DRAFT AMENDMENT

ISO/IEC 18013-4:2011/DAM 1

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

Voting begins on:
2016-03-24

Voting terminates on:
2016-06-23

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

Part 4:
Test methods

AMENDMENT 1: Extended access control v1 & pace

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

Partie 4: Méthodes d'essai

AMENDEMENT 1: .

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 18013-4:2011/DAM 1:2016(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 1 to ISO/IEC 18013-4:2011 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

This amendment prescribes requirements for testing the compliance of the 1 line MRZ machine readable zone, Extended Access Control v1 mechanism, PACE protocol and the related data structures on an IDL with the requirements of ISO/IEC 18013-2 and ISO/IEC 18013-3 including ISO/IEC 18013-3:2009/AMD1, ISO/IEC 18013-3:2009/AMD2 and ISO/IEC 18013-3:2009/AMD3.

Information Technology — Personal identification — ISO-compliant driving licence — Part 4: Test methods

AMENDMENT 1: **Extended Access Control v1 & PACE**

Page 2, Normative references

Insert the following referenced documents:

BSI Technical Guideline TR-03105-3.2*, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EACv1) – Tests for Security Implementation – Version 1.4.1 – 2014-04-06*

BSI *Technical Guideline* TR-03111, *Elliptic Curve Cryptography (ECC) – Version 2.0 – 2012-06-28 [BSI TR-03111]*

ICAO Technical Report – *Supplemental Access Control for Machine Readable Travel Documents – Version 1.01 – 2010 [TR-PACE]*

ICAO Technical Report – *RF Protocol and Application Test Standard for eMRTD – Part 3 Version 2.07 – 2014-11-30 [TR-ICAO Part 3]*[1]

Page 2, Abbreviated terms

Insert the following abbreviations:

FID	file identifier
SFI	short EF identifier

[1] Final publication expected before this amendment is published at which time the reference will be updated if necessary

Page 10, Table A.1

Insert the following rows:

Profile	Information for test setup	Applicable (YES or NO)	Protection level (Plain, BAP or EAP)
EAC	Extended Access Control v1		
PACE	Password Authenticated Connection Establishment		
MRZ	Machine Readable Zone		

Page 16, Test Case SE_LDS_COM_011

Replace the entire table with the following table:

Test Case-ID	SE_LDS_COM_011
Purpose	This test checks the encoding of the EAP mechanism in the SMI.
Version	1.2
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 18013-3:2009
Profile	SMI, EAP
Preconditions	1. EF.COM has been retrieved from the IDL. 2. The SMI has been retrieved from EF.COM. 3. The SMI has a valid DER TLV structure.
Test Scenario	Perform the following checks for the security mechanism in the SMI that specifies the EAP mechanism: 1. Check the presence of the mechanism id-sm-EAP. 2. Check the encoding of the parameters for the mechanism id-sm-EAP. 3. Check the version of the EAP parameters. 4. Check the chipAuthPublicKeyDG field of the EAP parameters. 5. Check the consistency of chipAuthPublicKeyDG and the Taglist in EF.COM. 6. Check the smConfiguration field of the EAP parameters. 7. Check the currentTrustRoot field of the EAP parameters. 8. Check the alternateTrustRoot field of the EAP parameters.
Expected Results	1. The mechanism id-sm-EAP shall be present. 2. The parameters for the mechanism id-sm-EAP shall be encoded as specified in ISO/IEC 18013-3:2009, C.6. 3. The version shall be '00' (V1). 4. The chipAuthPublicKeyDG field shall be set to '0E' (DG14). 5. The data group indicated by chipAuthPublicKeyDG shall occur in the Taglist.

	6. The smConfiguration field shall use one of the identifiers from ISO/IEC 18013-3:2009, B.8 (i.e. oid_bap_config_1, oid_bap_config_2, oid_bap_config_3, or oid_bap_config_4). 7. The currentTrustRoot field shall be set to the current trust root's SKID, formatted as in the corresponding card-verifiable certificate, including the preceding length byte. The currentTrustRoot field shall be 17 bytes length. If the resulting octet string is shorter than 17 bytes, it shall be padded to the right with ‘00’ bytes. 8. The alternateTrustRoot field shall be set to the alternate trust root's SKID, formatted as in the corresponding card-verifiable certificate, including the preceding length byte. The alternateTrustRoot field shall be 17 bytes length. If the resulting octet string is shorter than 17 bytes, it shall be padded to the right with ‘00’ bytes.

