Federal Office
for Information Security

afnor
NORMALISATION

MACHINE READABLE TRAVEL DOCUMENTS

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

TESTS FOR SECURITY IMPLEMENTATION

Version 1.4.1
Date: April 6th, 2014

Version history

Version	Date	Editor	Description
0.3	17-04-2007	AFNOR	Proposal for harmonized document
0.5	24-04-2007	BSI/Secunet	EAC conformity tests – Harmonization document Working Draft
0.6	15-05-2007	AFNOR	EAC conformity tests – Harmonization document Working Draft - - AFNOR tests addition - Test cases EAC_CV_E_13, EAC_CV_E_14 and EAC_CV_E_15 have been deleted
0.7	24-05-2007	BSI/Secunet	- Editorial changes, - renumbered test case IDs - Add test for migration policy
0.72	01-06-2007	AFNOR	- Editorial changes
0.73	01-06-2007	BSI/Secunet	- Editorial change in certificate definition
0.8	09-07-2007	BSI/Secunet	- Resolved comments on 0.73
0.81	10-07-2007	AFNOR	- Resolved comments on 0.73 (suite)
0.82	10-07-2007	BSI/Secunet	- Minor editorial changes
0.83	13-07-2007	AFNOR	- Resolved comments on 0.73 (suite)
0.84	16-07-2007	BSI/Secunet	- Resolved comments on 0.73 (suite)
0.85	16-07-2007	BSI/Secunet	- Resolved comments on 0.73 (suite)
0.86	16-07-2007	AFNOR	- Minor editorial changes
0.87	18-07-2007	BSI/Secunet	- Fix expected results for ISO7816_I_8, ISO7816_J_14, ISO7816_J_16, ISO7816_K_8
0.88	19-07-2007	AFNOR	- Fix expected results for ISO7816_I_6
1.0	23-07-2007	BSI/Secunet	- Minor fix ISO7816_H_2 - Add clarification to ISO7816_I_8
1.1 RC1	13-11-2007	BSI/Secunet	- Resolved comments on 1.0 - Additional tests for EAC 1.1
1.1	23-11-2007	BSI/Secunet	- Resolved comments on 1.1 RC1

Version	Date	Editor	Description
1.11RC1	12-03-2008	BSI/Secunet	- Changes based on EAC 1.11
1.11RC2	15-04-2008	BSI/Secunet	- Changes based on EAC 1.11 - Paris testing
1.11RC3	25-04-2008	BSI/Secunet	- Resolved comments on 1.1 RC2
1.11	30-04-2008	BSI/Secunet	- Resolved comments on 1.1 RC3
1.12 RC1	03-07-2008	AFNOR/Soliatis	- ISO7816_K_19 test case addition
1.12 RC2	07-08-2008	BSI/Secunet	- Resolved comments from Ispra testing
1.12 RC3	25-09-2008	BSI/Secunet	- Resolved comments from Prague testing
1.12	03-10-2008	BSI/Secunet	- Released without changes
1.2 RC1	16-04-2012	BSI	- Added test cases for PACE/TA binding and Chip Authentication with MSE:Set AT & General Authenticate commands
1.2. RC2	13-06-2012	BSI/AFNOR	- Resolved comments from AFNOR
1.2 RC3	21-06-2012	BSI/AFNOR	- Minor corrections
1.2 RC4	08-11-2012	BSI	- Resolved comments on V1.2RC3 from Article 6 Technical Subgroup meeting
1.2 RC5	23-11-2012	BSI	- Minor clarifications on test case ISO7816_J_12 and ISO7816_L_13
1.2 RC6	30-11-2012	BSI/AFNOR	- Resolved comments from AFNOR
1.2	05-12-2012	BSI/AFNOR	- Released finalized version 1.2
1.3	25-02-2013	BSI	- Minor corrections
1.4	13-03-2014	BSI/AFNOR	- Minor clarifications on test case ISO7816_II_4, ISO7816_L_13 and ISO7816_L_14

Content

1 Introduction 9
  1.1 Abbreviations 9
  1.2 Reference documentation 10
  1.3 Terminology 10

2 General test requirements 11
  2.1 Test setup 11
  2.2 Test profiles 12
  2.3 Key pair definition 13
  2.4 Certificate specification 14
    2.4.1 Certificate Set 1 15
    2.4.2 Certificate Set 2 24
    2.4.3 Certificate Set 3 27
    2.4.4 Certificate Set 4 29
    2.4.5 Certificate Set 5 31
    2.4.6 Certificate Set 6 32
    2.4.7 Certificate Set 7 36
    2.4.8 Certificate Set 8 38
    2.4.9 Certificate Set 10 41
    2.4.10 Certificate Set 11 45
    2.4.11 Certificate Set 12 52
    2.4.12 Certificate Set 13 65
    2.4.13 Certificate Set 14 68

3 Tests for layer 6 (ISO 7816) 72
  3.1 Test case notation 72
  3.2 General requirements 72
    3.2.1 Security Status 72
    3.2.2 Extended length APDUs 73
  3.3 Unit ISO7816_H – Security Conditions for EAC protected MRTDs 73
    3.3.1 Test case ISO7816_H_1 73
    3.3.2 Test case ISO7816_H_2 74
    3.3.3 Test case ISO7816_H_3 74
    3.3.4 Test case ISO7816_H_4 74
    3.3.5 Test case ISO7816_H_5 75
    3.3.6 Test case ISO7816_H_6 75
    3.3.7 Test case ISO7816_H_7 76
    3.3.8 Test case ISO7816_H_8 76
    3.3.9 Test case ISO7816_H_9 77
    3.3.10 Test case ISO7816_H_10 77
    3.3.11 Test case ISO7816_H_11 78
    3.3.12 Test case ISO7816_H_12 78
    3.3.13 Test case ISO7816_H_13 79
    3.3.14 Test case ISO7816_H_14 79

3.3.15 Test case ISO7816_H_15 79
3.3.16 Test case ISO7816_H_16 80
3.4 Unit ISO7816_I – Chip Authentication (MSE:Set KAT) 81
3.4.1 Test case ISO7816_I_1 81
3.4.2 Test case ISO7816_I_2 82
3.4.3 Test case ISO7816_I_3 82
3.4.4 Test case ISO7816_I_4 83
3.4.5 Test case ISO7816_I_5 84
3.4.6 Test case ISO7816_I_6 84
3.4.7 Test case ISO7816_I_7 85
3.4.8 Test case ISO7816_I_8 85
3.4.9 Test case ISO7816_I_9 86
3.4.10 Test case ISO7816_I_10 86
3.4.11 Test case ISO7816_I_11 87
3.4.12 Test case ISO7816_I_12 88
3.4.13 Test case ISO7816_I_13 88
3.4.14 Test case ISO7816_I_14 89
3.4.15 Test case ISO7816_I_15 90
3.4.16 Test case ISO7816_I_16 90
3.4.17 Test case ISO7816_I_17 91
3.5 Unit ISO7816_II – Chip Authentication (MSE:Set AT & GA) 91
3.5.1 Test case ISO7816_II_1 92
3.5.2 Test case ISO7816_II_2 92
3.5.3 Test case ISO7816_II_3 93
3.5.4 Test case ISO7816_II_4 94
3.5.5 Test case ISO7816_II_5 95
3.5.6 Test case ISO7816_II_6 95
3.5.7 Test case ISO7816_II_7 96
3.5.8 Test case ISO7816_II_8 97
3.5.9 Test case ISO7816_II_9 97
3.5.10 Test case ISO7816_II_10 98
3.5.11 Test case ISO7816_II_11 99
3.5.12 Test case ISO7816_II_12 100
3.5.13 Test case ISO7816_II_13 100
3.5.14 Test case ISO7816_II_14 101
3.5.15 Test case ISO7816_II_15 102
3.6 Unit ISO7816_J – Certificate verification 103
3.6.1 Test case ISO7816_J_1 103
3.6.2 Test case ISO7816_J_2 104
3.6.3 Test case ISO7816_J_3 105
3.6.4 Test case ISO7816_J_4 106
3.6.5 Test case ISO7816_J_5 107
3.6.6 Test case ISO7816_J_6 108
3.6.7 Test case ISO7816_J_7 109

3.6.8 Test case ISO7816_J_8 110
3.6.9 Test case ISO7816_J_9 111
3.6.10 Test case ISO7816_J_10 112
3.6.11 Test case ISO7816_J_11 114
3.6.12 Test case ISO7816_J_12 115
3.6.13 Test case ISO7816_J_13 117
3.6.14 Test case ISO7816_J_14 117
3.6.15 Test case ISO7816_J_15 117
3.6.16 Test case ISO7816_J_16 118
3.6.17 Test case ISO7816_J_17 118
3.6.18 Test case ISO7816_J_18 119
3.6.19 Test case ISO7816_J_19 120
3.6.20 Test case ISO7816_J_20 121
3.6.21 Test case ISO7816_J_21 122
3.6.22 Test case ISO7816_J_22 124
3.6.23 Test case ISO7816_J_23 125
3.6.24 Test case ISO7816_J_24 126
3.6.25 Test case ISO7816_J_25 127
3.6.26 Test case ISO7816_J_26 128
3.6.27 Test case ISO7816_J_27 129
3.6.28 Test case ISO7816_J_28 130
3.6.29 Test case ISO7816_J_29 131
3.6.30 Test case ISO7816_J_30 132
3.6.31 Test case ISO7816_J_31 133
3.6.32 Test case ISO7816_J_32 134
3.6.33 Test case ISO7816_J_33 135
3.6.34 Test case ISO7816_J_34 136
3.6.35 Test case ISO7816_J_35 138
3.6.36 Test case ISO7816_J_36 138
3.6.37 Test case ISO7816_J_37 140
3.6.38 Test case ISO7816_J_38 141
3.6.39 Test case ISO7816_J_39 142
3.6.40 Test case ISO7816_J_40 143
3.6.41 Test case ISO7816_J_41 144
3.6.42 Test case ISO7816_J_42 145
3.6.43 Test case ISO7816_J_43 145
3.6.44 Test case ISO7816_J_44 146
3.6.45 Test case ISO7816_J_45 147
3.6.46 Test case ISO7816_J_46 148
3.6.47 Test case ISO7816_J_47 149
3.6.48 Test case ISO7816_J_48 150
3.6.49 Test case ISO7816_J_49 151
3.6.50 Test case ISO7816_J_50 152
3.6.51 Test case ISO7816_J_51 153

3.6.52 Test case ISO7816_J_52 154
3.6.53 Test case ISO7816_J_53 155
3.6.54 Test case ISO7816_J_54 157
3.6.55 Test case ISO7816_J_55 157
3.5.56 Test case ISO7816_J_56 158
3.7 Unit ISO7816_K – Terminal Authentication 159
3.7.1 Test case ISO7816_K_1 159
3.7.2 Test case ISO7816_K_2 161
3.7.3 Test case ISO7816_K_3 163
3.7.4 Test case ISO7816_K_4 163
3.7.5 Test case ISO7816_K_5 164
3.7.6 Test case ISO7816_K_6 165
3.7.7 Test case ISO7816_K_7 166
3.7.8 Test case ISO7816_K_8 167
3.7.9 Test case ISO7816_K_9 167
3.7.10 Test case ISO7816_K_10 167
3.7.11 Test case ISO7816_K_11 169
3.7.12 Test case ISO7816_K_12 169
3.7.13 Test case ISO7816_K_13 170
3.7.14 Test case ISO7816_K_14 170
3.7.15 Test case ISO7816_K_15 172
3.7.16 Test case ISO7816_K_16 173
3.7.17 Test case ISO7816_K_17 173
3.7.18 Test case ISO7816_K_18 175
3.7.19 Test case ISO7816_K_19 176
3.7.20 Test case ISO7816_K_20 178
3.8 Unit ISO7816_L – Effective Access Conditions 179
3.8.1 Test case ISO7816_L_1 179
3.8.2 Test case ISO7816_L_2 181
3.8.3 Test case ISO7816_L_3 182
3.8.4 Test case ISO7816_L_4 184
3.8.5 Test case ISO7816_L_5 185
3.8.6 Test case ISO7816_L_6 187
3.8.7 Test case ISO7816_L_7 188
3.8.8 Test case ISO7816_L_8 190
3.8.9 Test case ISO7816_L_9 191
3.8.10 Test case ISO7816_L_10 192
3.8.11 Test case ISO7816_L_11 194
3.8.12 Test case ISO7816_L_12 195
3.8.13 Test case ISO7816_L_13 196
3.8.14 Test case ISO7816_L_14 198
3.9 Unit ISO7816_M – Update mechanism 200
3.9.1 Test case ISO7816_M_1 200
3.9.2 Test case ISO7816_M_2 201

3.9.3 Test case ISO7816_M_3 203
3.9.4 Test case ISO7816_M_4 205
3.9.5 Test case ISO7816_M_5 206
3.9.6 Test case ISO7816_M_6 207
3.10 Unit ISO7816_N – Migration policies 208
3.10.1 Test case ISO7816_N_1 208
4 Tests for layer 7 (LDS) 210
4.1 Unit LDS_E – Data group 14 210
4.1.1 Test case LDS_E_1 210
4.1.2 Test case LDS_E_2 210
4.1.3 Test case LDS_E_3 211
4.1.4 Test case LDS_E_4 212
4.1.5 Test case LDS_E_5 213
4.2 Unit LDS_F – EF.CVCA 213
4.2.1 Test case LDS_F_1 213
4.3 Unit LDS_G – Data group 3 214
4.3.1 Test case LDS_G_1 214
4.3.2 Test case LDS_G_2 214
4.3.3 Test case LDS_G_3 214
4.3.4 Test case LDS_G_4 215
4.3.5 Test case LDS_G_5 215
4.3.6 Test case LDS_G_6 215
4.3.7 Test case LDS_G_7 216
4.3.8 Test case LDS_G_8 216
4.3.9 Test case LDS_G_9 217
4.3.10 Test case LDS_G_10 217
4.3.11 Test case LDS_G_11 218
4.4 Unit LDS_H – Data group 4 218
4.4.1 Test case LDS_H_1 218
4.4.2 Test case LDS_H_2 218
4.4.3 Test case LDS_H_3 219
4.4.4 Test case LDS_H_4 219
4.4.5 Test case LDS_H_5 219
4.4.6 Test case LDS_H_6 220
4.4.7 Test case LDS_H_7 220
4.4.8 Test case LDS_H_8 221
4.4.9 Test case LDS_H_9 221
4.4.10 Test case LDS_H_10 222
4.4.11 Test case LDS_H_11 222
Annex A Implementation conformance statement 223
A.1 Supported profiles 223
A.2 Supported cryptographic algorithm 223
A.3 Cryptosystem migration policy 224
A.4 CVCA trust point information 224

1 Introduction

The TR 03105 defines a RF protocol and application test standard for machine readable travel documents (eMRTDs).

This document enhances this test plan for machine readable travel documents (eMRTDs) with advanced security mechanisms. These mechanisms are used to protect the additional and more sensitive biometric data like fingerprints introduced with the second generation of eMRTDs.

As the original test plan, this specification has a layer based structure. The layers 1 - 4 refer the RF protocol according to the ISO 14443 1-4 standard. Since the advanced security mechanisms have no direct influence on this abstraction layer, this amendment does not contain any additional test for these layers. In the future it may be useful to define an EAC specific test command sequence for the tests of layer 1-4.

However, this document concentrates on the additional tests for the layer 6 (ISO 7816) and 7 (LDS encoding). For a full conformance test for EAC protected MRTDs, the tests specified in this document MUST be performed in addition to the original tests as described in [R8].

1.1 Abbreviations

Abbreviation	
APDU	Application Protocol Data Unit
AT	Authentication Template
BAC	Basic Access Control
CA	Chip Authentication
CAN	Card Access Number
CAR	Certification Authority Reference
CHR	Cardholder reference
CVCA	Country Verifying Certification Authority
DG	Data Group
EAC	Extended Access Control
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
DH	Diffie-Hellman
DST	Digital Signature Template
DV	Document Verifier
ICS	Implementation Conformance Statement
IS	Inspection System
LDS	Logical Data Structure
KAEG	Key Agreement ElGamal-type
KAT	Key Agreement Template
MSE	Manage Security Environment
OID	Object Identifier
PACE	Password Authenticated Connection Establishment
PSO	Perform Security Operation
RSA	Rivest Shamir Adleman
TA	Terminal Authentication

1.2 Reference documentation

The following documentation serves as a reference for this specification:

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

[R2] Technical Guideline TR-03110-1 “Advanced Security Mechanisms for Machine 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 to Doc ICAO 9303 Release 11, 17. November 2011

[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] ADVANCED SECURITY MECHANISMS FOR MACHINE READABLE
TRAVEL DOCUMENTS – EXTENDED ACCESS CONTROL (EACv1)
Complementary test methods for MRTDs using static binding

[R11] Technical Guideline TR-03110-3 “Advanced Security Mechanisms for Machine Readable Travel Documents - Part 3: Common Specifications”, Version 2.10, March 2012

1.3 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

For setting up these tests, any contactless reader supporting type A and type B protocols can be used. However, this reader has to support extended length APDUs requested for Terminal Authentication.

One personalized eMRTD sample is needed for executing the tests.

Some of the tests specified for layer 6 (ISO7816) rely on the proper coding of the logical data structure stored in the chip (esp. data group 14 and the EF.CVCA file). Therefore it is RECOMMENDED that the layer 7 tests (LDS) are performed before the layer 6 tests to detect coding related issues beforehand.

IMPORTANT NOTE: This test plan contains certain test cases which verify the MRTDs behavior with expired certificates. During these test, the effective date stored inside the chip is changed. For these tests a set of certificates can be used only once with a single eMRTD sample. After these tests have been performed, another sample or a new set of certificates is needed to repeat the tests. Therefore it is recommended to perform these tests as the last one in a test sequence.

As already mentioned in the introduction of this document, the test cases specified herein have to be performed in addition to the test defined in [R8].

However some of the original test cases will fail with an EAC enabled eMRTD. This is because of the restricted access conditions to the data groups 3 and 4. This concerns the following test cases:

ISO7816_B_41

ISO7816_B_42

ISO7816_D_9

ISO7816_D_10

ISO7816_E_9

ISO7816_E_10

LDS_D_06

All these test case have an established BAC session as a test requirement. For eMRTDs with EAC these tests MUST be performed with an established EAC session. It is RECOMMENDED to perform the BAC tests before the EAC related test cases and to use the DV_CERT_1 and IS_CERT_1 as defined in this document to establish an EAC session when needed.

Most of the test cases in this document require an established PACE or BAC session and a selected ePassport Application as described in [R2] and [R9]. In the preconditions this procedure is called “Open ePassport Application”. If the Open ePassport Application procedure is performed with PACE the MRZ SHALL be used.

