Open Driving Licence Application

For the entire clause, read:

The Driving Licence Application does not support PACE. Consequently Step 1 (Read CardAccess) and Step 2 (PACE) of the opening procedure are not applicable to the IDL.

G.2.8 Clause 3: Protocol Specifications

For the entire clause, read:

The Driving Licence Application does not support PACE.

G.2.9 Clause 3.5: Terminal Authentication Version 1

For the MRTD chip's Document Number as contained in the MRZ, read the input string.

When EACv1 is used in combination with BAP, the input string of the IDL is used as the ID_{PICC}.

G.3 Changes to TR-03110-3 v2.10

TR-03110-3 v2.10 is a “toolbox” similar to ISO/IEC 7816 from which only the “tools” applicable to the application in hand is used. Hence the “tools” in TR-03110-3 v2.10 that are not applicable to EACv1 are not listed for exclusion in this section.

This section describes the changes that apply to TR-03110-3 v2.10 to support EACv1 for the IDL.

G.3.1 General

For BAC, read BAP.

For DG2, read DG6.

For DG3, read DG7.

For DG4, read DG8.

For DG15, read DG13.

For ePassport, read Driving Licence.

For ePassport Application, read Driving Licence Application.

For MRTD, read IDL.

For MRTD chip, read SIC.

For MRZ, read input string.

For PCD, read IS/IFD.

For PICC, read SIC.

G.3.1 Clause B.8: Reading Data Groups

Replace the content of this clause with the following:

In accordance with ISO/IEC 18013-3 any unauthorized access to EACv1 protected data groups SHALL be denied and the SIC MUST respond with status bytes 0x6982 (“Security status not satisfied”).

G.3.2 Clause C.4.1: Inspection Systems

Successful Terminal Authentication shall grant access to all data groups protected by EACv1 with the exception of DG7 and DG8, each of which requires effective authorisation.

For Table 20, read the following table:

Table 20 — Authorisation of Inspection Systems

7	6	5	4	3	2	1	0	Description
x	x							**Role**
1	1							CVCA
1	0							DV (official domestic)
0	1							DV (official foreign)
0	0							Inspection System
-	-	x	x	x	x	x	x	**Access Rights**
-	-	x	x	x	x	-	-	RFU