Page 16

Insert the following clauses after clause A.3.1.12:

A.3.1.13 Test case SE_LDS_COM_013

Test – ID	SE_LDS_COM_013
Purpose	This test checks the encoding of the EAC mechanism in the SMI.
Version	1.2
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 18013-3:2009/AMD2 Annex G.4
Profile	SMI, EAC
Preconditions	1. EF.COM has been retrieved from the IDL. 2. The SMI has been retrieved from EF.COM. 3. The SMI has a valid DER TLV structure.
Test scenario	Perform the following checks for the security mechanism in the SMI that specifies the EAC mechanism. 1. Check the presence of the mechanism id-TA. 2. Check the encoding of the parameters for the mechanism id-TA. 3. Check the version of the EAC parameters. 4. Check the data groups.
Expected results	1. The mechanism id-TA shall be present. 2. The parameters for the mechanism id-TA shall be encoded as specified in ISO/IEC 18013-3:2009/AMD2 Annex G.4. 3. The version shall be ‘01’. 4. The data groups shall only contain any combination of the following integers: '05', '06', '07', '08', '09', '0A', '0B'.

A.3.1.14 Test case SE_LDS_COM_014

Test – ID	SE_LDS_COM_014
Purpose	This test checks the presence of the EAC mechanism in the SMI.
Version	1.2
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 18013-3:2009/AMD2 Annex G.4
Profile	SMI EAC NOT supported or EAP
Preconditions	1. EF.COM has been retrieved from the IDL. 2. The SMI has been retrieved from EF.COM. 3. The SMI has a valid DER TLV structure.
Test scenario	1. Check the presence of the mechanism id-TA if EAC is NOT supported.
Expected results	1. The mechanism id-TA shall be absent.

A.3.1.15 Test case SE_LDS_COM_015

Test – ID	SE_LDS_COM_015
Purpose	This test checks the presence of the EAP mechanism in the SMI.
Version	1.2
References	ISO/IEC 18013-2:2008, Annex C ISO/IEC 18013-3:2009/AMD3 Clause H.2.3
Profile	SMI, PACE
Preconditions	1. EF.COM has been retrieved from the IDL. 2. The SMI has been retrieved from EF.COM. 3. The SMI has a valid DER TLV structure.
Test scenario	1. Check the presence of the mechanism id-ICAuth.
Expected results	1. The mechanism id-ICAuth shall be absent.

Page 38, Test Case SE_LDS_DG5_002

Replace the entire table with the following table:

Test Case-ID	SE_LDS_DG5_002
Purpose	This test checks the encoding of EF.DG5 element length.
Version	1.2
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG5
Preconditions	1. EF.DG5 has been retrieved from the IDL.

Test Scenario	1. Analyze the encoding of the bytes that follow the template tag. 2. Verify the length of the EF.DG5 object.
Expected Results	1. The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2. The encoded length shall match the size of the given EF.DG5 object.

Page 38, Test Case SE_LDS_DG5_003

Replace the entire table with the following table:

Test Case-ID	SE_LDS_DG5_003
Purpose	This test checks the Type of Image (Tag '89') present in EF.DG5.
Version	1.2
References	ISO/IEC 18013-2:2008, Annex C
Profile	DG5
Preconditions	1. EF.DG5 has been retrieved from the IDL.
Test Scenario	1. Search for the Type of Image (Tag '89') inside EF.DG5. 2. Check the length of the Type of Image data element. 3. Check the value of the Type of Image data element.
Expected Results	1. Tag '89' shall be present. 2. The length of the Type of Image data element shall be 1 byte. 3. The Type of Image data element shall be one of the values indicated in ISO/IEC 18013-2:2008, 8.5 (i.e. '02', '03', or '04').