Throughout this document, the term PACE refers to PACEv2.

2.2 Test profiles

This test plan refers to the EACv1 specification as described in [R2] and [R11]. The test objects MUST fully comply with this version.

In addition to the profiles already specified in the original test plan this amendment defines the following additional profiles.

Profile-ID	Profile	Remark
CA_KAT	Chip Authentication with MSE:Set KAT	A MRTD which does not contain sensitive biometric data, like finger prints, can still use the Chip Authentication mechanism to support chip cloning protection and strong communication encryption. The support of CA is indicated by the presence of the LDS data group 14.Chip Authentication with 3DES Secure Messaging will use the command MSE:Set KAT.
CA_ATGA	Chip Authentication with MSE:Set AT & General Authenticate	A MRTD which does not contain sensitive biometric data, like finger prints, can still use the Chip Authentication mechanism to support chip cloning protection and strong communication encryption. The support of CA is indicated by the presence of the LDS data group 14. Chip Authentication with AES Secure Messaging will use the commands MSE:Set AT and General Authenticate. Additionally, these commands may be used for Chip Authentication with 3DES.
DH	Diffie-Hellman	According to the EAC specification, the chip can support Diffie-Hellman or elliptic curve based Diffie-Hellman key agreement algorithms. Test cases which belong to the DH profile are only applicable if the DH algorithm is used.
ECDH	Elliptic Curve Diffie-Hellman	According to the EAC specification, the chip can support Diffie-Hellman or elliptic curve based Diffie-Hellman key agreement algorithms. Test cases which belong to the ECDH profile are only applicable if the elliptic curve based DH algorithm is used.
KeyRef	Explicit key selection supported	This profile signals that a chip supports the explicit selection of the private key used for Chip Authentication. In this case, the private key reference is defined in the DataGroup 14.
TA	Terminal Authentication	In addition to the Chip Authentication mechanism the Terminal Authentication profile is used by MRTDs with sensitive biometric data to protect the file access for the data group 3 and/or 4.
ECDSA	Elliptic curve algorithm	According to the EAC specification a chip is free to support either elliptic curve or RSA based keys. All tests which belong to the ECDSA profile MUST only be processed if the test object is personalized with elliptic curve based keys.
RSA	RSA algorithm	According to the EAC specification a chip is free to support either elliptic curve or RSA based keys. All tests which belong to the RSA profile MUST only be processed if the test object is personalized with RSA

Profile-ID	Profile	Remark
		based keys.
MIG	Migration	According to the EAC specification the algorithm used for the Terminal Authentication process can be changed with an appropriate link certificate if the chip supports more than one algorithm. The tests for this Migration profile MUST only be performed, if the chip supports the migration from one cryptosystem to another. This must be stated in the ICS.
DATE	Date validation	Since the validation of the certificates effective and expiration date is not explicitly required by the EAC specification, the optional tests which belong to the Date validation profile must only be performed if this is supported by the chip. This must be stated in the ICS.
PACE	Password Authenticated Connection Establishment	In some test cases the binding between PACE and Terminal Authentication is tested. In these cases the eMRTD must support the PACE protocol.
DG3	Data Group 3	According to ICAO Doc 9303 [R1] Data Group 3 is optional. If chip contains encoded fingerprints in DG3 this optional test cases have to be performed.
DG4	Data Group 4	According to ICAO Doc 9303 [R1] Data Group 4 is optional. If chip contains encoded iris scans in DG4 this optional test cases have to be performed.

2.3 Key pair definition

The certificate sets defined in chapter 2.4 are based on several asymmetric key pairs. In preparation to the tests, these key pairs have to be generated. The parameter used for these keys are depending on the initial CVCA private key.

The initial CVCA root private key SHOULD be provided by the eMRTD vendor. It is also possible the eMRTD vendor generates all keys and certificates on its own and passes it to the test operator for the tests.

For the key set 13 (CVCA_KEY_13, DV_KEY_13, IS_KEY_13) the algorithm for the cryptosystem migration MUST be used as defined in the ICS.

All key pairs MUST be generated independently, so it is not permitted to use the same key pair for all sets.

Key pair	
CVCA_KEY_00	The key pair CV_KEY_00 is the public/private key for the initial CVCA root.
DV_KEY_01	Key pair of the test DV 01
IS_KEY_01	Key pair of the test IS 01
DV_KEY_02	Key pair of the test DV 02
IS_KEY_02	Key pair of the test IS 02
DV_KEY_03	Key pair of the test DV 03
IS_KEY_03	Key pair of the test IS 03
DV_KEY_04	Key pair of the test DV 04

Key pair	
IS_KEY_04	Key pair of the test IS 04
DV_KEY_05	Key pair of the test DV 05
IS_KEY_05	Key pair of the test IS 05
DV_KEY_06	Key pair of the test DV 06
IS_KEY_06	Key pair of the test IS 06
CVCA_KEY_07	Key pair of the test CVCA 07
DV_KEY_07	Key pair of the test DV 07
IS_KEY_07	Key pair of the test IS 07
CVCA_KEY_08	Key pair of the test CVCA 08
CVCA_KEY_09	Key pair of the test CVCA 09
DV_KEY_09	Key pair of the test DV 09
CVCA_KEY_10	Key pair of the test CVCA 10
DV_KEY_10	Key pair of the test DV 10
IS_KEY_10	Key pair of the test IS 10
CVCA_KEY_11	Key pair of the test CVCA 11
DV_KEY_11	Key pair of the test DV 11
IS_KEY_11	Key pair of the test IS 11
DV_KEY_12	Key pair of the test DV 12
CVCA_KEY_13	Key pair of the test CVCA 13
DV_KEY_13	Key pair of the test DV 13
IS_KEY_13	Key pair of the test IS 13
DV_KEY_14a	Key pair of the test DV 14 (length equal to CVCA Key length)
DV_KEY_14b	Key pair of the test DV 14 (MUST be shorter than CVCA Key length)
IS_KEY_14a	Key pair of the test IS 14 (length equal to CVCA Key length)
IS_KEY_14b	Key pair of the test IS 14 (MUST be shorter than CVCA Key length)

2.4 Certificate specification

Since the advanced security mechanisms are using a certificate based authentication schema it is necessary to provide a set of well prepared certificates in order to perform all tests.

This chapter defines the exact set of certificates referred in the tests. Besides the regular certificate chain there is also the need for special encoded certificates.

The certificates are specified in two different ways. For provider of personalized eMRTD samples, which do already have a preconfigured trust point based on their own CVCA key pair, the chapters below defines a set of certificates relative to the effective date ($CVCA_{eff}$) and expiration date($CVCA_{exp}$) of the given the CVCA. The time span between $CVCA_{eff}$ and $CVCA_{exp}$ MUST be at least two month to allow proper adoption of the certificate time scheme defined below. The “current date” of the provided sample MUST be set to $CVCA_{eff}$ before the tests are started. The provider of the sample or the test laboratory has to generate the corresponding certificate according to this specification based on the CVCA data.

If no preconfigured key pair is available or if the production process allows the use of an externally defined CVCA, a certificate set can be used which is defined as a “worked example” by this specification. This set is provided for ECDSA, RSA and RSAPSS based certificates and is defined in a full binary form with fixed keys and dates. It also includes a definition for an initial CVCA key pair and its effective and expiry dates.

2.4.1 Certificate Set 1

The certificate set consist of a regular certificate chain (DV -> IS) which is used for the positive tests regarding the certificate verification. Furthermore it contains variants of the original DV certificate to simulate a variety of certificate coding issues (missing elements, badly encoded dates …).

2.4.1.1 DV_CERT_1

ID	DV_CERT_1
Purpose	This certificate is a regular DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.
Version	1.11
Referred by	ISO7816_J_1, ISO7816_J_2, ISO7816_J_3, ISO7816_J_4, ISO7816_J_5, ISO7816_J_12, ISO7816_J_15, ISO7816_J_17, ISO7816_J_18, ISO7816_J_22, ISO7816_J_25, ISO7816_J_26, ISO7816_J_27, ISO7816_J_28, ISO7816_J_29, ISO7816_J_30, ISO7816_J_31, ISO7816_J_32, ISO7816_J_33, ISO7816_J_34, ISO7816_J_35, ISO7816_J_36, ISO7816_J_37, ISO7816_J_38, ISO7816_J_39, ISO7816_J_40, ISO7816_J_41, ISO7816_K, ISO7816_L_9, ISO7816_L_10, ISO7816_L_11, ISO7816_L_12, ISO7816_L_13 The DV_CERT_1 SHOULD also be used for all other test cases that rely on a established EAC session to access DG3 and DG4 (like the LDS unit G and H, or the BAC test cases mentioned in 2.1.

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE001
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_01

	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.1.2 DV_CERT_1a

ID	DV_CERT_1a
Purpose	This certificate is similar to DV_CERT_1, but does not contain a Certificate Holder Authorization
Version	1.11
Referred by	ISO7816_J_6

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
      7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
            5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE001
	Certificate Holder Authorisation	absent
	Certificate effective date	$CVCA_{eff}$
	Certificate expiration date	$CVCA_{eff}$ + 1 month
	Public Key reference	Public key of key pair DV_KEY_01
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.1.3 DV_CERT_1b

ID	DV_CERT_1b
Purpose	This certificate is similar to DV_CERT_1, but does not contain a Certificate Effective Date
Version	1.11
Referred by	ISO7816_J_7

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE001
	Certificate Holder Authorization	domestic DV, DG 3, DG 4
	Certificate effective date	absent
	Certificate expiration date	CVCA_{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_01
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.1.4 DV_CERT_1c

ID	DV_CERT_1c
Purpose	This certificate is similar to DV_CERT_1, but does not contain a Certificate Expiration Date
Version	1.11
Referred by	ISO7816_J_8

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object

	cc is the encoded length of the Certificate Authority Reference *dd* is the placeholder for the Certificate Authority Reference (cc bytes) *ee* is the encoded length of the certificates public key, *ff* is the placeholder for the certificates public key bytes (ee bytes), *gg* is the placeholder for the BCD encoded effective date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE001
	Certificate Holder Authorization	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	absent
	Public Key reference	Public key of key pair DV_KEY_01
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.1.5 DV_CERT_1d

ID	DV_CERT_1d
Purpose	This certificate is similar to DV_CERT_1, but contains a badly encoded Certificate Effective Date (Invalid BCD encoding)
Version	1.11
Referred by	ISO7816_J_9

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 0A 0B 0C 0D 0E 0F
            5F 24 06 hh
      5F 37 ii jj
```

	aa is the encoded combined length of certificate body and signature objects *bb* is the encoded length the certificate body object *cc* is the encoded length of the Certificate Authority Reference *dd* is the placeholder for the Certificate Authority Reference (cc bytes) *ee* is the encoded length of the certificates public key, *ff* is the placeholder for the certificates public key bytes (ee bytes), *hh* is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE001
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	0A 0B 0C 0D 0E 0F (invalid BCD encoding)

	Certificate expiration date	CVCA$_{\text{eff}}$ + 1 month
	Public Key reference	Public key of key pair DV_KEY_01
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.1.6 DV_CERT_1e

ID	DV_CERT_1e	
Purpose	This certificate is similar to DV_CERT_1, but contains a badly encoded Certificate Expiration Date(Invalid BCD encoding)	
Version	1.11	
Referred by	ISO7816_J_10	

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 0A 0B 0C 0D 0E 0F
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE001
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA$_{\text{eff}}$
	Certificate expiration date	0A 0B 0C 0D 0E 0F (invalid BCD encoding)
	Public Key reference	Public key of key pair DV_KEY_01
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.1.7 DV_CERT_1f

ID	DV_CERT_1f
Purpose	This certificate is similar to DV_CERT_1, but contains a badly encoded Certificate Effective Date (Invalid Gregorian date)
Version	1.11

Referred by	ISO7816_J_19
Content definition	

```
7F 21 aa
        7F 4E bb
                5F 29 01 00
                42 cc dd
                7F 49 ee ff
                5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
                7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
        5F 25 06 gg
                5F 24 06 hh
        5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE001
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	The month and the year used as defined by the CVCA_{eff} and the day is always set to the 32nd so that it becomes an invalid Gregorian date.
	Certificate expiration date	CVCA_{exp}
	Public Key reference	Public key of key pair DV_KEY_01
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.1.8 DV_CERT_1g

ID	DV_CERT_1g
Purpose	This certificate is similar to DV_CERT_1, but contains a badly encoded Certificate Expiration Date (Invalid Gregorian date)
Version	1.11
Referred by	ISO7816_J_20
Content definition	

```
7F 21 aa
        7F 4E bb
                5F 29 01 00
                42 cc dd
                7F 49 ee ff
                5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
                7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
        5F 25 06 gg
        5F 24 06 hh
    5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE001
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	$CVCA_{eff}$
	Certificate expiration date	The month and the year used as defined by the $CVCA_{eff}$ and the day is always set to the 32nd so that it becomes an invalid Gregorian date.
	Public Key reference	Public key of key pair DV_KEY_01
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.1.9 DV_CERT_1h

ID	DV_CERT_1h
Purpose	This certificate is similar to DV_CERT_1, but contains a Certificate Expiration Date BEFORE the Certificate Effective Date
Version	1.11
Referred by	ISO7816_J_21
Content definition	

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 cc dd
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
    5F 25 06 gg
        5F 24 06 hh
    5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate

	hh is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE001
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA$_{\mathrm{eff}}$ + 1 day
	Certificate expiration date	CVCA$_{\mathrm{eff}}$
	Public Key reference	Public key of key pair DV_KEY_01
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.1.10 DV_CERT_1i

ID	DV_CERT_1i
Purpose	This certificate is similar to DV_CERT_1, but contains a Certificate Holder Authorization with an invalid OID
Version	1.11
Referred by	ISO7816_J_23

Content definition

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 cc dd
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 01 83
    5F 25 06 gg
        5F 24 06 hh
    5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE001
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA$_{\mathrm{eff}}$
	Certificate expiration date	CVCA$_{\mathrm{eff}}$ + 1 month
	Public Key reference	Public key of key pair DV_KEY_01

	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.1.11 DV_CERT_1j

ID	DV_CERT_1j
Purpose	This certificate is similar to DV_CERT_1, but contains a Public Key with an invalid OID
Version	1.12
Referred by	ISO7816_J_24

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE001
	Certificate Public Key	Bad OID (Use 0.4.0.127.0.7.2.2.2.5.1)
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_01
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.1.12 IS_CERT_1

ID	IS_CERT_1
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_1
Version	1.11
Referred by	ISO7816_J_1, ISO7816_J_2, ISO7816_J_3, ISO7816_J_4, ISO7816_J_5,

	ISO7816_J_6, ISO7816_J_7, ISO7816_J_8, ISO7816_J_9, ISO7816_J_10, ISO7816_J_17, ISO7816_J_18, ISO7816_J_19, ISO7816_J_20, ISO7816_J_21, ISO7816_J_22, ISO7816_J_23, ISO7816_J_24, ISO7816_K, ISO7816_L_9, ISO7816_L_10, ISO7816_L_11, ISO7816_L_12, ISO7816_L_13

Content definition

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 30 31
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
        5F 25 06 gg
        5F 24 06 hh
  5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTDVDE001
	Certificate Holder Reference	DETESTISDE001
	Certificate Holder Authorisation	IS, DG 3, DG 4
	Certificate effective date	$\mathrm{CVCA}_{\mathrm{eff}}$
	Certificate expiration date	$\mathrm{CVCA}_{\mathrm{eff}}$ + 14 days
	Public Key reference	Public key of key pair IS_KEY_01
	Signing Key reference	Signed with the private key of key pair DV_KEY_01

2.4.2 Certificate Set 2

This certificate set contains certificates which are used to verify the behaviour of ePassports in respect to foreign IS certificates.

2.4.2.1 DV_CERT_2

ID	DV_CERT_2
Purpose	This certificate is a regular foreign DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.
Version	1.11
Referred by	ISO7816_J_11

Content definition

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 cc dd
```

```
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 32
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 43
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE002
	Certificate Holder Authorization	foreign DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_02
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.2.2 IS_CERT_2a

ID	IS_CERT_2a
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_2. It has an advanced effective date. (Beyond the expiration date of IS_CERT_2b).
Version	1.11
Referred by	ISO7816_J_11
Content definition	

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 0D 44 45 54 45 53 54 44 56 44 45 30 30 32
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 30 32
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
            5F 25 06 gg
            5F 24 06 hh
   5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,

	ff is the placeholder for the certificates public key bytes (ee bytes), *gg* is the placeholder for the BCD encoded effective date of the certificate *hh* is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	DETESTDVDE002
	Certificate Holder Reference	DETESTISDE002
	Certificate Holder Authorisation	IS, DG 3, DG 4
	Certificate effective date	CVCA_{eff} + 14 days
	Certificate expiration date	CVCA_{eff} + 1 month
	Public Key reference	Public key of key pair IS_KEY_02
	Signing Key reference	Signed with the private key of key pair DV_KEY_02

2.4.2.3 IS_CERT_2b

ID	IS_CERT_2b
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_2. It has an expiration date BEFORE the effective date of IS_CERT_2a.
Version	1.11
Referred by	ISO7816_J_11
Content definition	

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 0D 44 45 54 45 53 54 44 56 44 45 30 30 32
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 30 32
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
        5F 25 06 gg
        5F 24 06 hh
  5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTDVDE002
	Certificate Holder Reference	DETESTISDE002
	Certificate Holder Authorisation	IS, DG 3, DG 4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{eff} + 13 days
	Public Key reference	Public key of key pair IS_KEY_02

	Signing Key reference	Signed with the private key of key pair DV_KEY_02

2.4.3 Certificate Set 3

The certificate set follows a certification scheme where the DV permits full access to data group 3 and 4 while the IS certificate restricts the access to specific data group.

2.4.3.1 DV_CERT_3

ID	DV_CERT_3
Purpose	This certificate is a regular DV certificate, with access rights for both data group 3 AND 4.
Version	1.11
Referred by	ISO7816_L_1, ISO7816_L_2, ISO7816_L_3, ISO7816_L_4

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 33
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE003
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	$CVCA_{eff}$
	Certificate expiration date	$CVCA_{eff}$ + 1 month
	Public Key reference	Public key of key pair DV_KEY_03
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.3.2 IS_CERT_3a

ID	IS_CERT_3a
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_3. It encodes access rights for data group 3 only.
Version	1.11
Referred by	ISO7816_L_1, ISO7816_L_2
Content definition	

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 0D 44 45 54 45 53 54 44 56 44 45 30 30 33
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 30 33
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 01
            5F 25 06 gg
            5F 24 06 hh
   5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTDVDE003
	Certificate Holder Reference	DETESTISDE003
	Certificate Holder Authorisation	IS, DG 3
	Certificate effective date	CVCA$_{\text{eff}}$
	Certificate expiration date	CVCA$_{\text{eff}}$ + 1 month
	Public Key reference	Public key of key pair IS_KEY_03
	Signing Key reference	Signed with the private key of key pair DV_KEY_03

2.4.3.3 IS_CERT _3b

ID	IS_CERT_3b
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_3. It encodes access rights for data group 4 only.
Version	1.11
Referred by	ISO7816_L_3, ISO7816_L_4
Content definition	

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 0D 44 45 54 45 53 54 44 56 44 45 30 30 33
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 30 33
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 02
            5F 25 06 gg
            5F 24 06 hh
  5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTDVDE003
	Certificate Holder Reference	DETESTISDE003
	Certificate Holder Authorisation	IS, DG 4
	Certificate effective date	$\mathrm{CVCA}_{\mathrm{eff}}$
	Certificate expiration date	$\mathrm{CVCA}_{\mathrm{eff}}$ + 1 month
	Public Key reference	Public key of key pair IS_KEY_03
	Signing Key reference	Signed with the private key of key pair DV_KEY_03

2.4.4 Certificate Set 4

The certificate set follows a certification scheme where the DV permits only access to data group 3 while the IS certificate permits full access to data group 3 and 4.

2.4.4.1 DV_CERT_4

ID	DV_CERT_4
Purpose	This certificate is a regular DV certificate, with access rights for group 3 only.
Version	1.11
Referred by	ISO7816_L_5, ISO7816_L_6
Content definition	

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 34
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 81
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

	aa is the encoded combined length of certificate body and signature objects *bb* is the encoded length the certificate body object *cc* is the encoded length of the Certificate Authority Reference *dd* is the placeholder for the Certificate Authority Reference (cc bytes) *ee* is the encoded length of the certificates public key, *ff* is the placeholder for the certificates public key bytes (ee bytes), *gg* is the placeholder for the BCD encoded effective date of the certificate *hh* is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE004
	Certificate Holder Authorisation	domestic DV, DG 3
	Certificate effective date	$CVCA_{eff}$
	Certificate expiration date	$CVCA_{eff}$ + 1 month
	Public Key reference	Public key of key pair DV_KEY_04
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.4.2 IS_CERT_4

ID	IS_CERT_4
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_4. It encodes access rights for data group 3 AND data group 4.
Version	1.11
Referred by	ISO7816_L_5, ISO7816_L_6
Content definition	

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 0D 44 45 54 45 53 54 44 56 44 45 30 30 34
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 30 34
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
        5F 25 06 gg
        5F 24 06 hh
  5F 37 ii jj
```

