INTERNATIONAL STANDARD

ISO/IEC 18013-3

Second edition
2017-04

AMENDMENT 1
2022-01

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

Part 3: Access control, authentication and integrity validation

AMENDMENT 1: PACE protocol

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 1: Protocole de PAC

Reference number
ISO/IEC 18013-3:2017/Amd. 1:2022(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 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 and IEC websites.

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 1: PACE protocol

Page 2, Clause 2

Replace:

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

with:

> 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*

Page 4, 3.10

Delete Note 1 to entry and designate the existing "Note 2 to entry" as "Note 1 to entry".

Page 31, 8.4.4.1

Replace Table 10 with:

Table 10 — Non-match alert parameters

Name, Fixed (F) or Variable (V), Mandatory (M) or Optional (O)	Field format/length/type	Example
SAI_referencestring, V, M	Byte 1: — '00' if the input string follows; — '01' if a reference to where the input string can be obtained follows. Subsequent bytes: — If byte 1 = '00', the input string follows from byte 2 (inclusive). The input string is encoded in accordance with ISO/IEC 8859-1:1998; — If byte 1 = '01', the reference to the field that contains the input string is constructed as aabb where aa is the data group and bb is the sequence number of the referenced data element, with aabb encoded as unsigned BCD.	An input string of ABC4DEF contained in the SAI_referencestring field will be coded as '00 41 42 43 34 44 45 46', where '41 42 43 34 44 45 46' is the encoded form of ABC4DEF. If the licence number is used as the input string, this will be coded as '01 01 08'. If the 16th data element of Data Group 12 is used as the input parameter, the input string will be coded as '01 12 16'.
SAI_inputmethod, V, O	Byte 1: SAI standard and input method. The four most significant bits (upper nibble) of byte 1 can take on any of the following values: — '0x' if the input string is based on an existing field; — '1x' if the input string is based on a dedicated field; — '2x' if the input string is stored in a barcode; — '4x' if the input string is based on IDL MRZ. The four least significant bits (lower nibble) of byte 1 denotes the input method, and can take on any of the following values: — 'x0' if the input string is intended for manual input; — 'x1' if the input string is intended for OCR interpretation; — 'x2' if the input string is stored as a barcode. Byte 2: Barcode standard. If the first byte is of the form 'x2', byte 2 is mandatory, taking on any of the following values:	If the licence number is used as the input string (i.e. a SAI is constructed around the existing licence number field on the IDL), the value of SAI_inputmethod will be '00'. If, in addition, the input string is printed in OCR-B font, the input string will be '00 01', or alternatively '00 01 00'. If, in addition, the SAI is located on the portrait side of the IDL, with the top left corner of the SAI at 29 mm from the left edge of the card and 24 mm from the bottom edge of the card, and the right bottom corner of the SAI at 59 mm from the left edge of the card and 14 mm from the bottom edge of the card, the input string will be '00 01 00 00 29 24 59 14'.

Table 10 *(continued)*

Name, Fixed (F) or Variable (V), Mandatory (M) or Optional (O)	Field format/length/type	Example
	— '00' for PDF417; — '01' for Code 39 (ISO/IEC 16388); — '02' for Code 128 (ISO/IEC 15417); — '03' for data matrix (ISO/IEC 16022); — 'FE' for other barcode standards not provided for above. If the first byte is not of the form 'x2', byte 2 is optional. If present, it shall have the following value: — 'FF' for no barcode.	
	Byte 2 is also mandatory if Bytes 3 to 7 are present. Bytes 3 to 7: Position of the SAI, expressed as 'aa bb cc dd ee', where 'aa' is the side of the card on which the SAI appears ('00' for portrait side, and '01' for non-portrait side), 'bb cc' is the top left corner of the SAI (where 'bb' is the distance from the left edge of the IDL and 'cc' is the distance from the bottom edge of the card), and 'dd ee' is the bottom right corner of the SAI (where 'dd' is the distance from the left edge of the IDL and 'ee' is the distance from the bottom edge of the card), with all distances measured in millimetres, and encoded as BCD. The bytes are progressively mandatory, i.e. SAI_inputmethod can consist only of byte 1, or only of bytes 1 and 2, or of bytes 1 to 7.	