Page 38, Test Case SE_LDS_DG5_004

Replace the entire table with the following table:

Test Case-ID	SE_LDS_DG5_004
Purpose	This test checks the Image of Signature or Mark (Tag '5F 43') present in EF.DG5.
Version	1.2
References	ISO/IEC 18013-2:2008, Annex C, Annex E
Profile	DG5
Preconditions	1. EF.DG5 has been retrieved from the IDL.
Test Scenario	1. Search for the Image of Signature or Mark (Tag '5F 43') inside EF.DG5. 2. Check the encoded length of the Image of Signature or Mark data element. 3. Check the length of the Image of Signature or Mark data element.

	4. Verify the type of Image. 5. Verify consistency of Image type with encoded element.
Expected Results	1. Tag '5F 43' shall be present. 2. The bytes that follow the Tag '5F 43' shall contain a valid length encoding (according to ASN.1 encoding rules). 3. The encoded length shall match the size of the Image of Signature or Mark data element. 4. The type of Image shall match one of the values in Table E.1 in ISO/IEC 18013-2:2008. 5. The encoded Image format shall match the image type stated in the Type of image field.

Page 82, Test Case SE_LDS_DG12_004

Replace the entire table with the following table:

Test Case-ID	SE_LDS_DG12_004
Purpose	This test checks the encoding of the SAI Input Method (Tag '81') present in EF.DG12.
Version	1.2
References	ISO/IEC 18013-3:2009
Profile	NMA
Preconditions	1. EF.DG12 has been retrieved from the IDL.
Test Scenario	1. Search for the SAI Input Method (Tag '81') inside EF.DG12. 2. Check the encoded length of the SAI Input Method data element, if present. 3. Check the length of the SAI Input Method data element. 4. Check the value of the SAI Input Method. 5. Check the value of the SAI Input Method. 6. If the SAI Input Method starts with '02', check the presence of byte 2 of the SAI Input Method. 7. Check the value of byte 2 of the SAI Input Method. 8. Check the value of byte 3 of the SAI Input Method, if present. 9. Check the value of the bytes 4 - 7 of the SAI Input Method, if present. 10. Check the consistency of the bytes 4 and 6 of the SAI Input Method, if present. 11. Check the consistency of the bytes 5 and 7 of the SAI Input Method, if present.
Expected Results	1. Tag '81' may be present and shall not occur more than once. 2. The encoded length shall be '01', '02', or '07'. 3. The encoded length shall match the size of the SAI Input Method data element. 4. The first nibble of byte 1 of the SAI Input Method shall be '0', '1', '2' or '4'. 5. The second nibble of byte 1 of the SAI Input Method shall be '0', '1'

	or '2'. 6. Byte 2 of the SAI Input Method shall be present. 7. Byte 2 of the SAI Input Method shall have one of the following values: '00', '01', '02', '03', 'FE', or 'FF'. 8. Byte 3 of the SAI Input Method shall have the value '00' or '01'. 9. Byte 4 - 7 of the SAI Input Method shall be BCD encoded. 10. Byte 4 of the SAI Input Method shall be smaller than byte 6 of the SAI Input Method. 11. Byte 7 of the SAI Input Method shall be smaller than byte 5 of the SAI Input Method.

Page 88, Test Case SE_LDS_DG14_006

Replace the entire table with the following table:

Test Case-ID	SE_LDS_DG14_006
Purpose	If the algorithm used is Diffie Hellman, test the value of the parameters of the icAuthPublicKey field of the IC Auth PublicKey Info for each Security Info that defines the CA public key in the Security Infos Set.
Version	1.2
References	ISO/IEC 18013-3:2009
Profile	CA-DH
Preconditions	1. EF.DG14 has been retrieved from the IDL. 2. The Security Infos data element has been retrieved from EF.DG14. 3. At least one Security Info element in the Security Infos data element has the protocol OID id-ICAuth.
Test Scenario	Perform the following checks for each Security Info that defines the CA public key in the Security Infos Set: 1. Check the DH parameters of the algorithm. 2. Check the encoding of the base g. 3. Check the encoding of the prime p. 4. Check the consistency of g and p. 5. If private value length l is present, check the encoding of l. 6. If private value length l is present, check the value of l. 7. If private value length l is present, check the value of l. 8. Check the encoding of the DH Public Key. 9. Check the consistency of the DH Public Key value and prime p.
Expected Results	1. The parameters shall be ASN.1 encoded and follow PKCS #3 (DH), i.e. the DH parameters shall specify a prime (integer), a base (integer), and optionally a privateValueLength (integer). 2. g shall be a positive integer. 3. p shall be a positive integer. 4. g shall be less than p (0 < g < p). 5. length l shall be a positive integer. 6. length l shall be non-zero (l > 0). 7. length l shall be such that 2l-1 < p.