	aa is the encoded combined length of certificate body and signature objects *bb* is the encoded length the certificate body object *ee* is the encoded length of the certificates public key, *ff* is the placeholder for the certificates public key bytes (ee bytes), *gg* is the placeholder for the BCD encoded effective date of the certificate *hh* is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	DETESTDVDE004

	Certificate Holder Reference	DETESTISDE004
	Certificate Holder Authorisation	IS, DG 3, DG 4
	Certificate effective date	CVCA$_{\text{eff}}$
	Certificate expiration date	CVCA$_{\text{eff}}$ + 1 month
	Public Key reference	Public key of key pair IS_KEY_04
	Signing Key reference	Signed with the private key of key pair DV_KEY_04

2.4.5 Certificate Set 5

The certificate set follows a certification scheme where the DV permits only access to data group 4 while the IS certificate permits full access to data group 3 and 4.

2.4.5.1 DV_CERT_5

ID	DV_CERT_5
Purpose	This certificate is a regular DV certificate, with access rights for group 4 only.
Version	1.11
Referred by	ISO7816_L_7, ISO7816_L_8

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 35
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 82
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE005
	Certificate Holder Authorisation	domestic DV, DG 4
	Certificate effective date	CVCA$_{\text{eff}}$
	Certificate expiration date	CVCA$_{\text{eff}}$ + 1 month
	Public Key reference	Public key of key pair DV_KEY_05

	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.5.2 IS_CERT_5

ID	IS_CERT_5
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_5. It encodes access rights for data group 3 AND data group 4.
Version	1.11
Referred by	ISO7816_L_7, ISO7816_L_8

Content definition

```
7F 21 aa
        7F 4E bb
                5F 29 01 00
                42 0D 44 45 54 45 53 54 44 56 44 45 30 30 35
                7F 49 ee ff
                5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 30 35
                7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
                5F 25 06 gg
                5F 24 06 hh
    5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTDVDE005
	Certificate Holder Reference	DETESTISDE005
	Certificate Holder Authorisation	IS, DG 3, DG 4
	Certificate effective date	CVCA$_{eff}$
	Certificate expiration date	CVCA$_{eff}$ + 1 month
	Public Key reference	Public key of key pair IS_KEY_05
	Signing Key reference	Signed with the private key of key pair DV_KEY_05

2.4.6 Certificate Set 6

This certificate set contains certificate which have different effective and expiration dates to test the ePassports behaviour in respect to the update of the effective date and with expired certificates.

2.4.6.1 DV_CERT_6

ID	DV_CERT_6
Purpose	This certificate is a domestic DV certificate, which validity period starts at the

	effective date of the CVCA and expires after one month.
Version	1.11
Referred by	ISO7816_M_1, ISO7816_M_2
Content definition	

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 36
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE006
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	$\mathrm{CVCA}_{\mathrm{eff}}$
	Certificate expiration date	$\mathrm{CVCA}_{\mathrm{eff}}$ + 1 month
	Public Key reference	Public key of key pair DV_KEY_06
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.6.2 DV_CERT_6a

ID	DV_CERT_6a
Purpose	This DV certificate is similar to DV_CERT_6, but the certificate effective date is beyond the DV_CERT_6 expiration date.
Version	1.11
Referred by	ISO7816_M_2
Content definition	

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 36
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
        5F 25 06 gg
            5F 24 06 hh
        5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE006
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff} + 1 month + 1 day
	Certificate expiration date	CVCA_{eff} + 2 month
	Public Key reference	Public key of key pair DV_KEY_06
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.6.3 IS_CERT_6a

ID	IS_CERT_6a
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_6. This IS certificate has an advanced effective date. (Beyond the expiration date of IS_CERT_6b)
Version	1.11
Referred by	ISO7816_M_1

Content definition

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 0D 44 45 54 45 53 54 44 56 44 45 30 30 36
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 30 36
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
        5F 25 06 gg
        5F 24 06 hh
  5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),

	gg is the placeholder for the BCD encoded effective date of the certificate *hh* is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	DETESTDVDE006
	Certificate Holder Reference	DETESTISDE006
	Certificate Holder Authorisation	IS, DG 3, DG 4
	Certificate effective date	CVCA_{eff} + 14 days
	Certificate expiration date	CVCA_{eff} + 1 month
	Public Key reference	Public key of key pair IS_KEY_06
	Signing Key reference	Signed with the private key of key pair DV_KEY_06

2.4.6.4 IS_CERT_6b

ID	IS_CERT_6b
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_6. This IS certificate has an expiration date BEFORE the effective date of IS_CERT_6a.
Version	1.11
Referred by	ISO7816_M_1

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 0D 44 45 54 45 53 54 44 56 44 45 30 30 36
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 30 36
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
            5F 25 06 gg
            5F 24 06 hh
   5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTDVDE006
	Certificate Holder Reference	DETESTISDE006
	Certificate Holder Authorisation	IS, DG 3, DG 4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{eff} + 13 days

	Public Key reference	Public key of key pair IS_KEY_06
	Signing Key reference	Signed with the private key of key pair DV_KEY_06

2.4.7 Certificate Set 7

This certificate set defines a link certificate used for the tests about the trust point update mechanism.

2.4.7.1 LINK_CERT_7

Note for ECDSA profile: Since the crypto mechanism is not changed by this link certificate it must be stated by the vendor of the test sample if the domain parameter should be included in this certificate (see ICS Annex A).

ID	LINK_CERT_7
Purpose	This certificate is a link certificate, which validity period starts one day before the original CVCA certificate expires.
Version	1.11
Referred by	ISO7816_M_3
Content definition	

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 10 44 45 54 45 53 54 5F 4C 49 4E 4B 44 45 30
30 37
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3
            5F 25 06 gg
            5F 24 06 hh
   5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETEST_LINKDE007
	Certificate Holder Authorisation	CVCA, DG 3, DG 4
	Certificate effective date	CVCA_{exp} - 1 day
	Certificate expiration date	CVCA_{exp} + 2 month
	Public Key reference	Public key of key pair CVCA_KEY_07

	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.7.2 DV_CERT_7a

ID	DV_CERT_7a
Purpose	This certificate is a domestic DV certificate, which was issued by the original CVCA.
Version	1.11
Referred by	ISO7816_M_3

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 37
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE007
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{exp}
	Public Key reference	Public key of key pair DV_KEY_07
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.7.3 DV_CERT_7b

ID	DV_CERT_7b
Purpose	This certificate is a domestic DV certificate, which was issued by the update CVCA (LINK_CERT_7).

Version	1.11
Referred by	ISO7816_M_3

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 10 44 45 54 45 53 54 5F 4C 49 4E 4B 44 45 30 30 37
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 37
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETEST_LINKDE007
	Certificate Holder Reference	DETESTDVDE007
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{exp} + 1 day
	Certificate expiration date	CVCA_{exp} + 1 month
	Public Key reference	Public key of key pair DV_KEY_07
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_07

2.4.8 Certificate Set 8

This certificate set defines a link certificate used for the tests about the trust point update mechanism.

Note for ECDSA profile: Since the crypto mechanism is not changed by the link certificates defined in this certificate set, it must be stated by the vendor of the test sample if the domain parameter should be included. (see ICS Annex A).

2.4.8.1 LINK_CERT_8

This link certificate is used to update the trust point defined by LINK_CERT_7.

ID	LINK_CERT_8
Purpose	This certificate is a link certificate, based on the LINK_CERT_7
Version	1.11
Referred by	ISO7816_M_4

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 10 44 45 54 45 53 54 5F 4C 49 4E 4B 44 45 30 30
37
            7F 49 ee ff
            5F 20 10 44 45 54 45 53 54 5F 4C 49 4E 4B 44 45 30
30 38
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3
            5F 25 06 gg
            5F 24 06 hh
  5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETEST_LINKDE007
	Certificate Holder Reference	DETEST_LINKDE008
	Certificate Holder Authorisation	CVCA, DG 3, DG 4
	Certificate effective date	CVCA_{exp} + 1 month
	Certificate expiration date	CVCA_{exp} + 4 month
	Public Key reference	Public key of key pair CVCA_KEY_08
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_07

2.4.8.2 LINK_CERT_9

ID	LINK_CERT_9
Purpose	This certificate is a link certificate, based on the LINK_CERT_8
Version	1.11
Referred by	ISO7816_M_4

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 10 44 45 54 45 53 54 5F 4C 49 4E 4B 44 45 30 30
38
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 43 41 44 45 30 30 39
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),

	gg is the placeholder for the BCD encoded effective date of the certificate *hh* is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	DETEST_LINKDE008
	Certificate Holder Reference	DETESTCADE009
	Certificate Holder Authorisation	CVCA, DG 3, DG 4
	Certificate effective date	CVCA$_{exp}$ + 3 month
	Certificate expiration date	CVCA$_{exp}$ + 6 month
	Public Key reference	Public key of key pair CVCA_KEY_09
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_08

2.4.8.3 DV_CERT_9

ID	DV_CERT_9
Purpose	This certificate is a domestic DV certificate, which was issued by LINK_CERT_9.
Version	1.11
Referred by	ISO7816_M_4

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 0D 44 45 54 45 53 54 44 56 44 45 30 30 39
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 39
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
            5F 25 06 gg
            5F 24 06 hh
  5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTCADE009
	Certificate Holder Reference	DETESTDVDE009
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA$_{exp}$ + 3 month
	Certificate expiration date	CVCA$_{exp}$ + 4 month
	Public Key reference	Public key of key pair DV_KEY_09
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_09

2.4.9 Certificate Set 10

2.4.9.1 LINK_CERT_10

ID	LINK_CERT_10
Purpose	This certificate is an irregular CVCA certificate. The signing key is a DV key.
Version	1.11
Referred by	ISO7816_J_44, ISO7816_J_45

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 43 41 44 45 30 31 30
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTDVDE010
	Certificate Holder Reference	As defined by the initial CVCA root
	Certificate Holder Authorisation	CVCA, DG 3, DG 4
	Certificate effective date	CVCA$_{\text{eff}}$
	Certificate expiration date	CVCA$_{\text{exp}}$
	Public Key reference	Public key of key pair CVCA_KEY_00
	Signing Key reference	Signed with the private key of key pair DV_KEY_10

2.4.9.2 DV_CERT_10a

ID	DV_CERT_10a
Purpose	This certificate is a regular domestic DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.
Version	1.11

Referred by	ISO7816_J_44, ISO7816_J_46, ISO7816_J_47

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 30
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE010
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_10
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.9.3 DV_CERT_10b

ID	DV_CERT_10b
Purpose	This certificate is a regular foreign DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.
Version	1.11
Referred by	ISO7816_J_45, ISO7816_J_48, ISO7816_J_49

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 30
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 43
      5F 25 06 gg
```

```
        5F 24 06 hh
    5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE010
	Certificate Holder Authorisation	foreign DV, DG 3, DG 4
	Certificate effective date	$\mathrm{CVCA}_{\mathrm{eff}}$
	Certificate expiration date	$\mathrm{CVCA}_{\mathrm{eff}}$ + 1 month
	Public Key reference	Public key of key pair DV_KEY_10
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.9.4 DV_CERT_10c

ID	DV_CERT_10c
Purpose	This certificate is an irregular DV domestic certificate. The signing key is a DV key.
Version	1.11
Referred by	ISO7816_J_46, ISO7816_J_48

Content definition

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 cc dd
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 30
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
    5F 25 06 gg
        5F 24 06 hh
    5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate

	`ii` is the encoded length of the certificates signature object, `jj` is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	DETESTDVDE010
	Certificate Holder Reference	DETESTDVDE010
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	$\mathrm{CVCA}_{\mathrm{eff}}$
	Certificate expiration date	$\mathrm{CVCA}_{\mathrm{eff}}$ + 1 month
	Public Key reference	Public key of key pair DV_KEY_10
	Signing Key reference	Signed with the private key of key pair DV_KEY_10

2.4.9.5 DV_CERT_10d

ID	DV_CERT_10d
Purpose	This certificate is an irregular DV foreign certificate. The signing key is a DV key.
Version	1.11
Referred by	ISO7816_J_47, ISO7816_J_49

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 30
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 43
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTDVDE010
	Certificate Holder Reference	DETESTDVDE010
	Certificate Holder Authorisation	foreign DV, DG 3, DG 4
	Certificate effective date	$\mathrm{CVCA}_{\mathrm{eff}}$
	Certificate expiration date	$\mathrm{CVCA}_{\mathrm{eff}}$ + 1 month
	Public Key reference	Public key of key pair DV_KEY_10
	Signing Key reference	Signed with the private key of key pair DV_KEY_10

2.4.9.6 IS_CERT_10

ID	IS_CERT_10
Purpose	This certificate is an irregular domestic IS certificate. This IS certificate is signed by the CVCA key.
Version	1.11
Referred by	ISO7816_J_43

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 31 30
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTISDE010
	Certificate Holder Authorisation	IS, DG 3, DG 4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{eff} + 13 days
	Public Key reference	Public key of key pair IS_KEY_10
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.10 Certificate Set 11

2.4.10.1 LINK_CERT_11a

ID	LINK_CERT_11a
Purpose	This certificate is a link certificate. The signing key is an IS key.
Version	1.11

Referred by	ISO7816_J_53

Content definition

```
7F 21 aa
        7F 4E bb
                5F 29 01 00
                42 cc dd
                7F 49 ee ff
                5F 20 0D 44 45 54 45 53 54 43 41 44 45 30 31 31
                7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3
        5F 25 06 gg
                5F 24 06 hh
        5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTISDE011
	Certificate Holder Reference	As defined by the initial CVCA root
	Certificate Holder Authorisation	CVCA, DG 3, DG 4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{exp}
	Public Key reference	Public key of key pair CVCA_KEY_00
	Signing Key reference	Signed with the private key of key pair IS_KEY_11

2.4.10.2 LINK_CERT_11b

ID	LINK_CERT_11b
Purpose	This certificate is a valid link certificate.
Version	1.11
Referred by	ISO7816_M_5

Content definition

```
7F 21 aa
        7F 4E bb
                5F 29 01 00
                42 cc dd
                7F 49 ee ff
                5F 20 0D 44 45 54 45 53 54 43 41 44 45 30 31 31
                7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3
        5F 25 06 gg
                5F 24 06 hh
        5F 37 ii jj
```

	aa is the encoded combined length of certificate body and signature objects *bb* is the encoded length the certificate body object *cc* is the encoded length of the Certificate Authority Reference *dd* is the placeholder for the Certificate Authority Reference (cc bytes) *ee* is the encoded length of the certificates public key, *ff* is the placeholder for the certificates public key bytes (ee bytes), *gg* is the placeholder for the BCD encoded effective date of the certificate *hh* is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	DETESTCADE009
	Certificate Holder Reference	DETESTCADE011
	Certificate Holder Authorisation	CVCA, DG 3, DG 4
	Certificate effective date	$CVCA_{exp}$ + 5 months
	Certificate expiration date	$CVCA_{exp}$ + 8 months
	Public Key reference	Public key of key pair CVCA_KEY_11
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_09

2.4.10.3 DV_CERT_11a

ID	DV_CERT_11a
Purpose	This certificate is a regular domestic DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.
Version	1.11
Referred by	ISO7816_J_50, ISO7816_J_51, ISO7816_J_52, ISO7816_J_53
Content definition	

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 31
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,

	jj is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE011
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_11
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.10.4 DV_CERT_11b

ID	DV_CERT_11b
Purpose	This certificate is an irregular foreign DV certificate. The signing key is an IS key.
Version	1.11
Referred by	ISO7816_J_50
Content definition	

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 cc dd
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 43
    5F 25 06 gg
        5F 24 06 hh
    5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTISDE011
	Certificate Holder Reference	DETESTDVDE011
	Certificate Holder Authorisation	foreign DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_11
	Signing Key reference	Signed with the private key of key pair IS_KEY_11

2.4.10.5 DV_CERT_11c

ID	DV_CERT_11c
Purpose	This certificate is an irregular domestic DV certificate. The signing key is an IS key.
Version	1.11
Referred by	ISO7816_J_51

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 31
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTISDE011
	Certificate Holder Reference	DETESTDVDE011
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_11
	Signing Key reference	Signed with the private key of key pair IS_KEY_11

2.4.10.6 IS_CERT_11a

ID	IS_CERT_11a
Purpose	This certificate is a regular IS certificate.
Version	1.11
Referred by	ISO7816_J_50, ISO7816_J_51, ISO7816_J_52, ISO7816_J_53

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
```

```
        42 cc dd
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 31 31
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
    5F 25 06 gg
        5F 24 06 hh
    5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTDVDE011
	Certificate Holder Reference	DETESTISDE011
	Certificate Holder Authorisation	IS, DG 3, DG 4
	Certificate effective date	CVCA$_{eff}$
	Certificate expiration date	CVCA$_{eff}$ + 13 days
	Public Key reference	Public key of key pair IS_KEY_11
	Signing Key reference	Signed with the private key of key pair DV_KEY_11

2.4.10.7 IS_CERT_11b

ID	IS_CERT_11b
Purpose	This certificate is an irregular IS certificate. The signing key is an IS key.
Version	1.11
Referred by	ISO7816_J_52
Content definition	

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 cc dd
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 31 31
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
    5F 25 06 gg
        5F 24 06 hh
    5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference

	dd is the placeholder for the Certificate Authority Reference (cc bytes) `ee` is the encoded length of the certificates public key, `ff` is the placeholder for the certificates public key bytes (ee bytes), `gg` is the placeholder for the BCD encoded effective date of the certificate `hh` is the placeholder for the BCD encoded expiration date of the certificate `ii` is the encoded length of the certificates signature object, `jj` is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	DETESTISDE011
	Certificate Holder Reference	DETESTISDE011
	Certificate Holder Authorisation	IS, DG 3, DG 4
	Certificate effective date	CVCA$_{eff}$
	Certificate expiration date	CVCA$_{eff}$ + 13 days
	Public Key reference	Public key of key pair IS_KEY_11
	Signing Key reference	Signed with the private key of key pair IS_KEY_11

2.4.10.8 IS_CERT_11c

ID	IS_CERT_11c
Purpose	This certificate is an irregular IS certificate. The signing key is a CVCA key.
Version	1.11
Referred by	ISO7816_M_5

Content definition

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 0D 44 45 54 45 53 54 43 41 44 45 30 31 31
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 31 31
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
        5F 25 06 gg
        5F 24 06 hh
  5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTCADE011
	Certificate Holder Reference	DETESTISDE011
	Certificate Holder Authorisation	IS, DG 3, DG 4
	Certificate effective date	CVCA$_{exp}$ + 5 months
	Certificate expiration date	CVCA$_{exp}$ + 6 months

	Public Key reference	Public key of key pair IS_KEY_11
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_11

2.4.11 Certificate Set 12

This certificate set is used for the certificate structure tests.