Page 35, 8.7.3

Delete the NOTE and insert the following sentence at the end of this subclause:

The chip access procedure shall be in accordance with ICAO Doc 9303-11:2015, 4.2. The SecurityInfos shall be in accordance with ICAO Doc 9303-10:2015, 5.3.1 and ICAO Doc 9303-11:2015, 9.2.8.

Page 39, 10.4

Insert the following NOTE at the end of this subclause:

NOTE '6F' is nested within DO '7E' when used as file control information template for ISO/IEC 18013 (all parts).

Page 40, 10.5

Replace the NOTE with:

NOTE See ICAO Doc 9303-11:2015, 9.2.8.

Page 40, 10.6

Replace the NOTE with:

NOTE See ICAO Doc 9303-10:2015, 5.3.1.

Page 67, C.1

Replace the second paragraph with:

PACE is specified in ICAO Doc 9303-11:2015, 4.4.1 to 4.4.5. Specification defined in ICAO Doc 9303-11:2015, 9.1, 9.2 and 9.4 to 9.8 applicable to PACE also apply for IDL in respect of the limitations defined in C.2.1.

Replace the third paragraph with:

After PACE, AES and 3DES shall be applied in Secure Messaging as specified in ICAO Doc 9303-11:2015, 9.8.

Replace NOTE 2 with:

NOTE 2 According to ICAO Doc 9303-11:2015, padding is always performed by the secure messaging layer, so that the underlying message authentication code does not need to perform any internal padding.

Page 67, C.2

Replace the entire subclause with:

C.2 Changes to ICAO Doc 9303-11

C.2.1 General

This subclause describes the changes that apply to ICAO Doc 9303-11:2015, 4.4.1 to 4.4.5 to support access to the IDL application using PACE.

Only ECDH generic mapping shall be used.

For eMRTD Application, read Driving Licence Application.

For eMRTD, read IDL.

For eMRTD chip or MRTD chip, read SIC.

For MRZ, read input string.

For password, read input string.

C.2.2 Key derivation function

The key derivation function for PACE is specified in ICAO Doc 9303-11:2015, 9.7.3. This document replaces the encoding of passwords with "f (π) = input string".

C.3

Add the following new subclause after C.2:

C.3 Worked example

C.3.1 General

This subclause provides a worked example for PACE. Not all steps are explicitly shown. As a precondition, the MF is selected.

C.3.2 Read PACEInfo

1. Select EF.CardAccess (file identifier = '01 1C')

   Unprotected command APDU

CLA	INS	P1	P2	Lc	Command data field
'00'	'A4'	'02'	'0C'	'02'	'01 1C'

   Unprotected response APDU

SW1-SW2
'90 00'

2. Read EF.CardAccess

   Read the first 8 bytes of EF.CardAccess.

   Unprotected command APDU

CLA	INS	P1	P2	Le
'00'	'B0'	'00'	'00'	'08'

   Unprotected response APDU

Response data field	SW1-SW2
resp_data	'90 00'

   resp_data = '31 14 30 12 06 0A 04 00'

   Read the rest of EF.CardAccess.

Unprotected command APDU

CLA	INS	P1	P2	Le
'00'	'B0'	'00'	'08'	'0E'

Unprotected response APDU

Response data field	SW1-SW2
resp_data	'90 00'

resp_data = '7F 00 07 02 02 04 02 02 02 01 02 02 01 0C'

Hex string of EF.CardAccess is '31 14 30 12 06 0A 04 00 7F 00 07 02 02 04 02 02 02 01 02 02 01 0C'

Content of EF.CardAccess in this worked example is described in Table C.1.

