RÉPUBLIQUE FRANÇAISE

AGENCE NATIONALE DES TITRES SÉCURISÉS

MACHINE READABLE TRAVEL DOCUMENTS

ADVANCED SECURITY MECHANISMS FOR MACHINE READABLE TRAVEL DOCUMENTS – EXTENDED ACCESS CONTROL (EACv1)

COMPLEMENTARY TO TEST METHODS FOR MRTDs USING STATIC BINDING

Version 1.0

September 12, 2012

Version history

Version	Date	Editor	Description
1.0 RC1	25-06-2012	N.Regnault	Initial version
1.0RC2	27-06-2012	N.Regnault	AFNOR review
1.0RC3	02-07-2012	N.Regnault	BSI comments: • Static binding is not defined but noted in EACv2.10, • Suppression of annex A specifying the StaticBindingInfo element, • Addition of a reference to the Application Notes on Static Binding and addition of a note about the StaticBindingInfo workaround
1.0	12-09-21012	N.Regnault	Public Release

Content

1 Introduction

This document is a complement to [R10]. It specifies alternative and additional test cases for MRTD using static bindings for the combination of PACE and Terminal Authentication, as noted in [R2] (§3.5).

Alternative test cases replace some test cases which are defined in [R10] i.e. the replaced test case in [R10] MUST NOT be executed with a static binding MRTD.

Additionnal test cases do not replace test cases but come in addition.

1.1 Reference documentation

The following documentation serves as a reference for this specification:

[R1] ICAO 9303 Edition 6 Part 1, Part 2 and Part 3

[R2] Technical Guideline TR-03110-1 “Advanced Security Mechanisms forMachine Readable Travel Documents - Part 1: eMRTDs with BAC/PACEv2 and EACv1”, Version 2.10, March 2012

[R3] RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

[R4] ISO/IEC 7816-4:2005. Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange

[R5] Supplement ICAO 9303 V4.0, June 2006

[R6] PKCS #3: Diffie-Hellman Key-Agreement Standard

[R7] TR-03111: Technical Guideline, Elliptic Curve Cryptography (ECC) based on ISO 15946

[R8] ICAO Technical Report “RF protocol and application test standard for ePassport Part 3”, Version 1.01, February 2007

[R9] ICAO Technical Report “Supplemental Access Control for Machine Readable Travel Documents”, Version 1.01, November 2010

[R10] AFNOR/BSI “Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EACv1) – Tests for Security Implementation”, Version 1.2

[R11] Gixel, Application Notes on Static Binding, v1.0

1.2 Terminology

The key words "MUST", "SHALL", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY" in this document are to be interpreted as described in [R3].

MUST	This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
MUST NOT	This phrase, or the phrase „SHALL NOT“, means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications MUST be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" mean that there may

	exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications SHOULD be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the adjective „OPTIONAL“, means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

2 General test requirements

2.1 Test setup

The Test setup defined in [R10] applies to this document.

2.2 Test profiles

In addition to the profiles already specified in [R10] this complement defines the following additional profiles.

Profile-ID	Profile	Remark
SB	Static Binding	The MRTD is using the static binding for the combination of PACE and Terminal Authentication. When PACE is done with the MRZ, ID_{PICC} is the MRTD chip's Document Number as contained in the MRZ including the check digit. When PACE is done with the CAN, ID_{PICC} is the CAN.
DG14SB	EF.DG14 containing a SecurityInfo element for static binding	A SecurityInfo element is present in the EF.DG14 to indicate to the terminal that the MRTD is using the static binding.[1]

[1] See Application Notes [R11] for the SecurityInfo workaround on static binding

3 Complementary tests for layer 6 (ISO 7816)

This chapter defines alternative and additionnal tests which replace test case ISO7816_K_1b and ISO7816_K_20 specified in [R10].

The following test cases from [R10] MUST NOT be executed with an eMRTD using static binding:

- ISO7816_K_1b
- ISO7816_K_20

3.1 Unit ISO7816_K Terminal Authentication

3.1.1 Test case ISO7816_KSB_1

This test case is an alternative to test case ISO7816_K_1b

Test - ID	ISO7816_KSB_1
Purpose	Test the card to perform Terminal Authentication with PACE using the MRZ.
Version	1.0
Profile	TA, PACE, SB
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. PACE with MRZ MUST be used. 2. The Chip Authentication mechanism MUST have been performed as well. 3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).
Test scenario	1. Send the given MSE: Set DST APDU to the eMRTD. '0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <certificate authority reference> • The Certification Authority Reference MUST be used as read from the EF.CVCA file. 2. Send the appropriate DV-Certificate as specified in the "Certificate Set 1" chapter as DV_CERT_1. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. Send the given MSE: Set DST APDU to the eMRTD. '0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <certificate authority reference> • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the "Certificate Set 1" chapter as IS_CERT_1.