2.4.11.1 DV_CERT_12a

ID	DV_CERT_12a
Purpose	This certificate is a domestic DV certificate.
Version	1.11
Referred by	ISO7816_J_25, ISO7816_J_35

Content definition

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 cc dd
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
    5F 25 06 gg
        5F 24 06 hh
    5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff} + 1 month + 20 days
	Certificate expiration date	CVCA_{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.2 DV_CERT_12b

ID	DV_CERT_12b
Purpose	Certificate with a wrong “certificate body” tag
Version	1.11
Referred by	ISO7816_J_26

Content definition

```
7F 21 aa
        7F 4F bb
                5F 29 01 00
                42 cc dd
        7F 49 ee ff
                5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
                7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
                5F 25 06 gg
                5F 24 06 hh
        5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff} + 1 month + 20 days
	Certificate expiration date	CVCA_{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.3 DV_CERT_12c

ID	DV_CERT_12c
Purpose	Certificate with a wrong “certificate signature” tag
Version	1.11
Referred by	ISO7816_J_27

Content definition

```
7F 21 aa
        7F 4E bb
                5F 29 01 00
                42 cc dd
                7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
    5F 25 06 gg
        5F 24 06 hh
    5F 38 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff} + 1 month + 20 days
	Certificate expiration date	CVCA_{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.4 DV_CERT_12d

ID	DV_CERT_12d
Purpose	Certificate with an unconsistent “certificate body” D.O. (wrong length)
Version	1.11
Referred by	ISO7816_J_28

Content definition

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 cc dd
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
    5F 25 06 gg
        5F 24 06 hh
    5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object **decreased by one**
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)

	`ee` is the encoded length of the certificates public key, `ff` is the placeholder for the certificates public key bytes (ee bytes), `gg` is the placeholder for the BCD encoded effective date of the certificate `hh` is the placeholder for the BCD encoded expiration date of the certificate `ii` is the encoded length of the certificates signature object, `jj` is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA$_{eff}$ + 1 month + 20 days
	Certificate expiration date	CVCA$_{eff}$ + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.5 DV_CERT_12e

ID	DV_CERT_12e
Purpose	Certificate with an unconsistent “certificate signature” D.O. (The length byte specifies one by less than the actual signature length)
Version	1.11
Referred by	ISO7816_J_29

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object,
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object **decreased by one**,
`jj` is the placeholder for the certificates signature (ii+1 bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4

	Certificate effective date	$CVCA_{eff}$ + 1 month + 20 days
	Certificate expiration date	$CVCA_{eff}$ + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.6 DV_CERT_12f

ID	DV_CERT_12f
Purpose	Certificate with a wrong signature
Version	1.11
Referred by	ISO7816_J_30

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object,
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes) **last byte is increased by one (mod 256)**

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	$CVCA_{eff}$ + 1 month + 20 days
	Certificate expiration date	$CVCA_{eff}$ + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.7 DV_CERT_12g

ID	DV_CERT_12g
Purpose	Certificate with a wrong signature
Version	1.11
Referred by	ISO7816_J_31

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object,
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes) – **last byte is dropped and ii is updated according to the new length**

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff} + 1 month + 20 days
	Certificate expiration date	CVCA_{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.8 DV_CERT_12h

ID	DV_CERT_12h
Purpose	Modification in the certificate public key : O.I.D is missing
Version	1.11
Referred by	ISO7816_J_37

Content definition

```
7F 21 aa
      7F 4E bb
```

```
                5F 29 01 00
                42 cc dd
                7F 49 ee ff
                5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
                7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
        5F 25 06 gg
                5F 24 06 hh
        5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes) – **It does not contain any O.I.D D.O.**,
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	$CVCA_{eff}$ + 1 month + 20 days
	Certificate expiration date	$CVCA_{eff}$ + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.9 DV_CERT_12i

ID	DV_CERT_12i
Purpose	Modification in the certificate public key : wrong O.I.D
Version	1.11
Referred by	ISO7816_J_36

Content definition

```
7F 21 aa
        7F 4E bb
                5F 29 01 00
                42 cc dd
                7F 49 ee ff
                5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
                7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
        5F 25 06 gg
                5F 24 06 hh
        5F 37 ii jj
```

	`aa` is the encoded combined length of certificate body and signature objects `bb` is the encoded length the certificate body object `cc` is the encoded length of the Certificate Authority Reference *dd* is the placeholder for the Certificate Authority Reference (cc bytes) `ee` is the encoded length of the certificates public key, `ff` is the placeholder for the certificates public key bytes (ee bytes) – **The O.I.D has an uncorrect value that does not indicate id-TA: (0.4.0.127.0.7.2.2.3.x.y),** `gg` is the placeholder for the BCD encoded effective date of the certificate `hh` is the placeholder for the BCD encoded expiration date of the certificate `ii` is the encoded length of the certificates signature object, `jj` is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff} + 1 month + 20 days
	Certificate expiration date	CVCA_{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.10 DV_CERT_12j

ID	DV_CERT_12j
Purpose	**For ECDSA profile only:** Modification in the certificate public key : the elliptic curve public point is missing
Version	1.11
Referred by	ISO7816_J_38
Content definition	

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes) – **The elliptic curve public point is missing,**
`gg` is the placeholder for the BCD encoded effective date of the certificate

	hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff} + 1 month + 20 days
	Certificate expiration date	CVCA_{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.11 DV_CERT_12k

ID	DV_CERT_12k
Purpose	**For RSA profile only:** Modification in the certificate public key : the RSA modulus is missing
Version	1.11
Referred by	ISO7816_J_39

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes) – **The RSA modulus is missing**,
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff} + 1 month + 20 days

	Certificate expiration date	CVCA$_{eff}$ + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.12 DV_CERT_12l

ID	DV_CERT_12l
Purpose	**For RSA profile only:** Modification in the certificate public key : the RSA public exponent is missing
Version	1.11
Referred by	ISO7816_J_40

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes) – **The RSA public exponent is missing**,
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA$_{eff}$ + 1 month + 20 days
	Certificate expiration date	CVCA$_{eff}$ + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.13 DV_CERT_12m

ID	DV_CERT_12m
Purpose	Modification in the certificate public key For ECDSA profile: an unknown D.O. is present within the EC parameters (tag ‘77’), For RSA profile: an unknown D.O. is present within the RSA parameters (’77 01 00’),
Version	1.11
Referred by	ISO7816_J_41

Content definition

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 cc dd
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
    5F 25 06 gg
        5F 24 06 hh
    5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes) – **An unknown D.O. ‘77’ is present**
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff} + 1 month + 20 days
	Certificate expiration date	CVCA_{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.14 DV_CERT_12n

ID	DV_CERT_12n
Version	Has been merged with DV_CERT_12m in version 1.1

2.4.11.15 DV_CERT_12o

ID	DV_CERT_12o
Purpose	**For RSA profile only:** Certificate with a wrong signature
Version	1.11
Referred by	ISO7816_J_32

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object,
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes) – **the signature is greater than the modulus of the issuing key CVCA_KEY_00, the length of signature matches the length of the modulus**

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff} + 1 month + 20 days
	Certificate expiration date	CVCA_{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.16 DV_CERT_12p

ID	DV_CERT_12p
Purpose	**For ECDSA profile only:** The certificate signature is wrong. It is obtained by filling the ‘r’ part of the signature with ‘00’. The length of ‘r’ is still matches the size of the prime.

Version	1.11
Referred by	ISO7816_J_33

Content definition

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 cc dd
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
    5F 25 06 gg
        5F 24 06 hh
    5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object,
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes) – **with r = 0**

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff} + 1 month + 20 days
	Certificate expiration date	CVCA_{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11.17 DV_CERT_12q

ID	DV_CERT_12q
Purpose	**For ECDSA profile only:** The certificate signature is wrong. It is obtained by filling the ‘s’ part of the signature with ‘00’. The length of ‘s’ is still matches the size of the prime.
Version	1.11
Referred by	ISO7816_J_34

Content definition

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 cc dd
        7F 49 ee ff
```

```
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 32
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

`aa` is the encoded combined length of certificate body and signature objects
`bb` is the encoded length the certificate body object,
`cc` is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
`ee` is the encoded length of the certificates public key,
`ff` is the placeholder for the certificates public key bytes (ee bytes),
`gg` is the placeholder for the BCD encoded effective date of the certificate
`hh` is the placeholder for the BCD encoded expiration date of the certificate
`ii` is the encoded length of the certificates signature object,
`jj` is the placeholder for the certificates signature (ii bytes) – **with s = 0**

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA_{eff} + 1 month + 20 days
	Certificate expiration date	CVCA_{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.12 Certificate Set 13

This certificate set defines a link certificate used to update the chip signature mechanism according to the migration policy as defined by the manufacturer. The cryptographic elements of these certificates MUST use the new mechanisms besides the signature of the LINK_CERT_13 which is done with the original signature mechanism. This certificate set is only needed if the "Migration" profile is supported.

2.4.12.1 LINK_CERT_13

Note for ECDSA profile: Since the crypto mechanism is changed by this certificate, the domain parameter MUST be included in this certificate.

ID	LINK_CERT_13
Purpose	**For MIG profile only:** This certificate is a link certificate, which defines a new crypto mechanism to be used by chip.
Version	1.11
Referred by	ISO7816_N_1
Content definition	

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
```

```
        42 0D 44 45 54 45 53 54 43 41 44 45 30 30 39
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 43 41 44 45 30 31 33
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3
        5F 25 06 gg
        5F 24 06 hh
  5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTCADE011
	Certificate Holder Reference	DETESTCADE013
	Certificate Holder Authorisation	CVCA, DG 3, DG 4
	Certificate effective date	CVCA$_{exp}$ + 7 months
	Certificate expiration date	CVCA$_{exp}$ + 10 month
	Public Key reference	Public key of key pair CVCA_KEY_13
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_11

2.4.12.2 DV_CERT_13

ID	DV_CERT_13
Purpose	**For MIG profile only:** This certificate is a domestic DV certificate, which was issued by the new CVCA.
Version	1.11
Referred by	ISO7816_N_1

Content definition

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 0D 44 45 54 45 53 54 43 41 44 45 30 31 33
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31 33
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
        5F 25 06 gg
        5F 24 06 hh
  5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,

	ff is the placeholder for the certificates public key bytes (ee bytes), *gg* is the placeholder for the BCD encoded effective date of the certificate *hh* is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	DETESTCADE013
	Certificate Holder Reference	DETESTDVDE013
	Certificate Holder Authorisation	domestic DV, DG 3, DG 4
	Certificate effective date	$CVCA_{exp}$ + 7 months
	Certificate expiration date	$CVCA_{exp}$ + 8 months
	Public Key reference	Public key of key pair DV_KEY_13
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_13

2.4.12.3 IS_CERT_13

ID	IS_CERT_13
Purpose	**For MIG profile only:** This certificate is a regular IS certificate, which is issued by the DV_CERT_13
Version	1.11
Referred by	ISO7816_N_1
Content definition	

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 0D 44 45 54 45 53 54 44 56 44 45 30 31 33
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 31 33
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
        5F 25 06 gg
        5F 24 06 hh
  5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTDVDE013
	Certificate Holder Reference	DETESTISDE013
	Certificate Holder Authorisation	IS, DG 3, DG 4
	Certificate effective date	$CVCA_{exp}$ + 7 months
	Certificate expiration date	$CVCA_{exp}$ + 8 months
	Public Key reference	Public key of key pair IS_KEY_13
	Signing Key reference	Signed with the private key of key pair

		DV_KEY_13

2.4.13 Certificate Set 14

The certificate set follows a certification scheme where the DV and IS contain public key information from a generated key whose lengths are shorter than the CVCA key length.

2.4.13.2DV_CERT_14a

ID	DV_CERT_14a	
Purpose	This certificate is a regular domestic DV certificate which is issued by the CVCA	
Version	1.11	
Referred by	ISO7816_J_56	

Content definition

```
7F 21 aa
      7F 4E bb
            5F 29 01 00
            42 cc dd
            7F 49 ee ff
            5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 34
            7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 81
      5F 25 06 gg
            5F 24 06 hh
      5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE014
	Certificate Holder Authorisation	domestic DV, DG 3, DG4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_14a
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.13.3DV_CERT_14b

ID	DV_CERT_14b
Purpose	Certificate with a wrong (short) public key. For RSA profile, same Algorithm Identifier but PK.DVCA's modulus length is shorter than the CVCA's key modulus length. For ECDSA profile, same Algorithm Identifier but DVCA's domain parameters are different and have a shorter prime length than the CVCA's key. The hash algorithm should be adapted if necessary.
Version	1.11
Referred by	ISO7816_J_55

Content definition

```
7F 21 aa
        7F 4E bb
                5F 29 01 00
                42 cc dd
                7F 49 ee ff
                5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 30 34
                7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 81
        5F 25 06 gg
                5F 24 06 hh
        5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certificate Authority Reference
dd is the placeholder for the Certificate Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE014
	Certificate Holder Authorisation	domestic DV, DG 3, DG4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_14b
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.13.1 IS_CERT_14a

ID	IS_CERT_14a
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_14
Version	1.11
Referred by	ISO7816_J_55

Content definition

```
7F 21 aa
        7F 4E bb
        5F 29 01 00
        42 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 30 31
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
        5F 25 06 gg
        5F 24 06 hh
  5F 37 ii jj
```

aa is the encoded combined length of certificate body and signature objects

bb is the encoded length the certificate body object

ee is the encoded length of the certificates public key,

ff is the placeholder for the certificates public key bytes (ee bytes),

gg is the placeholder for the BCD encoded effective date of the certificate

hh is the placeholder for the BCD encoded expiration date of the certificate

ii is the encoded length of the certificates signature object,

jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	DETESTDVDE014
	Certificate Holder Reference	DETESTISDE014
	Certificate Holder Authorisation	IS, DG 3, DG 4
	Certificate effective date	CVCA_{eff}
	Certificate expiration date	CVCA_{eff} + 14 days
	Public Key reference	Public key of key pair IS_KEY_14a
	Signing Key reference	Signed with the private key of key pair DV_KEY_14b

2.4.13.2 IS_CERT_14b

ID	IS_CERT_14b
Purpose	Certificate with a wrong (short) Public key. For RSA profile, same Algorithm Identifier but IS key modulus length is shorter than the DVCA’s key modulus length. For ECDSA profile, same Algorithm Identifier but IS key domain parameters are different and have a shorter prime length than the DVCA’s key. The hash algorithm should be adapted if necessary.
Version	1.11
Referred by	ISO7816_J_56

Content definition