Table C.1 — Example content of EF.CardAccess

<table>
<tr><th>Tag</th><th>Length</th><th colspan="5">Value</th><th>Note</th></tr>
<tr><td rowspan="6">‘31’</td><td rowspan="6">‘14’</td><td colspan="5">SET data object</td><td>SecurityInfos</td></tr>
<tr><td>Tag</td><td>Length</td><td colspan="3">Value</td><td></td></tr>
<tr><td>‘30’</td><td>‘12’</td><td colspan="3">SEQUENCE data object</td><td>PACEInfo</td></tr>
<tr><td></td><td></td><td>Tag</td><td>Length</td><td>Value</td><td></td></tr>
<tr><td></td><td></td><td>‘06’</td><td>‘0A’</td><td>‘04 00 7F 00 07 02 02 04 02 02’</td><td>OID id-PACE-ECDH-GM-AES-CBC-CMAC-128</td></tr>
<tr><td></td><td></td><td>‘02’</td><td>‘01’</td><td>‘02’</td><td>Version 2</td></tr>
<tr><td colspan="7">[a] This value indicates NIST P-256 standard domain parameters.</td></tr>
</table>

The BER-TLV structure of public key data object is specified in ICAO Doc 9303-11:2015, 9.4. For convenience, an ASN.1 encoding of the NIST P-256 standard domain parameters is given in Table C.2.

Table C.2 — NIST P-256 standard domain parameters

T	L	V					Note
'30'	'81EC'	SEQUENCE data object					Domain Parameters
		T	**L**	**V**			
		'06'	'07'	'2A 86 48 CE 3D 02 01'			OID id-ecPublicKey
		'30'	'81E0'	SEQUENCE data object			ECParameters
				T	**L**	**V**	
				'02'	'01'	'01'	Version
				'30'	'2C'	SEQUENCE data object	FieldID
						T / **L** / **V**	
						'06' / '07' / '2A 86 48 CE 3D 01 01'	OID Prime field (ANSI X9.62)
						'02' / '21' / '00 FF FF FF FF 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF'	Prime p
				'30'	'44'	SEQUENCE data object	Curve
						'04' / '20' / 'FF FF FF FF 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF FF FF FF FC'	Parameter a
						'04' / '20' / '5A C6 35 D8 AA 3A 93 E7 B3 EB BD 55 76 98 86 BC 65 1D 06 B0 CC 53 B0 F6 3B CE 3C 3E 27 D2 60 4B'	Parameter b
				'04'	'41'	'04 6B 17 D1 F2 E1 2C 42 47 F8 BC E6 E5 63 A4 40 F2 77 03 7D 81 2D EB 33 A0 F4 A1 39 45 D8 98 C2 96' '4F E3 42 E2 FE 1A 7F 9B 8E E7 EB 4A 7C 0F 9E 16 2B CE 33 57 6B 31 5E CE CB B6 40 68 37 BF 51 F5'	Group Generator G
				'02'	'21'	'00 FF FF FF FF 00 00 00 00 FF FF FF FF FF FF FF BC E6 FA AD A7 17 9E 84 F3 B9 CA C2 FC 63 25 51'	Group order n
				'02'	'01'	'01'	Cofactor f

C.3.3 Generate password key K_π

In this worked example, IDL MRZ is used for input string.

IDL MRZ (See Table 9) = D123T09PJ3Y8478FSD<<<<<<<<<<<1

1. Generate an input string from IDL MRZ:

   Input string = 123T09PJ3Y8478FSD<<<<<<<<<<<

2. Computation of a shared secret K:

   K = '31 32 33 54 30 39 50 4A 33 59 38 34 37 38 46 53 44 3C 3C 3C 3C 3C 3C 3C 3C 3C 3C 3C'

3. Derivation of an encryption key(K_π) from a shared secret K:

   Concatenate K and c (c = 3):