	8. The DH Public Key shall be a positive integer. 9. The DH Public Key shall be smaller than p (0 < PublicKey < p).

Page 88, Test Case SE_LDS_DG14_007

Replace the entire table with the following table:

Test Case-ID	SE_LDS_DG14_007
Purpose	If the algorithm used is ECDH, test the value of the parameters of the icAuthPublicKey field of the IC Auth PublicKey Info for each Security Info that defines the CA public key in the Security Infos Set.
Version	1.2
References	ISO/IEC 18013-3:2009 RFC-3279
Profile	EAP, CA-ECDH
Preconditions	1. EF.DG14 has been retrieved from the IDL. 2. The Security Infos data element has been retrieved from EF.DG14. 3. At least one Security Info element in the Security Infos data element has the protocol OID id-ICAuth.
Test Scenario	Perform the following checks for each Security Info that defines the CA public key in the Security Infos Set: 1. Check the Elliptic Curve parameters. 2. Check the encoding of the prime p. 3. Check the value of the prime p. 4. Check the value of the curve parameter a. 5. Check the consistency of the curve parameter a and prime p. 6. Check the value of the curve parameter b. 7. Check the consistency of the curve parameter b and prime p. 8. Check the consistency of the curve parameters a and b. 9. Check the value of the base point G. 10. Check the encoding of the Cofactor f. 11. Check the value of the Cofactor f. 12. Check the encoding of the order r of base point. 13. Check the value of the order r of base point. 14. Check the consistency of the order r and prime p. 15. Check the consistency of the order r, prime p, and co-factor f. 16. Check value of the EC public key (base point Y).
Expected Results	1. The parameters shall follow ASN.1 structure specified in RFC 3279. 2. p shall be a positive integer. 3. p shall be larger than 2 (p>2). 4. a shall be larger than or equal to zero (a>=0). 5. a shall be smaller than p (a<p). 6. b shall be larger than or equal to zero (b>=0). 7. b shall be smaller than p (b<p). 8. The values of a and b shall be such that 4a3 + 27b2 <> 0.

	9. The base point G shall be on the curve, with both coordinates in range 0 .. (p - 1). 10. f shall be a positive integer. 11. f shall be larger than zero (f>0). 12. r shall be a positive integer. 13. r shall be larger than zero (r>0). 14. r shall not be equal to p (r <> p). 15. r, p, and f shall be such that r * f <= 2p. 16. The public base point Y is on the curve, with both coordinates in range 0 .. (p - 1).

Page 89

Insert the following clauses after clause A.3.14.7:

A.3.14.8 Test Case SE_LDS_DG14_008

Test – ID	SE_LDS_DG14_008
Purpose	This test checks the absence of EAC SecurityInfo in DG14 if EAP is supported.
Version	1.2
References	ISO/IEC 18013-3:2009/AMD2 clause 8.7.3
Profile	EAP
Preconditions	1. EF.DG14 has been retrieved from the IDL. 2. The SecurityInfos data element has been retrieved from EF.DG14.
Test scenario	1. Check the absence of SecurityInfo data elements with protocol OID id-TA. 2. Check the absence of SecurityInfo data elements with protocol OID id-PK-DH or id-PK-ECDH. 3. Check the absence of SecurityInfo data elements with protocol OID a. id-CA-DH-3DES-CBC-CBC or b. id-CA-DH-AES-CBC-CMAC-128 or c. id-CA-DH-AES-CBC-CMAC-192 or d. id-CA-DH-AES-CBC-CMAC-256 or e. id-CA-ECDH-3DES-CBC-CBC or f. id-CA-ECDH-AES-CBC-CMAC-128 or g. id-CA-ECDH-AES-CBC-CMAC-192 or h. id-CA-ECDH-AES-CBC-CMAC-256.
Expected results	1. True. 2. True. 3. True.