```
7F 21 aa
    7F 4E bb
        5F 29 01 00
        42 0D 44 45 54 45 53 54 44 56 44 45 30 30 31
        7F 49 ee ff
        5F 20 0D 44 45 54 45 53 54 49 53 44 45 30 30 31
        7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
        5F 25 06 gg
        5F 24 06 hh
  5F 37 ii jj
```

	aa is the encoded combined length of certificate body and signature objects *bb* is the encoded length the certificate body object *ee* is the encoded length of the certificates public key, *ff* is the placeholder for the certificates public key bytes (ee bytes), *gg* is the placeholder for the BCD encoded effective date of the certificate *hh* is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	DETESTDVDE014
	Certificate Holder Reference	DETESTISDE014
	Certificate Holder Authorisation	IS, DG 3, DG 4
	Certificate effective date	$\mathrm{CVCA}_{\mathrm{eff}}$
	Certificate expiration date	$\mathrm{CVCA}_{\mathrm{eff}}$ + 14 days
	Public Key reference	Public key of key pair IS_KEY_14b
	Signing Key reference	Signed with the private key of key pair DV_KEY_14a

3 Tests for layer 6 (ISO 7816)

This chapter defines the additional tests required for the extended command set used by the extended access control mechanisms.

3.1 Test case notation

The test cases defined below specify a set of command APDU which have to be sent to the test sample. While some parts of these APDUs are fixed, other elements have variable values which cannot be defined in general. The variable parts are marked by placeholder values which have to be replaced by the actual values. The following placeholders commonly used and therefore defined here in a global manner. All other placeholders are defined within the corresponding test case definition.

Placeholder	Definition
`<L_C>`	The length byte containing the length of the APDU command data.
`<Le>`	The length byte containing the length of the requested response data. Depending on the size of <Lc> the <Le> element must consist of one or two bytes (extended length). See ISO 7816-4 5.1 "*In any command-response pair comprising both L_c and L_e fields (see ISO/IEC 7816-3), short and extended length fields shall not be combined: either both of them are short, or both of them are extended*."
`<L_xy>`	The encoded length of the data object *xy*.
`<Cryptogram>`	The encrypted part of a Secure Messaging APDU. The data content of this cryptogram is defined in the corresponding test case definition.
`<Checksum>`	The cryptographic checksum which is calculated over the protected parts of the Secure Messaging command.
`<fid.EF.CVCA>`	With version 1.1 of the EAC specification a passport may define a different file ID (fid) for the EF.CVCA file. This definition can be done in the TerminalAuthentication element in data group 14. If this is the case for the test object, this placeholder has to be set to the passport specific file ID for the EF.CVCA file, otherwise this placeholder is set to the default value of '01 1C'.
`<sfi.EF.CVCA>`	With version 1.1 of the EAC specification a passport may define a different short file ID (sfi) for the EF.CVCA file. This definition can be done in the TerminalAuthentication element in data group 14. If this is the case for the test object, this placeholder has to be set to the passport specific short file ID for the EF.CVCA file, otherwise this placeholder is set to the default value of '1C'. Note: It may happen that there is only a fid defined in the TerminalAuthenticationInfo element, but NO sfi. In this case, the corresponding test cases have to be skipped.

3.2 General requirements

3.2.1 Security Status

According to the definition in the ICAO supplement documents [R5] and the EAC specification [R2] the Secure Messaging session SHOULD be aborted if and only if a secure messaging error occurs.

In respect to the Chip Authentication mechanism the EAC specification contains an additional specification about the security status:

> **Security Status**
> If Chip Authentication was successfully performed, Secure Messaging is restarted using the derived session keys K_{MAC} and K_{ENC}. Otherwise, Secure Messaging is continued using the previously established session keys (PACE or Basic Access Control).

Reference 1 : Security Status definition in the EAC specification

Base on these definitions, all responses received during the test cases MUST be coded in secure messaging context unless stated different in the test case. The test setup MUST check this and MUST verify the cryptographic checksum.

3.2.2 Extended length APDUs

If the size of cryptographic keys leads to certificates that exceed the size of a standard APDU, all appropriate commands have to be performed as extended length APDUs. Extended length APDUs have to be managed according to [R4], clause 5.1 “Command-response pairs”.

3.3 Unit ISO7816_H – Security Conditions for EAC protected MRTDs

On an EAC protected eMRTD, the data groups containing sensitive biometric data MUST be protected by the terminal authentication mechanisms. While all other data groups are accessible after the “Open ePassport Application" procedure [R2] has been performed, the data group 3 and/or 4 MUST only be accessible after a successful terminal authentication process.

All test cases of this test unit which require the “Open ePassport Application” procedure MUST be performed twice (one test run with BAC and one with PACE) if the chip supports both protocols. If the chip only supports one of these protocols (BAC or PACE), only one test run has to be performed with the supported protocol used in the “Open ePassport Application” procedure.

Note: Chip Authentication must be performed as described in [R2] and [R11] either with command *MSE:Set KAT* or commands *MSE:Set AT* and *General Authenticate*.

3.3.1 Test case ISO7816_H_1

Test - ID	ISO7816_H_1
Purpose	SELECT command for EF.DG3 within an established PACE or BAC session, but before the terminal authentication mechanism has been performed.
Version	1.2
Profile	TA, DG3
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The Chip Authentication mechanism MUST have been performed, too.
Test scenario	1. Send the given SELECT APDU for EF.DG3 (File Id ’01 03’) to the eMRTD. Though PACE or BAC and the CA mechanisms have been performed, the access to the data group 3 MUST be denied. `‘0C A4 02 0C 15 87 09 01 <Cryptogram> 8E 08 <Checksum> 00’` • <Cryptogram> contains the encrypted file ID (‘01 03’). 2. Send the following READ BINARY command to the eMRTD:

	`'0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'`
Expected results	1. ISO checking error or '90 00' within a valid SM response. If this step returns an ISO checking error, the next step SHALL be skipped. 2. ISO checking error within a valid SM response

3.3.2 Test case ISO7816_H_2

Test - ID	ISO7816_H_2
Purpose	SELECT command for EF.DG4 within an established PACE or BAC session, but without the terminal authentication
Version	1.2
Profile	TA, DG4
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The Chip Authentication mechanism MUST have been performed, too.

Test scenario	1. Send the given SELECT APDU for EF.DG4 (File Id '01 04') to the eMRTD. Though PACE or BAC and the CA mechanisms have been performed, the access to the data group 4 MUST be denied.
	`'0C A4 02 0C 15 87 09 01 <Cryptogram> 8E 08 <Checksum> 00'`
	- <Cryptogram> contains the encrypted file ID ('01 04').
	2. Send the following READ BINARY command to the eMRTD:
	`'0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'`

Expected results	1. ISO checking error or '90 00' within a valid SM response. If this step returns an ISO checking error, the next step SHALL be skipped 2. ISO checking error within a valid SM response

3.3.3 Test case ISO7816_H_3

Test - ID	ISO7816_H_3
Purpose	READ BINARY command with SFI for EF.DG3 within an established PACE or BAC session, but without the terminal authentication
Version	1.2
Profile	TA, DG3
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The Chip Authentication mechanism MUST have been performed, too.
Test scenario	1. Send the given READ BINARY APDU for EF.DG3 (SFI '03') to the eMRTD. Though PACE or BAC and the CA mechanisms have been performed, the access to the data group 3 MUST be denied. `'0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'`
Expected results	1. ISO checking error within a valid SM response

3.3.4 Test case ISO7816_H_4

Test - ID	ISO7816_H_4

Purpose	READ BINARY command with SFI for EF.DG4 within an established PACE or BAC session, but without the terminal authentication
Version	1.2
Profile	TA, DG4
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The Chip Authentication mechanism MUST have been performed, too.
Test scenario	1. Send the given READ BINARY APDU for EF.DG4 (SFI ’04’) to the eMRTD. Though PACE or BAC and the CA mechanisms have been performed, the access to the data group 4 MUST be denied. ‘0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’
Expected results	1. ISO checking error within a valid SM response

3.3.5 Test case ISO7816_H_5

Test - ID	ISO7816_H_5
Purpose	READ BINARY command with odd instruction byte and SFI for EF.DG3 within an established PACE or BAC session, but without the terminal authentication
Version	1.2
Profile	TA, DG3, OddIns
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The Chip Authentication mechanism MUST have been performed, too.
Test scenario	1. Send the given READ BINARY APDU for EF.DG3 (SFI ’03’) to the eMRTD. Though PACE or BAC and the CA mechanisms have been performed, the access to the data group 3 MUST be denied. ‘0C B1 00 03 17 85 <L$_{85}$> <Cryptogram> 97 01 07 8E 08 <Checksum> 00’ - The cryptogram contains the encrypted data object 54 with the encoded offset of 00 ’54 01 00’
Expected results	1. ISO checking error within a valid SM response

3.3.6 Test case ISO7816_H_6

Test - ID	ISO7816_H_6
Purpose	READ BINARY command with odd instruction byte and SFI for EF.DG4 within an established PACE or BAC session, but without the terminal authentication
Version	1.2
Profile	TA, DG4, OddIns
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The Chip Authentication mechanism MUST have been performed, too.
Test scenario	1. Send the given READ BINARY APDU for EF.DG4 (SFI ’04’) to the eMRTD. Though PACE or BAC and the CA mechanisms have been performed, the access to the data group 4 MUST be denied. ‘0C B1 00 04 17 85 <L$_{85}$> <Cryptogram> 97 01 07 8E

	`08 <Checksum> 00’` • `The cryptogram contains the encrypted data object 54 with the encoded offset of 00 ’54 01 00’`
Expected results	1. ISO checking error within a valid SM response

3.3.7 Test case ISO7816_H_7

Test - ID	ISO7816_H_7
Purpose	SELECT command for EF.CVCA without established PACE or BAC session
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST **NOT** have been performed. 2. The fileID information from data group 14 TerminalAuthenticationInfo element must be used if present. Otherwise the default value has to be used.

Test scenario	1. Select the ePassport application.
	`‘00 A4 04 0C 07 A0 00 00 02 47 10 01’`
	2. Send the given SELECT APDU for EF.CVCA (<fid.EF.CVCA>) to the eMRTD. Since the "Open ePassport Application" procedure has not been performed, the access to this file MUST be denied.
	`‘00 A4 02 0C 02` <fid.EF.CVCA>`’`
	3. Some chip implementations allow the selection of a protected file. In these cases an additional READ BINARY SHOULD be used to verify that at least the READ BINARY command is prohibited.
	`’00 B0 00 00 01’`

Expected results	1. ISO checking error or ’90 00’ as a plain response without Secure Messaging. If this step returns ISO checking error, the next steps SHALL be skipped. 2. ISO checking error or ’90 00’ as a plain response without Secure Messaging 3. ISO checking error as a plain response without Secure Messaging

3.3.8 Test case ISO7816_H_8

Test - ID	ISO7816_H_8
Purpose	READ BINARY command with SFI for EF.CVCA without established PACE or BAC session
Version	1.2
Profile	TA
Preconditions	1. The SFI information from data group 14 TerminalAuthenticationInfo element must be used if present. Otherwise the default value has to be used. If the TerminalAuthenticationInfo element specifies a file ID, but no short file ID, this test case is skipped.
Test scenario	1. Select the ePassport application. `‘00 A4 04 0C 07 A0 00 00 02 47 10 01’` 2. Send the given READ BINARY APDU for EF.CVCA (<sfi.EF.CVCA>)

	to the eMRTD. Since the "Open ePassport Application" procedure has not been performed, the access to the EF.CVCA has to be denied. ‘00 B0 <sfi.EF.CVCA> 00 01’
Expected results	1. ISO checking error or ’90 00’ as a plain response without Secure Messaging. If this step returns ISO checking error, the next steps SHALL be skipped. 2. ISO checking error as a plain response without Secure Messaging

3.3.9 Test case ISO7816_H_9

Test - ID	ISO7816_H_9
Purpose	READ BINARY command with odd instruction byte and with SFI for EF.CVCA without established PACE or BAC session
Version	1.2
Profile	TA, OddIns
Preconditions	1. The SFI information from data group 14 TerminalAuthenticationInfo element must be used if present. Otherwise the default value has to be used. If the TerminalAuthenticationInfo element specifies a file ID, but no short file ID, this test case is skipped
Test scenario	1. Select the ePassport application. ‘00 A4 04 0C 07 A0 00 00 02 47 10 01’ 2. Send the given READ BINARY APDU for EF.CVCA (<sfi.EF.CVCA>) to the eMRTD. Since the "Open ePassport Application" procedure has not been performed, the access to the EF.CVCA has to be denied. ‘00 B1 00 <sfi.EF.CVCA> 03 54 01 00 07’
Expected results	1. ISO checking error or ’90 00’ as a plain response without Secure Messaging. If this step returns ISO checking error, the next steps SHALL be skipped. 2. ISO checking error as a plain response without Secure Messaging

3.3.10 Test case ISO7816_H_10

Test - ID	ISO7816_H_10
Purpose	READ BINARY command with odd instruction byte and with FID for EF.CVCA without established PACE or BAC session
Version	1.2
Profile	TA, OddIns
Preconditions	1. The fileID information from data group 14 TerminalAuthenticationInfo element must be used if present. Otherwise the default value has to be used.
Test scenario	1. Select the ePassport application. ‘00 A4 04 0C 07 A0 00 00 02 47 10 01’ 2. Send the given READ BINARY APDU for EF.CVCA (<fid.EF.CVCA>) to the eMRTD. Since the "Open ePassport Application" procedure has not been performed, the access to the EF.CVCA has to be denied. ‘00 B1 <fid.EF.CVCA> 03 54 01 00 07’
Expected results	1. ISO checking error or ’90 00’ as a plain response without Secure Messaging.

	If this step returns ISO checking error, the next steps SHALL be skipped. 2. ISO checking error as a plain response without Secure Messaging

3.3.11 Test case ISO7816_H_11

Test - ID	ISO7816_H_11
Purpose	READ BINARY command with odd instruction byte and FID for EF.DG3 within an established PACE or BAC session, but without the terminal authentication
Version	1.2
Profile	TA, DG3, OddIns
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The Chip Authentication mechanism MUST have been performed, too.
Test scenario	1. Send the given READ BINARY APDU for EF.DG3 (FID ’0103’) to the eMRTD. Though "Open ePassport Application" procedure and the CA mechanisms have been performed, the access to the data group 3 MUST be denied. ‘0C B1 01 03 17 85 <L_{85}> <Cryptogram> 97 01 07 8E 08 <Checksum> 00’ - The cryptogram contains the encrypted data object 54 with the encoded offset of 00 ’54 01 00’
Expected results	1. ISO checking error within a valid SM response

3.3.12 Test case ISO7816_H_12

Test - ID	ISO7816_H_12
Purpose	READ BINARY command with odd instruction byte and FID for EF.DG4 within an established PACE or BAC session, but without the terminal authentication
Version	1.2
Profile	TA, DG4, OddIns
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The Chip Authentication mechanism MUST have been performed, too.
Test scenario	1. Send the given READ BINARY APDU for EF.DG4 (FID ’0104’) to the eMRTD. Though "Open ePassport Application" procedure and the CA mechanisms have been performed, the access to the data group 4 MUST be denied. ‘0C B1 01 04 17 85 <L_{85}> <Cryptogram> 97 01 07 8E 08 <Checksum> 00’ - The cryptogram contains the encrypted data object 54 with the encoded offset of 00 ’54 01 00’
Expected results	1. ISO checking error within a valid SM response

3.3.13 Test case ISO7816_H_13

Test - ID	ISO7816_H_13
Purpose	SELECT command for EF.CVCA with established PACE or BAC session (Positive test)
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The fileID information from data group 14 TerminalAuthenticationInfo element MUST be used if present. Otherwise the default value has to be used.

Test scenario	1. Send the given SELECT APDU for EF.CVCA (<fid.EF.CVCA>) to the eMRTD.
	`‘0C A4 02 0C 15 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- `The cryptogram contains the encrypted fileID of the EF.CVCA file` <fid.EF.CVCA>`’`
	2. According to [R2], the size of the EF_CVCA MUST be 36 bytes. So try to read the entire EF.CVCA file with a single READ BINARY Command.
	`’0C B0 00 00 0D 97 01 24 8E 08 <Checksum> 00’`

Expected results	1. ’90 00’ within a valid SM response 2. 36 bytes of content data and ’90 00’ in an SM response

3.3.14 Test case ISO7816_H_14

Test - ID	ISO7816_H_14
Purpose	READ BINARY command with SFI for EF.CVCA with established PACE or BAC session (Positive test)
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The SFI information from data group 14 TerminalAuthenticationInfo element must be used if present. Otherwise the default value has to be used. If the TerminalAuthenticationInfo element specifies a file ID, but no short file ID, this test case is skipped.
Test scenario	1. Send the given READ BINARY APDU for EF.CVCA (<sfi.EF.CVCA>) to the eMRTD. According to [R2], the size of the EF_CVCA MUST be 36 bytes. So try to read the entire EF.CVCA file with a single READ BINARY Command `‘0C B0` <sfi.EF.CVCA> `00 0D 97 01 24 8E 08 <Checksum> 00’`
Expected results	1. 36 bytes of content data and ’90 00’ in an SM response

3.3.15 Test case ISO7816_H_15

Test - ID	ISO7816_H_15

Purpose	READ BINARY command with odd instruction byte and with SFI for EF.CVCA with established PACE or BAC session (Positive test)
Version	1.2
Profile	TA, OddIns
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The SFI information from data group 14 TerminalAuthenticationInfo element must be used if present. Otherwise the default value has to be used. If the TerminalAuthenticationInfo element specifies a file ID, but no short file ID, this test case is skipped
Test scenario	1. Send the given READ BINARY APDU for EF.CVCA (<sfi.EF.CVCA>) to the eMRTD. According to [R2], the size of the EF_CVCA MUST be 36 bytes. So try to read the EF.CVCA file with a single READ BINARY Command `‘0C B1 00 <sfi.EF.CVCA> 17 85 <L85> <Cryptogram> 97 01 26 8E 08 <Checksum> 00` - The cryptogram contains the encrypted data object 54 with an encoded offset of 00 ‘54 01 00’
Expected results	1. 38 bytes of data including the tag 53 and the BER encoded length. The Status must be ’90 00’. The response must be protected by Secure Messaging.

3.3.16 Test case ISO7816_H_16

Test - ID	ISO7816_H_16
Purpose	READ BINARY command with odd instruction byte and with FID for EF.CVCA with established PACE or BAC session (Positive test)
Version	1.2
Profile	TA, OddIns
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The fileID information from data group 14 TerminalAuthenticationInfo element must be used if present. Otherwise the default value has to be used.
Test scenario	2. Send the given READ BINARY APDU for EF.CVCA (<fid.EF.CVCA>) to the eMRTD. According to [R2], the size of the EF_CVCA MUST be 36 bytes. So try to read the EF.CVCA file with a single READ BINARY Command `‘0C B1 <fid.EF.CVCA> 17 85 <L85> <Cryptogram> 97 01 26 8E 08 <Checksum> 00` - The cryptogram contains the encrypted data object 54 with an encoded offset of 00 ‘54 01 00’
Expected results	1. 38 bytes of data including the tag 53 and the BER encoded length. The Status must be ’90 00’. The response must be protected by Secure Messaging.

3.4 Unit ISO7816_I – Chip Authentication (MSE:Set KAT)

The chip authentication mechanism uses the manage security environment command to verify that the chip is genuine. The inspection system and the eMRTD generate a shared secret based of the public key data stored in the data group 14 of the document. This secret is used to derive new session keys for the continued secure messaging session. The genuineness of the MRTD chip is implicitly verified by its ability to perform Secure Messaging using the new session keys. The test cases specified in this unit verify the correct implementation of the “MSE:Set Kat” command as specified in [R2] and [R11].

The data group 14 may contain an optional key reference identifier. This is useful if the chip supports multiple keys for Chip Authentication. The MSE:Set Kat command can be called either with implicit key selection if no key reference is included in DG14 or with the explicit key reference defined in the DG 14 element. All tests in this unit SHOULD be used with implicit or explicit key reference depending on the presence of the key reference element in DG14.

The data group 14 may contain more than one ChipAuthenticationPublicKeyInfo. In this case, all appropriate tests must be performed for each key used with 3DES algorithm. The corresponding test case is only rated as a *PASS* if all passes are completed successfully. For test cases where the ChipAuthentication mechanism is just used a precondition always the first key is used.

All test cases of this test unit which require the “Open ePassport Application” procedure MUST be performed twice (one test run with BAC and one with PACE) if the chip supports both protocols. If the chip only supports one of these protocols (BAC or PACE), only one test run has to be performed with the supported protocol used in the “Open ePassport Application” procedure.

3.4.1 Test case ISO7816_I_1

Test - ID	ISO7816_I_1
Purpose	MSE:Set KAT command with correct ephemeral public key
Version	1.2
Profile	CA_KAT
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE APDU to the eMRTD. ‘0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the following encrypted data objects 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <private key reference> - The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14. 2. To verify the chips ability to continue the Secure Messaging with the new session keys, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the new session keys.
Expected results	1. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 2. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the NEW session keys.

3.4.2 Test case ISO7816_I_2

Test - ID	ISO7816_I_2
Purpose	MSE:Set KAT command with correct ephemeral public key, but afterwards the old session keys are used.
Version	1.2
Profile	CA_KAT
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.

Test scenario	1. Send the given MSE APDU to the eMRTD.
	`‘0C 22 41 A6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the following encrypted data objects
	`91 <L91> <ephemeral public key>`
	`84 <L84> <private key reference>`
	- The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14.
	2. Instead of using the new session keys, the session keys derived in step 1 of the test preconditions are used to send the Command APDU as defined in the ICS (Annex A, Table 2) SM-protected APDU.

Expected results	1. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 2. ISO checking error. The chip MUST delete the session keys derived in step 1 of the test preconditions and MUST NOT accept any APDUs with these session keys. The error must be a returned as plain response without Secure Messaging.

3.4.3 Test case ISO7816_I_3

Test - ID	ISO7816_I_3
Purpose	MSE:Set KAT command with invalid ephemeral public key (different key size)
Version	1.2
Profile	CA_KAT, ECDH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.

Test scenario	1. Send the given MSE APDU to the eMRTD.
	`‘0C 22 41 A6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the following encrypted data objects
	`91 <L91> <ephemeral public key>`