   D= '31 32 33 54 30 39 50 4A 33 59 38 34 37 38 46 53 44 3C 3C 3C 3C 3C 3C 3C 3C 3C 3C 00 00 00 03'

   Calculate Hash of D:

   keydata = $H_{SHA\text{-}1}$(K || c) = '77 E1 7B 6D 08 48 9C B3 5A CC A1 49 E4 50 CA A5 A1 FF 11 1A'

   Use octets 1 to 16 of keydata as 128-bit AES key:

   K_π = '77 E1 7B 6D 08 48 9C B3 5A CC A1 49 E4 50 CA A5'

C.3.4 Application flow of the ECDH-based example

1. MSE Set:AT

   The command MSE:Set AT is used to select and initialise the PACE protocol.

Command				
CLA	'00'			Interindustry class No command chaining No secure messaging Basic logical channel
INS	'22'			MSE
P1-P2	'C1 A4'			Set AT
Lc	'0F'			
Data field	Tag	Length	Value	Comment
	'80'	'0A'	'04 00 7F 00 07 02 02 04 02 02'	PACE with ECDH generic mapping AES 128
	'83'	'01'	'01'	Password: input string
Le	Absent			

Response		
Data field	Absent	
SW1-SW2	'90 00'	Normal processing

2. Encrypted nonce

   The SIC randomly generates the nonce s:

   Nonce s = " C9 8C FC B4 4F 55 80 1D F5 A6 22 1C 21 CE 1A 61"

   The SIC encrypts the nonce s by means of K_π:

   Encrypted nonce z = "99 08 FD A7 35 74 0C DE B4 6F 53 AF 8D 87 CF 90"

   IS requests encrypted nonce to SIC and SIC responds to IS with encrypted nonce. The encoding of the command APDU and the corresponding response can be found in the following:

Command				
CLA	'10'			Interindustry class Command chaining No secure messaging Basic logical channel
INS	'86'			General authenticate
P1-P2	'00 00'			Keys and protocol implicitly known
Lc	'02'			Length of data field
Data field	Tag	Length	Value	Comment
	'7C'	'00'		Dynamic authentication data
Le	'00'			Expected maximal byte length of the response data field is 256

Response						
Data field	Tag	Length	Value			Comment
	'7C'	'12'				Dynamic authentication data
			Tag	Length	Value	Comment
			'80'	'10'	'99 08 FD A7 35 74 0C DE B4 6F 53 AF 8D 87 CF 90'	Encrypted nonce
SW1-SW2	'90 00'					Normal processing

The IS decrypts the encrypted nonce z by means of K_{π} and then gets nonce s.

3. Map the nonce

The nonce is mapped to an ephemeral group generator via generic mapping. Both SIC and IS randomly generate ephemeral key pairs. An ephemeral key pairs example is shown in Table C.3.

Table C.3 — List of randomly chosen ephemeral key pairs (examples)

SIC private key for the mapping phase	'E3 E3 C4 3B 12 FA AF 19 03 03 78 90 9D D0 6A 0F 5D 6B D5 DC 2C 93 1C E4 1C 53 52 C5 DE CD 40 22'
SIC public key for the mapping phase	'F3 66 6F 52 79 53 B6 C0 78 30 35 F2 EC 6B DA 15 20 E1 EF 44 97 74 06 7F 32 E6 0F 0F 3E C0 C4 C0 76 7D B6 1B 4A AB 51 09 5A 31 2B E6 FC 99 87 0E DF 74 98 EA 19 44 A4 A2 7C A5 AA 0C 80 88 CB 3C'
IS private key for the mapping phase	'07 48 59 3F D5 A4 41 57 EA 4B 7D 8D 71 65 9A 3A 9A 85 35 00 CC 33 FD D4 24 EE 62 48 81 49 F0 E7'
IS public key for the mapping phase	'46 0F 72 04 CA D3 79 88 83 BE 6E 11 39 D8 87 8E 59 F7 C1 3A 42 CC 82 B7 A9 8D CF 1B BF 4F 2D 90 B9 FC 23 18 67 C2 80 DA 32 CB 06 D8 3B 5B 84 3D 8B B7 74 21 E4 32 A2 17 76 F4 DC C8 4E 24 FE 0A'