	'OC 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 5. Send the given MSE: Set AT APDU to the eMRTD. '0C 22 81 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <Certification Holder Reference > • The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eMRTD. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eMRTD. '0C 82 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • The MRTD chip's ephemeral PACE public key MUST be used to build the encrypted terminal signature (SPCD) for the External Authenticate command. IDPICC = Comp(ehpPKPICC) • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01. 8. Reset the chip by switching off the field and switching in on again • "Open the ePassport Application" using PACE with MRZ • Perform Chip Authentication • Read the Certification Authority Reference from the EF.CVCA file (Primary trust point) • Perform step 1 of this test case 9. Perform step 2 of this test case 10. Perform step 3 of this test case 11. Perform step 4 of this test case 12. Perform step 5 of this test case 13. Perform step 6 of this test case 14. Send the given external authenticate command to the eMRTD. '0C 82 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • The MRTD chip's Document Number as contained in the MRZ including the check digit. MUST be used to build the encrypted terminal signature (SPCD) for the External Authenticate command. IDPICC = Document Number as contained in the MRZ. • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.
Expected results	1. '90 00' in an SM response 2. '90 00' in an SM response 3. '90 00' in an SM response 4. '90 00' in an SM response

	5. ’90 00’ in an SM response 6. ‘<Eight bytes of random data> 90 00’ in an SM response 7. ISO checking error in an SM response. 8. ’90 00’ in an SM response 9. ’90 00’ in an SM response 10. ’90 00’ in an SM response 11. ’90 00’ in an SM response 12. ’90 00’ in an SM response 13. ‘<Eight bytes of random data> 90 00’ in an SM response 14. ’90 00’ in an SM response

3.1.2 Test case ISO7816_KSB_2

This test case is an alternative to test case ISO7816_K_1b

Test - ID	ISO7816_KSB_2
Purpose	Test the card to perform Terminal Authentication with PACE using the MRZ.
Version	1.0
Profile	TA, PACE, SB
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. PACE with MRZ MUST be used. 2. The Chip Authentication mechanism MUST have been performed as well. 3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).
Test scenario	1. Send the given MSE: Set DST APDU to the eMRTD. ‘0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ • <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <certificate authority reference> • The Certification Authority Reference MUST be used as read from the EF.CVCA file. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1. ‘0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. Send the given MSE: Set DST APDU to the eMRTD. ‘0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ • <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <certificate authority reference> • The Certification Holder Reference stored inside the DV-Certificate

	sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the "Certificate Set 1" chapter as IS_CERT_1. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 5. Send the given MSE: Set AT APDU to the eMRTD. '0C 22 81 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <Certification Holder Reference > • The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eMRTD. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eMRTD. '0C 82 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • The MRTD chip's Document Number as contained in the MRZ including the check digit. MUST be used to build the encrypted terminal signature (SPCD) for the External Authenticate command. IDPICC = Document Number as contained in the MRZ. • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.
Expected results	1. '90 00' in an SM response 2. '90 00' in an SM response 3. '90 00' in an SM response 4. '90 00' in an SM response 5. '90 00' in an SM response 6. '<Eight bytes of random data> 90 00' in an SM response 7. '90 00' in an SM response

3.1.3 Test case ISO7816_KSB_3

This test case is an alternative to test case ISO7816_K_20

Test - ID	ISO7816_KSB_3
Purpose	Test the card to perform Terminal Authentication with PACE using the CAN. This test case is only applicable for eMRTD which supports CAN.
Version	1.0
Profile	TA, PACE, SB
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. PACE with CAN MUST be used. 2. The Chip Authentication mechanism MUST have been performed as well.