	`84 <L84> <private key reference>`

	- The ephemeral public key MUST be generated with domain parameters specifying a different key size (e.g. for a 224 bit key in DG14 a 192 bit ephemeral key pair is created) - The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14. 2. To verify that the session keys derived in step 1 of the test preconditions can still be used, the Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the session keys derived in step 1 of the test precondition.
Expected results	1. ISO checking error, or warning ’63 00’ within a valid SM response. Since there are invalid domain parameters used to generate the ephemeral key pair, the key agreement process MUST always fail. 2. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions.

3.4.4 Test case ISO7816_I_4

Test - ID	ISO7816_I_4
Purpose	MSE:Set KAT command with a valid ephemeral public key, but without established PACE or BAC session
Version	1.2
Profile	CA_KAT
Preconditions	1. The "Open ePassport Application" procedure MUST NOT have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read BEFORE to be able to generate an ephemeral key pair.

Test scenario	1. Select the ePassport application.
	`‘00 A4 04 0C 07 A0 00 00 02 47 10 01’`
	2. Send the given MSE APDU to the eMRTD.
	`‘00 22 41 A6 <Lc> 91 <L91> <ephemeral public key> 84 <L84> <private key reference>’`
	- The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14.
	3. To verify that the chip does not activate the new session keys based on the key agreement, the Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the new session keys based on step 2.

Expected results	1. ISO checking error or ’90 00’ as a plain response without Secure Messaging. If this step returns ISO checking error, the next steps SHALL be skipped. 2. ISO checking error. The "Open ePassport Application" procedure MUST have been performed before the Chip Authentication can be done. The error code SHALL be returned as plain data without SM encoding. 3. ISO checking error. The error code SHALL be returned as plain data without SM encoding.

3.4.5 Test case ISO7816_I_5

Test - ID	ISO7816_I_5
Purpose	MSE:Set KAT command with a valid ephemeral public key, but without SecureMessaging
Version	1.2
Profile	CA_KAT
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read BEFORE to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE APDU to the eMRTD. '00 22 41 A6 <Lc> 91 <L$_{91}$> <ephemeral public key> 84 <L$_{84}$> <private key reference>' - The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14. 2. To verify that the chip does not activate the new session keys based on the key agreement, the Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the new session keys. 3. To verify that the chip has deleted the session keys derived in step 1 of the test preconditions, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the session keys derived in step 1 of the test preconditions.
Expected results	1. ISO checking error. The use of SecureMessaging SHALL be enforced by the chip. The error code SHALL be returned as plain data without SM encoding. 2. ISO checking error. The error code SHALL be returned as plain data without SM encoding. 3. ISO checking error. The error code SHALL be returned as plain data without SM encoding.

3.4.6 Test case ISO7816_I_6

Test - ID	ISO7816_I_6
Purpose	MSE:Set KAT command with correct ephemeral public key but invalid class byte
Version	1.2
Profile	CA_KAT
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE APDU to the eMRTD. '8C 22 41 A6 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> 00' - <Cryptogram> contains the following encrypted data objects 91 <L$_{91}$> <ephemeral public key> 84 <L$_{84}$> <private key reference>

	- The class byte has been set to an invalid value of 8C. - The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14. 2. To verify that the chip does not activate the new session keys, the Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the new session keys.
Expected results	1. ISO checking error. Note that the behaviour of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. 2. ISO checking error. Note since invalid session keys are used, the chip MUST return a Secure Messaging error in a plain response regardless if the Secure Messaging session was already closed in step 1.

3.4.7 Test case ISO7816_I_7

Test - ID	ISO7816_I_7
Purpose	MSE:Set KAT command with invalid data object tag for the ephemeral public key
Version	1.2
Profile	CA_KAT
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.

Test scenario	1. Send the given MSE APDU to the eMRTD.
	`‘0C 22 41 A6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the following encrypted data objects
	`93 <L93> <ephemeral public key>`
	`84 <L84> <private key reference>`
	- The data object for the ephemeral public key has an invalid tag 93.
	- The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14.
	2. To verify that the session keys derived in step 1 of the test preconditions are still valid, the Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the session keys derived in step 1 of the preconditions.

Expected results	1. ISO checking error. The error MUST be encoded in a Secure Messaging response using the session keys derived in step 1 of the test preconditions. 2. ’90 00’ and a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions.

3.4.8 Test case ISO7816_I_8

Test - ID	ISO7816_I_8
Version	Deleted in version 1.1

3.4.9 Test case ISO7816_I_9

Test - ID	ISO7816_I_9
Purpose	MSE:Set KAT providing a (0,0) public key
Version	1.2
Profile	CA_KAT, ECDH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE APDU to the eMRTD. '0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' - <Cryptogram> contains the following encrypted data objects 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <private key reference> - The public key has to be coded as '04||x||y' where both x and y have a size according to the prime, but filled with '00'. - The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14. 2. To verify that the session keys derived in step 1 of the test preconditions are still valid, the Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the session keys derived in step 1 of the test preconditions.
Expected results	1. ISO checking error or warning processing '63 00'. Note: Even if public key validation is not done, ECDH computation SHOULD fail with this input. The error MUST be encoded in a Secure Messaging response using the session keys derived in step 1 of the test preconditions. 2. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions.

3.4.10 Test case ISO7816_I_10

Test - ID	ISO7816_I_10
Purpose	MSE:Set KAT test borderline cases for x- and y- coordinates (small x coordinate)
Version	1.2
Profile	CA_KAT, ECDH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral public key pair.

Test scenario	1. Send the given MSE APDU to the eMRTD. ‘0C 22 41 A6 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> 00’ • <Cryptogram> contains the following encrypted data objects 91 <L$_{91}$> <ephemeral public key> 84 <L$_{84}$> <private key reference> • Use an ephemeral public key with an x-coordinate requiring less than [$\log_{256}$ q] bytes to be represented. Pad with prepended zero bytes. (For details on q see [R7]) • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14. 2. To verify the chips ability to continue the Secure Messaging with the new session keys, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the new session keys.
Expected results	1. ‘90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 2. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the new session keys.

3.4.11 Test case ISO7816_I_11

Test - ID	ISO7816_I_11
Purpose	MSE:Set KAT test borderline cases for x- and y- coordinates (large x coordinate)
Version	1.2
Profile	CA_KAT, ECDH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral public key pair.
Test scenario	1. Send the given MSE APDU to the eMRTD. ‘0C 22 41 A6 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> 00’ • <Cryptogram> contains the following encrypted data objects 91 <L$_{91}$> <ephemeral public key> 84 <L$_{84}$> <private key reference> • Use a ephemeral public key with an x-coordinate having its most significant bit set to 1 • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14. 2. To verify the chips ability to continue the Secure Messaging with the new session keys, the Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the new session keys.
Expected results	1. ‘90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 2. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the new session keys.

3.4.12 Test case ISO7816_I_12

Test - ID	ISO7816_I_12
Purpose	MSE:Set KAT test borderline cases for x- and y- coordinates (small y coordinate)
Version	1.2
Profile	CA_KAT, ECDH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral public key pair.
Test scenario	1. Send the given MSE APDU to the eMRTD. `‘0C 22 41 A6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’` • <Cryptogram> contains the following encrypted data objects `91 <L91> <ephemeral public key>` `84 <L84> <private key reference>` • Use an ephemeral public key with an y-coordinate requiring less than [$\log_{256}$ q] bytes to be represented. Pad with prepended zero bytes. (For details on q see [R7]) • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14. 2. To verify the chips ability to continue the Secure Messaging with the new session keys, the Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the new session keys.
Expected results	1. ‘90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 2. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the new session keys.

3.4.13 Test case ISO7816_I_13

Test - ID	ISO7816_I_13
Purpose	MSE:Set KAT test borderline cases for x- and y- coordinates (large y coordinate)
Version	1.2
Profile	CA_KAT, ECDH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral public key pair.

Test scenario	1. Send the given MSE APDU to the eMRTD. ‘0C 22 41 A6 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the following encrypted data objects 91 <L$_{91}$> <ephemeral public key> 84 <L$_{84}$> <private key reference> - Use a ephemeral public key with an y-coordinate having its most significant bit set to 1 - The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14. 2. To verify the chips ability to continue the Secure Messaging with the new session keys, the Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the new session keys.
Expected results	1. ‘90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 2. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the new session keys.

3.4.14 Test case ISO7816_I_14

Test - ID	ISO7816_I_14
Purpose	MSE:Set KAT command with an incorrect private key reference *Note: The support for key references is mandatory for the chip in case it has several chip authentication private keys, and optional in case it only has one private key.*
Version	1.2
Profile	CA_KAT, KeyRef
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral public key pair.
Test scenario	1. Send the given MSE APDU to the eMRTD. ‘0C 22 41 A6 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the following encrypted data objects 91 <L$_{91}$> <ephemeral public key> 84 <L$_{84}$> <invalid private key reference> - A private key reference MUST be included in the APDU. This key reference MUST be used as defined in the ICS in Annex A by the ePassport vendor. 2. To verify that the session keys derived in step 1 of the test preconditions are still valid, the Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the session keys derived in step 1 of the preconditions.
Expected results	1. ISO checking error or warning processing ’63 00’. The error MUST be encoded in a Secure Messaging response using the session keys derived in step 1 of the test preconditions.

	2. ’90 00’ and a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions.

3.4.15 Test case ISO7816_I_15

Test - ID	ISO7816_I_15
Purpose	Check the Chip authentication failure (using DH) – wrong value (value strictly bigger than the Prime)
Version	1.2
Profile	CA_KAT, DH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral public key pair.
Test scenario	1. Send the given MSE APDU to the eMRTD. ‘0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the following encrypted data objects 91 <L_{91}> <ephemeral public key> 84 <L_{84}> <private key reference> - Use an ephemeral public key with a wrong value (value strictly bigger than the Prime) ephemeral public key = prime p + 1 2. To verify that the session keys derived in step 1 of the test preconditions are still valid, the Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the session keys derived in step 1 of the test preconditions.
Expected results	1. ISO checking error or warning processing ’63 00’. The SW MUST be wrapped with the session keys derived in step 1 of the test preconditions. Subsequent command MUST be wrapped with the session keys derived in step 1 of the test preconditions. 2. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions.

3.4.16 Test case ISO7816_I_16

Test - ID	ISO7816_I_16
Purpose	Check the Chip authentication failure (using ECDH) – wrong point (value does not belong to the curve)
Version	1.2
Profile	CA_KAT, ECDH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral public key pair.
Test scenario	1. Send the given MSE APDU to the eMRTD. ‘0C 22 41 A6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08

	`<Checksum> 00’`
	• <Cryptogram> contains the following encrypted data objects
	`91 <`L_{91}`> <ephemeral public key>`
	`84 <`L_{84}`> < private key reference>`
	• Use an ephemeral public key with a wrong point (value does not belong to the curve)
	2. To verify that the session keys derived in step 1 of the test preconditions are still valid, the Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the session keys derived in step 1 of the preconditions.

Expected results	1. ISO checking error or warning processing ’63 00’. The SW MUST be wrapped with the session keys derived in step 1 of the test preconditions. Subsequent command MUST be wrapped with the session keys derived in step 1 of the test preconditions. 2. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions.

3.4.17 Test case ISO7816_I_17

Test - ID	ISO7816_I_17
Version	Deleted in version 0.8 since it was identical with ISO7816_I_7

3.5 Unit ISO7816_II – Chip Authentication (MSE:Set AT & GA)

The chip authentication mechanism uses the Manage Security Environment command to verify that the chip is genuine. The terminal and the eMRTD generate a shared secret based on the public key data stored in data group 14 file of the document. This secret is used to derive new session keys for the continued secure messaging session. The genuineness of the eMRTD chip is explicitly verified by the authentication token and implicitly verified by its ability to perform Secure Messaging using the new session keys. The test cases specified in this unit verify the correct implementation of the “MSE:Set AT” / ”General Authentication” command pair.

Data group 14 file may contain an optional key reference identifier. This is useful if the chip supports multiple keys for Chip Authentication. The MSE:Set AT command can be called either with implicit key selection if no key reference is included in data group 14 or with the explicit key reference defined in the data group 14 element. All tests in this unit SHOULD be used with implicit or explicit key reference depending on the presence of the key reference element in data group 14.

Data group 14 may contain more then one ChipAuthenticationInfo. In this case, all appropriate tests must be performed for each ChipAuthenticationInfo. The corresponding test case is only rated as a PASS if all passes are completed successfully. For test cases where the Chip Authentication mechanism is just used as precondition always the first key is used.

All test cases of this test unit which require the “Open ePassport Application” procedure MUST be performed twice (one test run with BAC and one with PACE) if the chip supports both protocols. If the chip only supports one of these protocols (BAC or PACE), only one test run has to be performed with the supported protocol used in the “Open ePassport Application” procedure.

3.5.1 Test case ISO7816_II_1

Test - ID	ISO7816_II_1
Purpose	MSE:Set AT / General Authenticate commands with correct ephemeral public key
Version	1.2
Profile	CA_ATGA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set AT APDU to the eMRTD. ‘0C 22 41 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the following encrypted data objects 80 <L_{80}> <cryptographic mechanism reference> 84 <L_{84}> <private key reference> - The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in data group 14. 2. Send the given General Authenticate APDU to the eMRTD. ‘0C 86 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 97 <L_{97}> <Ne> 8E 08 <Checksum> <Le>’ - <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L_{80}> <ephemeral public key> 3. To verify the chips ability to continue the Secure Messaging with the new session keys, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the new session keys.
Expected results	1. ‘90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test precondition. 2. ‘7C 00 90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 3. ‘90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the NEW session keys.

3.5.2 Test case ISO7816_II_2

Test - ID	ISO7816_II_2
Purpose	MSE:Set AT / General Authenticate commands with correct ephemeral public key, but afterward the old session keys are used.
Version	1.2
Profile	CA_ATGA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set AT APDU to the eMRTD. ‘0C 22 41 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the following encrypted data objects 80 <L_{80}> <cryptographic mechanism reference> 84 <L_{84}> <private key reference>

	- The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in data group 14. 2. Send the given General Authenticate APDU to the eMRTD. '0C 86 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 97 <L_{97}> <Ne> 8E 08 <Checksum> <Le>' - <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L_{80}> <ephemeral public key> 3. Instead of using the new session keys, the session keys derived in step 1 of the test preconditions are used to send the Command APDU as defined in the ICS (Annex A, Table 2) as SM-protected APDU.
Expected results	1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 2. '7C 00 90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 3. ISO checking error. The chip MUST delete the session keys which were derived in step 1 of the test preconditions and MUST NOT accept any APDUs with these session keys.

3.5.3 Test case ISO7816_II_3

Test - ID	ISO7816_II_3
Purpose	MSE:Set AT / General Authenticate commands with invalid ephemeral public key (different key size)
Version	1.2
Profile	CA_ATGA, ECDH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set AT APDU to the eMRTD. '0C 22 41 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' - <Cryptogram> contains the following encrypted data objects 80 <L_{80}> <cryptographic mechanism reference> 84 <L_{84}> <private key reference> - The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14. 2. Send the given General Authenticate APDU to the eMRTD. '0C 86 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 97 <L_{97}> <Ne> 8E 08 <Checksum> <Le>' - <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L_{80}> <ephemeral public key> - The ephemeral public key MUST be generated with domain parameters specifying a different key size (e.g. for a 224 bit key in DG14 a 192 bit ephemeral key pair is created) 3. To verify that the session keys derived in step 1 of the test preconditions can still be used, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the session keys derived in step 1 of the test preconditions.
Expected results	1. '90 00' in a valid Secure Messaging response. The returned data MUST be

	encoded with the session keys derived in step 1 of the test preconditions. 2. ISO checking error, or warning SW ’63 00’. If chip returns SW ’63 00’, response data field MAY contain ‘7C 00’. If chip returns an ISO checking error SW, response data field SHALL be absent. Since there are invalid domain parameters used to generate the ephemeral key pair, the key agreement process MUST always fail. 3. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions.

3.5.4 Test case ISO7816_II_4

Test - ID	ISO7816_II_4
Purpose	MSE:Set AT / General Authenticate commands with a valid ephemeral public key, but without established PACE or BAC session
Version	1.4
Profile	CA_ATGA
Preconditions	1. The "Open ePassport Application" procedure MUST NOT have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read BEFORE to be able to generate an ephemeral key pair.

Test scenario	1. Select the ePassport application.
	`‘00 A4 04 0C 07 A0 00 00 02 47 10 01’`
	2. Send the given MSE:Set AT APDU to the eMRTD.
	‘00 22 41 A4 <Lc> 80 <L_{80}> <cryptographic mechanism reference> 84 <L_{84}> <private key reference>’
	- The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in data group 14.
	3. Send the given General Authenticate APDU to the eMRTD.
	`‘00 86 00 00 <Lc> 7C <L7C> 80 <L80> <ephemeral public key> <Le>’`
	4. To verify that the chip does not activate the new session keys based on the key agreement, the Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the new session keys based on step 3.

Expected results	1. ISO checking error or ’90 00’ as a plain response without Secure Messaging. If this step returns ISO checking error, the next steps SHALL be skipped. 2. ISO checking error or ’90 00’ as a plain response without Secure Messaging. Note that some chip OS accept the selection of an unavailable private key and return an error only when the public key is used for the selected purpose. 3. ISO checking error or ’90 00’ as a plain response without Secure Messaging. 4. ISO checking error. The error code SHALL be returned as plain data without SM encoding.

3.5.5 Test case ISO7816_II_5

Test - ID	ISO7816_II_5
Purpose	MSE:Set AT / General Authenticate commands with a valid ephemeral public key, but without SecureMessaging
Version	1.2
Profile	CA_ATGA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set AT APDU to the eMRTD (without Secure Messaging). '00 22 41 A4 <Lc> 80 <L$_{80}$> <CA OID> 84 <L$_{84}$> <private key reference>' • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in data group 14. 2. Send the given General Authenticate APDU to the eMRTD (without Secure Messaging). '00 86 00 00 <Lc> 7C <L$_{7C}$> 80 <L$_{80}$> <ephemeral public key> <Le>' 3. To verify that the chip has deleted the session keys derived in step 1 of the test preconditions, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the session keys derived in step 1 of the test precondition.
Expected results	1. ISO checking error or '90 00'. In case of an error code, it SHALL be returned as plain data without SM encoding. 2. ISO checking error. The error code SHALL be returned as plain data without SM encoding. 3. ISO checking error. The error code SHALL be returned as plain data without SM encoding.

3.5.6 Test case ISO7816_II_6

Test - ID	ISO7816_II_6
Purpose	MSE:Set AT / General Authenticate commands with correct ephemeral public key but invalid class byte
Version	1.2
Profile	CA_ATGA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set AT APDU to the eMRTD. '8C 22 41 A4 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 80 <L$_{80}$> <cryptographic mechanism reference> 84 <L$_{84}$> <private key reference> • The class byte has been set to an invalid value of 8C. • The private key reference MUST be included in the APDU if and only

	if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14. 2. Send the given General Authenticate APDU to the eMRTD. ‘8C 86 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 97 <L_{97}> <Ne> 8E 08 <Checksum> <Le>’ - <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L_{80}> <ephemeral public key> - The class byte has been set to an invalid value of 8C.