IS and SIC exchange ephemeral public keys. The encoding of the command APDU and the corresponding response can be found in the following:

Command						
CLA	'10'					Interindustry class Command chaining No secure messaging Basic logical channel
INS	'86'					General authenticate
P1/P2	'00 00'					Keys and protocol implicitly known
Lc	'45'					Length of data field
Data field	Tag	Length	Value			Comment
	'7C'	'43'				Dynamic authentication data
			Tag	Length	Value	Comment
			'81'	'41'	'04 46 0F 72 04 CA D3 79 88 83 BE 6E 11 39 D8 87 8E 59 F7 C1 3A 42 CC 82 B7 A9 8D CF 1B BF 4F 2D 90 B9 FC 23 18 67 C2 80 DA 32 CB 06 D8 3B 5B 84 3D 8B B7 74 21 E4 32 A2 17 76 F4 DC C8 4E 24 FE 0A'	Mapping data
Le	'00'					Expected maximal byte length of the response data field is 256

Response						
Data field	Tag	Length	Value			Comment
	'7C'	'43'				Dynamic authentication data
			Tag	Length	Value	Comment
			'82'	'41'	'04 F3 66 6F 52 79 53 B6 C0 78 30 35 F2 EC 6B DA 15 20 E1 EF 44 97 74 06 7F 32 E6 0F 0F 3E C0 C4 C0 76 7D B6 1B 4A AB 51 09 5A 31 2B E6 FC 99 87 0E DF 74 98 EA 19 44 A4 A2 7C A5 AA 0C 80 88 CB 3C'	Mapping data
SW1-SW2	’90 00’					Normal processing

SIC and IS compute shared secret H and mapped generator $\hat{G}$ as shown in Table C.4.

Table C.4 — Shared secret H and mapped generator (examples)

Shared secret H	'1E B6 FA CA 3F BB E0 28 23 38 1E 43 59 64 46 AA 06 25 39 07 8D 89 96 5E E5 F4 A3 D1 DF B4 01 4E A0 95 43 C2 BF 8B 05 5D CC D1 25 07 8D F1 BA 3C EC 59 7D C2 34 3A 78 AE 85 C9 CA E6 FE 53 95 B9'
Mapped generator $\hat{G}$	'82 F9 5F 49 6B 84 BC 63 56 17 78 0C 8F BE 55 C3 81 6E 69 5B 09 A0 62 CA C8 B6 B8 79 8D A5 A3 6A 6C 39 41 23 0F 0D 8C 45 25 7E 9D 37 40 C6 4F 08 20 EF 45 DE 12 B6 ED A2 12 B2 94 2C 78 C0 14 45'

4. Perform key agreement

In the third step, SIC and IS perform an anonymous ECDH key agreement using the new domain parameters determined by the mapped generator of the previous step. SIC and IS anonymous key pairs are shown in Table C.5.

Table C.5 — List of anonymous key pairs (examples)

IS's private key	'8F D4 48 83 6A E1 FD DB 35 75 98 70 CE 97 D3 13 6F 2F 91 35 C2 88 B0 9D 4F 72 C5 89 52 47 B3 4F'
IS's public key	'F1 BA 6B 51 20 86 07 A9 BC 0D 68 58 37 F1 C0 57 38 DB B1 6D CD 8C 1C 7C 44 B5 E5 D3 62 CA 04 EB 93 9D 85 59 64 6C 3E 96 0D 84 CB A2 40 26 F2 01 FC B1 3E 90 76 05 1A 29 B0 59 0E 1E D0 94 3D 94'
SIC's private key	'BA 5C 89 E4 EF 91 7F 44 2A 5D DB CE 9B C1 7C 3A 71 C9 72 C2 D4 2A 10 00 89 91 DF 97 98 77 36 67'
SIC's public key	'C2 41 53 5D 32 FB 17 A7 18 26 D1 B7 0C E1 6B E7 E3 3E 81 9F 41 8B 80 73 52 1A 4D 18 40 AC 2C 9A F1 D5 3E BC 6C BA A7 27 37 CF 10 9C A2 5D 38 A4 A9 57 B2 0F 9A CA 95 CC F0 D0 46 A3 69 5A 54 00'