A.3.14.9 Test Case SE_LDS_DG14_009

Test – ID	SE_LDS_DG14_009
Purpose	This test checks the absence of EAP SecurityInfo in DG14 if EAC is supported.
Version	1.2
References	ISO/IEC 18013-3:2009/AMD 2 clause 8.7.3 ISO/IEC 18013-3:2009
Profile	EAC
Preconditions	1. EF.DG14 has been retrieved from the IDL. 2. The SecurityInfos data element has been retrieved from EF.DG14.
Test scenario	1. Check the absence of SecurityInfo data elements with protocol OID id-ICAuth.
Expected results	1. True.

A.3.14.10 Test Case SE_LDS_DG14_010

Test – ID	SE_LDS_DG14_010
Purpose	This test checks the absence of PACE SecurityInfo in DG14 if EAP is supported.
Version	1.2
References	ISO/IEC 18013-3:2009/AMD3 clause H.2.3
Profile	EAP
Preconditions	1. EF.DG14 has been retrieved from the IDL. 2. The SecurityInfos data element has been retrieved from EF.DG14.
Test scenario	1. Check the absence of SecurityInfo data elements with protocol OID a. id-PACE-ECDH-GM-3DES-CBC-CBC or b. id-PACE-ECDH-GM-AES-CBC-CMAC-128 or c. id-PACE-ECDH-GM-AES-CBC-CMAC-192 or d. id-PACE-ECDH-GM-AES-CBC-CMAC-256. 2. Check the absence of SecurityInfo data elements with protocol OID id-PACE-ECDH-GM.
Expected results	1. True. 2. True.

A.3.14.11 Test Case SE_LDS_DG14_011

Test – ID	SE_LDS_DG14_011
Purpose	This test checks the absence of EAP SecurityInfo in DG14 if PACE is supported.
Version	1.2
References	ISO/IEC 18013-3:2009/AMD 2 clause H.2.3 ISO/IEC 18013-3:2009
Profile	PACE
Preconditions	1. EF.DG14 has been retrieved from the IDL. 2. The SecurityInfos data element has been retrieved from EF.DG14.

Test scenario	1. Check the absence of SecurityInfo data elements with protocol OID id-ICAuth.
Expected results	1. True.

A.3.14.12 Test Case SE_LDS_DG14_012

Refer to [TR-ICAO Part 3], clause 4.5.1.

For eMRTD, read IDL.

For [R7], read [TR-PACE]

A.3.15 Test Unit SE_LDS_CardAccess – Tests for EF.CardAccess

Refer to [TR-ICAO Part 3], clause 4.6.

For eMRTD, read IDL.

For [R7], read [TR-PACE]

In Test case LDS_I_02 step 2, replace the algorithm identifier list by the following:

- id-PACE-ECDH-GM-3DES-CBC-CBC
  (OID : 0.4.0.127.0.7.2.2.4.2.1)
- id-PACE-ECDH-GM-AES-CBC-CMAC-128
  (OID : 0.4.0.127.0.7.2.2.4.2.2)
- id-PACE-ECDH-GM-AES-CBC-CMAC-192
  (OID : 0.4.0.127.0.7.2.2.4.2.3)
- id-PACE-ECDH-GM-AES-CBC-CMAC-256
  (OID : 0.4.0.127.0.7.2.2.4.2.4)

In Test case LDS_I_02 step 4, remove the following ParameterId from the list:

- ‘00’ if 1024-bit MODP Group with 160-bit Prime Order Subgroup is used.
- ‘01’ if 2048-bit MODP Group with 224-bit Prime Order Subgroup is used.
- ‘02’ if 2048-bit MODP Group with 256-bit Prime Order Subgroup is used.

In Test case LDS_I_03 step 2, replace the protocol identifier list by the following:

- id-PACE-ECDH-GM
  (OID : 0.4.0.127.0.7.2.2.4.2)

In Test case LDS_I_03 step 3, replace the algorithm identifier list by the following:

- ecPublicKey (OID: 1.2.840.10045.2.1)