Expected results	1. ISO checking error. Note that the behavior of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. 2. ISO checking error. Response data field SHALL be absent. Note that the behavior of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response.

3.5.7 Test case ISO7816_II_7

Test - ID	ISO7816_II_7
Purpose	MSE:Set AT / General Authenticate commands with invalid data object tag for the ephemeral public key
Version	1.2
Profile	CA_ATGA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set AT APDU to the eMRTD. ‘0C 22 41 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the following encrypted data objects 80 <L_{80}> <cryptographic mechanism reference> 84 <L_{84}> <private key reference> - The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14. 2. Send the given General Authenticate APDU to the eMRTD. ‘0C 86 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 97 <L_{97}> <Ne> 8E 08 <Checksum> <Le>’ - <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 81 <L_{81}> <ephemeral public key> - The data object for the ephemeral public key has an invalid tag 81. 3. To verify that the session keys derived in step 1 of the test preconditions are still valid, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the session keys derived in step1 of the test precondition.
Expected results	1. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 2. ISO checking error. Response data field SHALL be absent. The error MUST be encoded in a Secure Messaging response using the session keys derived in step 1 of the test preconditions. 3. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions.

3.5.8 Test case ISO7816_II_8

Test - ID	ISO7816_II_8
Purpose	MSE:Set AT / General Authenticate commands, providing a (0,0) public key to General Authenticate
Version	1.2
Profile	CA_ATGA, ECDH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set AT APDU to the eMRTD. ‘0C 22 41 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the following encrypted data objects 80 <L_{80}> <cryptographic mechanism reference> 84 <L_{84}> <private key reference> - The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14. 2. Send the given General Authenticate APDU to the eMRTD. ‘0C 86 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 97 <L_{97}> <Ne> 8E 08 <Checksum> <Le>’ - <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L_{80}> <ephemeral public key> - The public key has to be coded as ‘04||x||y’ where both x and y have a size according to the prime, but filled with ‘00’. 3. To verify that the session keys derived in step 1 of the test preconditions are still valid, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the session keys derived in step 1of the test precondition.
Expected results	1. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 2. ISO checking error or warning SW ’63 00’. If chip returns SW ’63 00’, response data field MAY contain ‘7C 00’. If chip returns an ISO checking error SW, response data field SHALL be absent. Note: Even if public key validation is not done, DH computation SHOULD fail with this input. The error MUST be encoded in a Secure Messaging response using the session keys derived in step 1 of the test preconditions. 3. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions.

3.5.9 Test case ISO7816_II_9

Test - ID	ISO7816_II_9
Purpose	MSE:Set AT / General Authenticate commands, test borderline cases for x- and y-coordinates (small x coordinate)
Version	1.2
Profile	CA_ATGA, ECDH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.

Test scenario	1. Send the given MSE:Set AT APDU to the eMRTD.
	`‘0C 22 41 A4 <Lc> 87 <`L_{87}`> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	• <Cryptogram> contains the following encrypted data objects
	`80 <`L_{80}`> <cryptographic mechanism reference>`
	`84 <`L_{84}`> <private key reference>`
	• The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14.
	2. Send the given General Authenticate APDU to the eMRTD.
	`‘0C 86 00 00 <Lc> 87 <`L_{87}`> 01 <Cryptogram> 97 <`L_{97}`> <Ne> 8E 08 <Checksum> <Le>’`
	• <Cryptogram> contains the following encrypted data objects
	`7C <`L_{7C}`> 80 <`L_{80}`> <ephemeral public key>`
	• Use an ephemeral public key with an x-coordinate requiring less than [$\log_{256}$ q] bytes to be represented. Pad with prepended zero bytes. (For details on q see [R7])
	3. To verify the chips ability to continue the Secure Messaging with the new session keys, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the new session keys.

Expected results	1. ‘90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 2. `‘7C 00 90 00’` in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 3. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the new session keys.

3.5.10 Test case ISO7816_II_10

Test - ID	ISO7816_II_10
Purpose	MSE:Set AT / General Authenticate commands, test borderline cases for x- and y-coordinates (large x coordinate)
Version	1.2
Profile	CA_ATGA, ECDH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.

Test scenario	1. Send the given MSE:Set AT APDU to the eMRTD.
	`‘0C 22 41 A4 <Lc> 87 <`L_{87}`> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	• <Cryptogram> contains the following encrypted data objects
	`80 <`L_{80}`> <cryptographic mechanism reference>`
	`84 <`L_{84}`> <private key reference>`
	• The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14.
	2. Send the given General Authenticate APDU to the eMRTD.
	`‘0C 86 00 00 <Lc> 87 <`L_{87}`> 01 <Cryptogram> 97 <`L_{97}`> <Ne> 8E 08 <Checksum> <Le>’`
	• <Cryptogram> contains the following encrypted data objects
	`7C <`L_{7C}`> 80 <`L_{80}`> <ephemeral public key>`

	- Use a ephemeral public key with an x-coordinate having its most significant bit set to 1 3. To verify the chips ability to continue the Secure Messaging with the new session keys, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the new session keys.
Expected results	1. ‘90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 2. ‘7C 00 90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 3. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the new session keys.

3.5.11 Test case ISO7816_II_11

Test - ID	ISO7816_II_11
Purpose	MSE:Set AT / General Authenticate commands, test borderline cases for x- and y-coordinates (small y coordinate)
Version	1.2
Profile	CA_ATGA, ECDH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set AT APDU to the eMRTD. ‘0C 22 41 A4 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the following encrypted data objects 80 <L$_{80}$> <cryptographic mechanism reference> 84 <L$_{84}$> <private key reference> - The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the data group 14. 2. Send the given General Authenticate APDU to the eMRTD. ‘0C 86 00 00 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 97 <L$_{97}$> <Ne> 8E 08 <Checksum> <Le>’ - <Cryptogram> contains the following encrypted data objects 7C <L$_{7C}$> 80 <L$_{80}$> <ephemeral public key> - Use an ephemeral public key with an y-coordinate requiring less than [log$_{256}$ q] bytes to be represented. Pad with zero bytes. (For details on q see [R7]) 3. To verify the chips ability to continue the Secure Messaging with the new session keys, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the new session keys.
Expected results	1. ‘90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 2. ’7C 00 90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 3. ’90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the new session keys.

3.5.12 Test case ISO7816_II_12

Test - ID	ISO7816_II_12
Purpose	MSE:Set AT / General Authenticate commands, test borderline cases for x- and y-coordinates (large y coordinate)
Version	1.2
Profile	CA_ATGA, ECDH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.

Test scenario	1. Send the given MSE:Set AT APDU to the eMRTD.
	`‘0C 22 41 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	• <Cryptogram> contains the following encrypted data objects
	`80 <L80> <cryptographic mechanism reference>`
	`84 <L84> <private key reference>`
	• The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in data group 14.
	2. Send the given General Authenticate APDU to the eMRTD.
	`‘0C 86 00 00 <Lc> 87 <L87> 01 <Cryptogram> 97 <L97> <Ne> 8E 08 <Checksum> <Le>’`
	• <Cryptogram> contains the following encrypted data objects
	`7C <L7C> 80 <L80> <ephemeral public key>`
	• Use a ephemeral public key with an y-coordinate having its highest bit set to 1
	3. To verify the chips ability to continue the Secure Messaging with the new session keys, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the new session keys.

Expected results	1. ‘90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 2. `‘7C 00 90 00’` in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 3. ’90 00’ and a valid Secure Messaging response. The returned data MUST be encoded with the new session keys.

3.5.13 Test case ISO7816_II_13

Test - ID	ISO7816_II_13
Purpose	MSE:Set AT command with an incorrect private key reference *Note: The support for key references is mandatory for the chip in case it has several chip authentication private keys, and optional in case it only has one private key.*
Version	1.2
Profile	CA_ATGA, KeyRef
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.
Test scenario	1. Send the given MSE:Set AT APDU to the eMRTD. `‘0C 22 41 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08`

	`<Checksum> 00'`
	• <Cryptogram> contains the following encrypted data objects
	`80 <L80> <cryptographic mechanism reference>`
	`84 <L84> <invalid private key reference>`
	• A private key reference MUST be included in the APDU. This key reference MUST be different from the one potentially specified in the ChipAuthenticationPublicKeyInfo structure stored in data grou 14 (see ICS).
	2. To verify that the session keys derived in step 1 of the test preconditions are still valid, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the session keys derived in step 1 of the test precondition.

Expected results	1. ISO checking error or warning processing '63 00'. The error MUST be encoded in a Secure Messaging response using the session keys derived in step 1 of the test preconditions. 2. '90 00' and a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions.

3.5.14 Test case ISO7816_II_14

Test - ID	ISO7816_II_14
Purpose	Check the Chip authentication failure (using DH) – wrong value (value strictly bigger than the Prime)
Version	1.2
Profile	CA_ATGA, DH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.

Test scenario	1. Send the given MSE:Set AT APDU to the eMRTD.
	`'0C 22 41 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'`
	• <Cryptogram> contains the following encrypted data objects
	`80 <L80> <cryptographic mechanism reference>`
	`84 <L84> <private key reference>`
	• The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in data group 14.
	2. Send the given General Authenticate APDU to the eMRTD.
	`'0C 86 00 00 <Lc> 87 <L87> 01 <Cryptogram> 97 <L97> <Ne> 8E 08 <Checksum> <Le>'`
	• <Cryptogram> contains the following encrypted data objects
	`7C <L7C> 80 <L80> <ephemeral public key>`
	• Use an ephemeral public key with a wrong value (value strictly bigger than the Prime)
	ephemeral public key = prime p + 1
	3. To verify that the session keys derived in step 1 of the test preconditions are still valid, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the session keys derived in step 1 of the precondition.

Expected results	1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions.

	2. ISO checking error or warning SW ’63 00’. If chip returns SW ’63 00’, response data field MAY contain ‘7C 00’. If chip returns an ISO checking error SW, response data field SHALL be absent. The error MUST be encoded in a Secure Messaging response using the session keys derived in step 1 of the test preconditions. 3. ’90 00’ and a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions.

3.5.15 Test case ISO7816_II_15

Test - ID	ISO7816_II_15
Purpose	Check the Chip authentication failure (using ECDH) – wrong point (value does not belong to the curve)
Version	1.2
Profile	CA_ATGA, ECDH
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The ChipAuthenticationPublicKeyInfo stored in data group 14 MUST have been read to be able to generate an ephemeral key pair.

Test scenario	1. Send the given MSE:Set AT APDU to the eMRTD.
	`‘0C 22 41 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the following encrypted data objects
	`80 <L80> <cryptographic mechanism reference>`
	`84 <L84> <private key reference>`
	- The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in data group 14.
	2. Send the given General Authenticate APDU to the eMRTD.
	`‘0C 86 00 00 <Lc> 87 <L87> 01 <Cryptogram> 97 <L97> <Ne> 8E 08 <Checksum> <Le>’`
	- <Cryptogram> contains the following encrypted data objects
	`7C <L7C> 80 <L80> <ephemeral public key>`
	- Use an ephemeral public key with a wrong point (value does not belong to the curve)
	3. To verify that the session keys derived in step 1 of the test preconditions are still valid, the Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the session keys derived in step 1 of the test precondition.

Expected results	1. ‘90 00’ in a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions. 2. ISO checking error or warning SW ’63 00’. If chip returns SW ’63 00’, response data field MAY contain ‘7C 00’. If chip returns an ISO checking error SW, response data field SHALL be absent. The error MUST be encoded in a Secure Messaging response using the session keys derived in step 1 of the test preconditions. 3. ’90 00’ and a valid Secure Messaging response. The returned data MUST be encoded with the session keys derived in step 1 of the test preconditions.

3.6 Unit ISO7816_J – Certificate verification

During the Terminal Authentication process the certificate chain from the trust point stored in the chips EF.CVCA file down to the inspection systems CV certificate is verified. This is done by an alternating sequence of MSE: Set DST and Verify Certificate commands. This unit covers all certificate verification test cases which do NOT update the chips persistent memory. This means that all tests in this unit can be repeated with the same set of certificates.

3.6.1 Test case ISO7816_J_1

Test - ID	ISO7816_J_1
Purpose	Positive test with a valid chain of CV certificates.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L$_{7F4E}$> <certificate body>
	5F 37 <L$_{5F37}$> <certificate signature>

Expected results	1. ’90 00’ in a valid SM response. 2. ’90 00’ in a valid SM response. 3. ’90 00’ in a valid SM response. 4. ’90 00’ in a valid SM response.

3.6.2 Test case ISO7816_J_2

Test - ID	ISO7816_J_2
Purpose	Test with an invalid Certification Authority Reference.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	• <Cryptogram> contains the following encrypted data objects
	83 <L_{83}> <BAD certificate authority reference>
	• The Certification Authority Reference read from the EF.CVCA is changed in the last character to create an invalid reference.
	2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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 <L87> 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 <L87> 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>

Expected results	1. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 2. ISO checking error or ‘6300’ in a valid SM response. 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or ‘6300’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.3 Test case ISO7816_J_3

Test - ID	ISO7816_J_3
Purpose	Test with an invalid certificate signature.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’`
	- <Cryptogram> contains the following encrypted data objects
	7F 4E <L_{7F4E}> <certificate body>
	5F 37 <L_{5F37}> <bad certificate signature>
	- The signature object of the certificate has been changed in last digit to make it invalid
	3. Send the given MSE: Set DST APDU to the eMRTD.
	`‘0C 22 81 B6 <Lc> 87 <L87> 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 <L87> 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>

Expected results	1. ’90 00’ in a valid SM response. 2. ISO checking error or ’63 00’ in a valid SM response. 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or ’63 00’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.4 Test case ISO7816_J_4

Test - ID	ISO7816_J_4
Purpose	Test with a missing certificate signature.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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> - The certificate signature object is omitted. 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	1. ’90 00’ in a valid SM response. 2. ISO checking error or ’63 00’ in a valid SM response. 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or ’63 00’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.5 Test case ISO7816_J_5

Test - ID	ISO7816_J_5
Purpose	Test with a missing certificate body.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 5F 37 <L$_{5F37}$> <certificate signature> - The certificate body object is omitted. 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 <L$_{7F4E}$> <certificate body> 5F 37 <L$_{5F37}$> <certificate signature>
Expected results	1. ’90 00’ in a valid SM response. 2. ISO checking error or ’63 00’ in a valid SM response. 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or ’63 00’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.6 Test case ISO7816_J_6

Test - ID	ISO7816_J_6
Purpose	Test a DV certificate with a missing Holder Authorization.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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_1a. ‘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> - The certificate does not contain a certificate holder authorization 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or ‘6300’ in a valid SM response. 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or ‘6300’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.7 Test case ISO7816_J_7

Test - ID	ISO7816_J_7
Purpose	Test a DV certificate with a missing effective date.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed.

	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_1b. ‘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> - The certificate does not have a certificate effective date tag. 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	1. ’90 00’ in a valid SM response. 2. ISO checking error or ‘6300’ in a valid SM response. 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or ‘6300’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.8 Test case ISO7816_J_8

Test - ID	ISO7816_J_8
Purpose	Test a DV certificate with a missing expiration date.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been

	performed. 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 <L87> 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_1c.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	- The certificate does not have a certificate expiration date tag.
	3. Send the given MSE: Set DST APDU to the eMRTD.
	`‘0C 22 81 B6 <Lc> 87 <L87> 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 <L87> 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>

Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or ‘6300’ in a valid SM response. 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or ‘6300’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.9 Test case ISO7816_J_9

Test - ID	ISO7816_J_9
Purpose	Test a DV certificate with an incorrect encoded effective date. (bad BCD coding) Note: The date format verification is not mandatory for the chip. This test is set optional.

Version	1.2
Profile	TA, DATE
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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_1d. ‘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> - The certificate contains a badly encoded BCD effective date. 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or ’63 00’ in a valid SM response. 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or ’63 00’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.10 Test case ISO7816_J_10

Test - ID	ISO7816_J_10

Purpose	Test a DV certificate with an incorrect encoded expiration date. (bad BCD coding) Note: The date format verification is not mandatory for the chip. This test is set optional.
Version	1.2
Profile	TA, DATE
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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_1e. '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> - The certificate contains a badly encoded BCD expiration date. 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	1. '90 00' in a valid SM response 2. ISO checking error or '6300' in a valid SM response. 3. '90 00' or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or '6300' in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.11 Test case ISO7816_J_11

Test - ID	ISO7816_J_11
Purpose	Test the “Current Date” update mechanism with a new foreign IS certificate.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	• <Cryptogram> contains the following encrypted data objects
	`83 <L83> <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 2” chapter as DV_CERT_2.
	`‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’`
	• <Cryptogram> contains the following encrypted data objects
	`7F 4E <L7F4E> <certificate body>`
	`5F 37 <L5F37> <certificate signature>`
	• This DV-certificate is marked as a foreign DV-certificate.
	3. Send the given MSE: Set DST APDU to the eMRTD.
	`‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	• <Cryptogram> contains the following encrypted data objects
	`83 <L83> <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 2” chapter as IS_CERT_2a.
	`‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’`
	• <Cryptogram> contains the following encrypted data objects
	`7F 4E <L7F4E> <certificate body>`
	`5F 37 <L5F37> <certificate signature>`
	• This certificate has an advanced effective date. Since the DV certificate was marked as a foreign one, the chip MUST NOT update the current date.
	• Reset the chip after this step and restore the preconditions for this test case before the next step is performed.
	5. Send the given MSE: Set DST APDU to the eMRTD.
	`‘0C 22 81 B6 <Lc> 87 <L87> 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. 6. Send the appropriate DV-Certificate as specified in the “Certificate Set 2” chapter as DV_CERT_2. ‘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> - This DV-certificate is marked as a foreign DV-certificate. 7. 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 6 has to be used. 8. Send the appropriate IS-Certificate as specified in the “Certificate Set 2” chapter as IS_CERT_2b. ‘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> - This certificate expiration date is BEFORE the effective date of the IS-Certificate used in step 4.
Expected results	1. ’90 00’ in a valid SM response. 2. ’90 00’ in a valid SM response. 3. ’90 00’ in a valid SM response. 4. ’90 00’ in a valid SM response. 5. ’90 00’ in a valid SM response. 6. ’90 00’ in a valid SM response. 7. ’90 00’ in a valid SM response. 8. ’90 00’ in a valid SM response. This certificate MUST still be accepted since the chip MUST NOT change the current date based on the foreign IS certificate.

3.6.12 Test case ISO7816_J_12

Test - ID	ISO7816_J_12
Purpose	Test with a valid chain of CV certificates but without using SecureMessaging.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed.

	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. `'00 22 81 B6 <Lc> 83 <Certification Authority Reference>'`
	- The Certification Authority Reference MUST be used as read from the EF.CVCA file.
	- The APDU is send in plain without Secure Messaging
	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>`
	- The APDU is send as a valid SM APDU.
	After step 2, the passport is reset and the preconditions of this test case are reestablished.
	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 Authority Reference MUST be used as read from the EF.CVCA file.
	- The APDU is send as a valid SM APDU.
	4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1. `'00 2A 00 BE <Lc> 7F 4E <L`$_{7F4E}$`> <body> 5F 37 <L`$_{5F37}$`> <signature>'`