	3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).
Test scenario	1. Send the given MSE: Set DST APDU to the eMRTD. '0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <certificate authority reference> • The Certification Authority Reference MUST be used as read from the EF.CVCA file. 2. Send the appropriate DV-Certificate as specified in the "Certificate Set 1" chapter as DV_CERT_1. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. Send the given MSE: Set DST APDU to the eMRTD. '0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <certificate authority reference> • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the "Certificate Set 1" chapter as IS_CERT_1. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 5. Send the given MSE: Set AT APDU to the eMRTD. '0C 22 81 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <Certification Holder Reference > • The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eMRTD. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eMRTD. '0C 82 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • The MRTD chip's ephemeral PACE public key MUST be used to build the encrypted terminal signature (SPCD) for the External Authenticate command. IDPICC = Comp(ehpPKPICC) • <Cryptogram> contains the encrypted terminal generated signature

	created with the private key of IS_KEY_01. 8. Reset the chip by switching off the field and switching in on again • "Open the ePassport Application" using PACE with CAN • Perform Chip Authentication • Read the Certification Authority Reference from the EF.CVCA file (Primary trust point) • Perform step 1 of this test case 9. Perform step 2 of this test case 10. Perform step 3 of this test case 11. Perform step 4 of this test case 12. Perform step 5 of this test case 13. Perform step 6 of this test case 14. Send the given external authenticate command to the eMRTD. '0C 82 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • The CAN MUST be used to build the encrypted terminal signature (SPCD) for the External Authenticate command. IDPICC = CAN. • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.
Expected results	1. '90 00' in an SM response 2. '90 00' in an SM response 3. '90 00' in an SM response 4. '90 00' in an SM response 5. '90 00' in an SM response 6. '<Eight bytes of random data> 90 00' in an SM response 7. ISO checking error in an SM response. 8. '90 00' in an SM response 9. '90 00' in an SM response 10. '90 00' in an SM response 11. '90 00' in an SM response 12. '90 00' in an SM response 13. '<Eight bytes of random data> 90 00' in an SM response 14. '90 00' in an SM response

3.1.4 Test case ISO7816_KSB_4

This test case is an alternative to test case ISO7816_K_20

Test - ID	ISO7816_KSB_4
Purpose	Test the card to perform Terminal Authentication with PACE using the CAN. This test case is only applicable for eMRTD which supports CAN.
Version	1.0
Profile	TA, PACE, SB
Preconditions	1. The "Open ePassport Application" procedure MUST have been

	performed. PACE with CAN MUST be used. 2. The Chip Authentication mechanism MUST have been performed as well. 3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).
Test scenario	1. Send the given MSE: Set DST APDU to the eMRTD. '0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <certificate authority reference> • The Certification Authority Reference MUST be used as read from the EF.CVCA file. 2. Send the appropriate DV-Certificate as specified in the "Certificate Set 1" chapter as DV_CERT_1. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. Send the given MSE: Set DST APDU to the eMRTD. '0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <certificate authority reference> • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the "Certificate Set 1" chapter as IS_CERT_1. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 5. Send the given MSE: Set AT APDU to the eMRTD. '0C 22 81 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <Certification Holder Reference > • The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eMRTD. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eMRTD. '0C 82 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • The CAN MUST be used to build the encrypted terminal signature (SPCD) for the External Authenticate command. IDPICC = CAN.

	• <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.
Expected results	**1.** ’90 00’ in an SM response **2.** ’90 00’ in an SM response **3.** ’90 00’ in an SM response **4.** ’90 00’ in an SM response **5.** ’90 00’ in an SM response **6.** ‘<Eight bytes of random data> 90 00’ in an SM response **7.** ’90 00’ in an SM response

4 Complementary tests for layer 7 (LDS)

This chapter defines additionnal tests to unit LDS_E Data group 14.

4.1 Unit LDS_ESB Data group 14

4.1.1 Test case ISO7816_ESB_1

This test case is an additional test.

Test - ID	ISO7816_ESB_1
Purpose	Test the ASN.1 encoding of the StaticBindingInfo
Version	1.0
Profile	TA, PACE, DG14SB
Preconditions	1. Data group 14 MUST have been read from the MRTD
Test scenario	1. The data content of the data group 14 MUST be encoded according to the SecurityInfos syntax definition. 2. The SecurityInfos set MUST contain one StaticBindingInfo element containing the Static Binding OID as defined in Annex A. 3. The StaticBindingInfo element MUST contain the version element set to 1.
Expected results	1. true 2. true 3. true