The encoding of the key agreement is examined in the following:

Command						
CLA	'10'					Interindustry class Command chaining No secure messaging Basic logical channel
INS	'86'					General authenticate
P1/P2	'00 00'					Keys and protocol implicitly known
Lc	'45'					Length of data field
Data field	Tag	Length	Value			Comment
	'7C'	'43'				Dynamic authentication data
			Tag	Length	Value	Comment
			'83'	'41'	'04 F1 BA 6B 51 20 86 07 A9 BC 0D 68 58 37 F1 C0 57 38 DB B1 6D CD 8C 1C 7C 44 B5 E5 D3 62 CA 04 EB 93 9D 85 59 64 6C 3E 96 0D 84 CB A2 40 26 F2 01 FC B1 3E 90 76 05 1A 29 B0 59 0E 1E D0 94 3D 94'	IS ephemeral public key
Le	'00'					Expected maximal byte length of the response data field is 256

Response						
Data field	Tag	Length	Value			Comment
	'7C'	'43'				Dynamic authentication data
			Tag	Length	Value	Comment
			'84'	'41'	'04 C2 41 53 5D 32 FB 17 A7 18 26 D1 B7 0C E1 6B E7 E3 3E 81 9F 41 8B 80 73 52 1A 4D 18 40 AC 2C 9A F1 D5 3E BC 6C BA A7 27 37 CF 10 9C A2 5D 38 A4 A9 57 B2 0F 9A CA 95 CC F0 D0 46 A3 69 5A 54 00'	SIC ephemeral public key
SW1-SW2	’90 00’					Normal processing

SIC and IS calculate the shared secret. Only the x-coordinate of the shared secret is required since the KDF uses only the first coordinate to derive the session keys. The x-coordinate of the shared secret is denoted as K.

Shared secret = '3A DA 9B CA C6 C0 52 14 81 E6 EA C6 FE A2 A0 BD C7 68 E7 25 C0 E5 CD 5D 45 95 C9 1B 46 A4 53 F5 64 74 2F 40 B9 69 15 7A 0F 93 1A 55 79 48 83 D1 8D F5 DA D1 AD 0D 11 2B C6 C8 3E 62 A4 22 4E 90'

K = '3A DA 9B CA C6 C0 52 14 81 E6 EA C6 FE A2 A0 BD C7 68 E7 25 C0 E5 CD 5D 45 95 C9 1B 46 A4 53 F5'

By means of the KDF, the AES 128 session keys KS_{ENC} and KS_{MAC} are derived from the shared secret.

Calculate KS_{ENC}:

keydata = $H_{SHA\text{-}1}$(K | c) with c = '00 00 00 01'

Use octets 1 to 16 of keydata as 128-bit AES key:

KS_{ENC} = 'AB FE 8A 37 36 79 80 27 5F 24 8B 74 83 EA 2D 91'

Calculate KS_{MAC}:

keydata = $H_{SHA\text{-}1}$(K | c) with c = '00 00 00 02'

Use octets 1 to 16 of keydata as 128-bit AES key:

KS_{MAC} = 'DE BA B9 8F 2A 3F B7 AF EF 11 1F 16 E7 8D 75 BD'

5. Mutual authentication

The authentication tokens are derived by means of KS_{MAC} using the input data to calculate T_{IS} and T_{SIC} that is shown in Table C.6. Details of these input data are shown in Tables C.7 and C.8.