	5. 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 4 has to be used.
	- The APDU is send as a valid SM APDU.

Expected results	1. ISO checking error. The SM channel MUST be closed as soon as an unprotected APDU is send. The error code SHALL be returned as plain data without SM encoding. 2. ISO checking error. Since the SM channel MUST have been closed in Step 1, the chip MUST return an error without SM encoding here. 3. ’90 00’ in a valid SM response 4. ISO checking error. The SM channel MUST be closed as soon as an unprotected APDU is send. The error code SHALL be returned as plain

	data without SM encoding. 5. ISO checking error. Since the SM channel MUST have been closed in Step 4, the chip MUST return an error without SM encoding here.

3.6.13 Test case ISO7816_J_13

Test - ID	ISO7816_J_13
Purpose	Test the MSE:Set DST command with an invalid class byte.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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. ‘8C 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. - The class byte is set to an invalid value. 2. If the error code in step 1 was returned in a Secure Messaging response, verify that the secure messaging session has not been aborted. If a plain error code was returned, this step is skipped. The Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the session keys derived in step 2 of the preconditions.
Expected results	1. ISO checking error. Note that the behaviour of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. 2. Skipped or ’90 00’ in a valid SM response

3.6.14 Test case ISO7816_J_14

Test - ID	ISO7816_J_14
Version	Deleted in version 1.1

3.6.15 Test case ISO7816_J_15

Test - ID	ISO7816_J_15
Purpose	Test the Verify Certificate command with an invalid class byte.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed.

	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. ‘8C 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> • The class byte has been set to an invalid value (‘8C’). 3. If the error code in step 2 was returned in a Secure Messaging response, verify that the secure messaging session has not been aborted. If a plain error code was returned, this step is skipped. The Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the session keys derived in step 2 of the preconditions.
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error. Note that the behaviour of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. 3. Skipped or ’90 00’ in a valid SM response

3.6.16 Test case ISO7816_J_16

Test - ID	ISO7816_J_16
Version	Deleted in version 1.1

3.6.17 Test case ISO7816_J_17

Test - ID	ISO7816_J_17
Purpose	Test with an invalid certificate body tag.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 4F <L$_{7F4F}$> <certificate body> 5F 37 <L$_{5F37}$> <certificate signature> • The certificate body tag has been changed to ‘7F 4F’ 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 <L$_{7F4E}$> <certificate body> 5F 37 <L$_{5F37}$> <certificate signature>
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or ’63 00’ in a valid SM response. 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or ’63 00’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.18 Test case ISO7816_J_18

Test - ID	ISO7816_J_18
Purpose	Test with an invalid certificate signature tag.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 38 <L_{5F38}> <certificate signature> - The certificate signature tag has been changed to ‘5F 38’ 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or ’63 00’ in a valid SM response. 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or ’63 00’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.19 Test case ISO7816_J_19

Test - ID	ISO7816_J_19
Purpose	Test a DV certificate with an incorrect Gregorian effective date. Note: The date format verification is not mandatory for the chip. This test is set optional.
Version	1.2
Profile	TA, DATE
Preconditions	1. The "Open ePassport Application" procedure MUST have been

	performed. 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_1f. '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> • The certificate contains an invalid Gregorian effective date. 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 <L$_{7F4E}$> <certificate body> 5F 37 <L$_{5F37}$> <certificate signature>
Expected results	1. '90 00' in a valid SM response 2. ISO checking error or '63 00' in a valid SM response. 3. '90 00' or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or '63 00' in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.20 Test case ISO7816_J_20

Test - ID	ISO7816_J_20
Purpose	Test a DV certificate with an incorrect Gregorian expiration date. Note: The date format verification is not mandatory for the chip. This test is set optional.

Version	1.2
Profile	TA, DATE
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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_1g. ‘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> - The certificate contains an invalid Gregorian expiration date. 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or ‘6300’ in a valid SM response. 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or ‘6300’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.21 Test case ISO7816_J_21

Test - ID	ISO7816_J_21

Purpose	Test a DV certificate with an expiration date BEFORE the effective date.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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_1h. ‘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> - The certificate contains an expiration date BEFORE the effective date. 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or ‘6300’ in a valid SM response. 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or ‘6300’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.22 Test case ISO7816_J_22

Test - ID	ISO7816_J_22
Purpose	Test correct removal of temporary keys.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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. Reset the chip, perform the “Open ePassport Application” procedure and the Chip Authentication. 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	1. ’90 00’ in a valid SM response. 2. ’90 00’ in a valid SM response 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or ‘6300’ in a valid SM response. The temporary key of the DV certificate MUST have been deleted during the reset. Therefore it MUST NOT be possible to verify the IS certificate based on this key.

3.6.23 Test case ISO7816_J_23

Test - ID	ISO7816_J_23
Purpose	Test a DV certificate with invalid OID in the Certificate Holder Authorization element.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 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_1i. `‘0C 2A 00 BE <Lc> 87 <L87> 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> • The certificate has an invalid OID in the Certificate Holder Authorization element. Note: If the chip supports further OIDs in addition to the ones specified in [R2], this MUST be stated in the ICS (See 4.3). For this test an OID MUST be used which is NOT supported by the chip. 3. Send the given MSE: Set DST APDU to the eMRTD. `‘0C 22 81 B6 <Lc> 87 <L87> 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 <L87> 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>
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or ‘6300’ in a valid SM response. 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error

	only when the public key is used for the selected purpose. 4. ISO checking error or ‘6300’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.24 Test case ISO7816_J_24

Test - ID	ISO7816_J_24
Purpose	Test a DV certificate invalid OID in the Public Key element.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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_1j. ‘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> • The certificate has an invalid OID in the Public Key element. 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or ‘6300’ in a valid SM response. 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip

	OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or ‘6300’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.25 Test case ISO7816_J_25

Test - ID	ISO7816_J_25
Purpose	Test the CVCA root key selection with a wrong name (CAR) - Current date not updated
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification to the eMRTD with a wrong CAR. ‘0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the encrypted wrong CVCA key Name. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12a. ‘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> - The certificate is issued by the CVCA whose selection SHOULD have failed. - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. - Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with a correct CVCA key name (CAR). ‘0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the encrypted Name (CAR) - The Certification Authority Reference MUST be used as read from the EF.CVCA file. 4. 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> - This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	1. ’90 00’ or ISO checking error in a valid SM response. A chip may permit the selection of an unknown key. 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.26 Test case ISO7816_J_26

Test - ID	ISO7816_J_26
Purpose	Test a DV certificate with a wrong certificate body tag - Current date not updated
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification ‘0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the encrypted CVCA key Name (CAR) - 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 12” chapter as DV_CERT_12b. ‘0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ - <Cryptogram> contains the following encrypted data objects **7F 4F** <L_{7F4F}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> - The tag of the certificate body is wrong. - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. - Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA. ‘0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the encrypted CVCA key Name (CAR) - The Certification Authority Reference MUST be used as read from the EF.CVCA file. 4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1”

	chapter as DV_CERT_1. `‘0C 2A 00 BE <Lc> 87 <L87> 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> - This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.27 Test case ISO7816_J_27

Test - ID	ISO7816_J_27
Purpose	Test a DV certificate with a wrong certificate signature tag - Current date not updated
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification `‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’` - <Cryptogram> contains the encrypted CVCA key Name (CAR). - 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 12” chapter as DV_CERT_12c. `‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’` - <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> **5F 38** <L_{5F38}> <certificate signature> - The tag of the certificate signature is wrong. - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. - Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA. `‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’` - <Cryptogram> contains the encrypted CVCA key Name (CAR)

	- The Certification Authority Reference MUST be used as read from the EF.CVCA file. 4. 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> - This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.28 Test case ISO7816_J_28

Test - ID	ISO7816_J_28
Purpose	Test a DV certificate with a wrong certificate body length - Current date not updated
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification ‘0C 22 81 B6 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the encrypted CVCA key Name (CAR). ´ - 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 12” chapter as DV_CERT_12d. ‘0C 2A 00 BE <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ - <Cryptogram> contains the following encrypted data objects 7F 4E <L$_{7F4E}$> + 1 <certificate body> 5F 37 <L$_{5F37}$> <certificate signature> - The length of the certificate body is unconsistent. - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. - Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE Set DST APDU to initiate the certificate verification to the

	eMRTD with the CAR of the CVCA. ‘0C 22 81 B6 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> 00’ • <Cryptogram> contains the encrypted CVCA key Name (CAR) • The Certification Authority Reference MUST be used as read from the EF.CVCA file. 4. 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> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.29 Test case ISO7816_J_29

Test - ID	ISO7816_J_29
Purpose	Test a DV certificate with a wrong certificate signature length - Current date not updated
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification. ‘0C 22 81 B6 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> 00’ • <Cryptogram> contains the encrypted CVCA key Name (CAR). • 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 12” chapter as DV_CERT_12e. ‘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$_{5F37}$> + 1 <certificate signature> • The length of the certificate signature is unconsistent. • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.

	- Reset the chip after this step and restore the preconditions for this test case before the next step is performed.
	3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.
	`‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the encrypted CVCA key Name (CAR)
	- The Certification Authority Reference MUST be used as read from the EF.CVCA file.
	4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	- This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.30 Test case ISO7816_J_30

Test - ID	ISO7816_J_30
Purpose	Test a DV certificate with a wrong certificate signature (Last byte increased by 1) - Current date not updated
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification
	`‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the encrypted CVCA key Name (CAR).
	- 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 12” chapter as DV_CERT_12f.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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 + 1>

	- The certificate signature is wrong. It is obtained by increasing a correct signature by one.
	- This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.
	- Reset the chip after this step and restore the preconditions for this test case before the next step is performed.
	3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.
	`‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the encrypted CVCA key Name (CAR)
	- The Certification Authority Reference MUST be used as read from the EF.CVCA file.
	4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	- This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.31 Test case ISO7816_J_31

Test - ID	ISO7816_J_31
Purpose	Test a DV certificate with a wrong certificate signature (Dropping last byte of the signature) - Current date not updated
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification. `‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’` - <Cryptogram> contains the encrypted CVCA key Name (CAR). - 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 12” chapter as DV_CERT_12g

	`'0C 2A 00 BE <Lc> 87 <L87> 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>
	• The certificate signature is wrong. It is obtained by dropping the last byte of the certificate signature (the length of the D.O. remains consistent)
	• This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.
	• Reset the chip after this step and restore the preconditions for this test case before the next step is performed.
	3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.
	`'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'`
	• <Cryptogram> contains the encrypted CVCA key Name (CAR)
	• The Certification Authority Reference MUST be used as read from the EF.CVCA file.
	4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
	`'0C 2A 00 BE <Lc> 87 <L87> 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>
	• This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.32 Test case ISO7816_J_32

Test - ID	ISO7816_J_32
Purpose	Test a DV certificate with a wrong certificate signature (Signature greater than the modulus) - Current date not updated
Version	1.2
Profile	RSA, TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification. `'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'`

	• <Cryptogram> contains the encrypted CVCA key Name (CAR). • 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 12” chapter as DV_CERT_12o ‘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> • The certificate signature is wrong. It is obtained by setting the signature to a value greater than the modulus. The length of the signature MUST match the length of the modulus. This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA. ‘0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ • <Cryptogram> contains the encrypted CVCA key Name (CAR) • The Certification Authority Reference MUST be used as read from the EF.CVCA file. 4. 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> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.33 Test case ISO7816_J_33

Test - ID	ISO7816_J_33
Purpose	Test a DV certificate with a wrong certificate signature (r = 0) - Current date not updated
Version	1.2
Profile	ECDSA, TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification.
	`‘0C 22 81 B6 <Lc> 87 <L`$_{87}$`> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the encrypted CVCA key Name (CAR).
	- 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 12” chapter as DV_CERT_12p
	`‘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>
	- The certificate signature is wrong. It is obtained by filling the ‘r’ part of the signature with ‘00’. The length of ‘r’ is still matches the size of the prime.
	- This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.
	- Reset the chip after this step and restore the preconditions for this test case before the next step is performed.
	3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.
	`‘0C 22 81 B6 <Lc> 87 <L`$_{87}$`> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the encrypted CVCA key Name (CAR)
	- The Certification Authority Reference MUST be used as read from the EF.CVCA file.
	4. 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>
	- This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.34 Test case ISO7816_J_34

Test - ID	ISO7816_J_34
Purpose	Test a DV certificate with a wrong certificate signature (s = 0) - Current date not updated

Version	1.2
Profile	ECDSA, TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification.
	`‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the encrypted CVCA key Name (CAR).
	- 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 12” chapter as DV_CERT_12q
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	- The certificate signature is wrong. It is obtained by filling the ‘s’ part of the signature with ‘00’. The length of ‘s’ is still matches the size of the prime.
	- This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.
	- Reset the chip after this step and restore the preconditions for this test case before the next step is performed.
	3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.
	`‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the encrypted CVCA key Name (CAR)
	- The Certification Authority Reference MUST be used as read from the EF.CVCA file.
	4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	- This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.35 Test case ISO7816_J_35

Test - ID	ISO7816_J_35
Purpose	Test a DV certificate without selecting any root key - Current date not updated
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12a. ‘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> - As no current key is selected, the certificate verification SHOULD fail. - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. - Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 2. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA. ‘0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the encrypted CVCA key Name (CAR) - The Certification Authority Reference MUST be used as read from the EF.CVCA file. 3. 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> - This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	1. ISO checking error or warning processing ’63 00’ in a valid SM response 2. ’90 00’ in a valid SM response 3. ’90 00’ in a valid SM response

3.6.36 Test case ISO7816_J_36

Test - ID	ISO7816_J_36

Purpose	Test a DV certificate while the Public Key D.O has a wrong O.I.D field - Current date not updated
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification.
	`‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the encrypted CVCA key Name (CAR).
	- 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 12” chapter as DV_CERT_12i
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	- The Public Key D.O. in the certificate body contains an uncorrect O.I.D that does not indicate id-TA (0.4.0.127.0.7.2.2.**3**.x.y).
	- This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.
	- Reset the chip after this step and restore the preconditions for this test case before the next step is performed.
	3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.
	`‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the encrypted CVCA key Name (CAR)
	- The Certification Authority Reference MUST be used as read from the EF.CVCA file.
	4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	- This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.37 Test case ISO7816_J_37

Test - ID	ISO7816_J_37
Purpose	Test a DV certificate while the Public Key D.O has no O.I.D field - Current date not updated
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification.
	`‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the encrypted CVCA key Name (CAR).
	- 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 12” chapter as DV_CERT_12h.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	- The Public Key D.O. in the certificate body does not contain an O.I.D field.
	- This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.
	- Reset the chip after this step and restore the preconditions for this test case before the next step is performed.
	3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.
	`‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the encrypted CVCA key Name (CAR)
	- The Certification Authority Reference MUST be used as read from the EF.CVCA file.
	4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	- This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

Expected results	1. ’90 00’ in a valid SM response

	2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.38 Test case ISO7816_J_38

Test - ID	ISO7816_J_38
Purpose	Test a DV certificate while the Public Key D.O has no Public point field - Current date not updated
Version	1.2
Profile	ECDSA, TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification. ‘0C 22 81 B6 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the encrypted CVCA key Name (CAR). - 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 12” chapter as DV_CERT_12j ‘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> - The Public Key D.O. in the certificate body does not contain any EC Public point field. - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. - Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA. ‘0C 22 81 B6 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the encrypted CVCA key Name (CAR) - The Certification Authority Reference MUST be used as read from the EF.CVCA file. 4. 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> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.39 Test case ISO7816_J_39

Test - ID	ISO7816_J_39
Purpose	Test a DV certificate while the Public Key D.O has no Modulus field - Current date not updated
Version	1.2
Profile	RSA, TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification.
	`‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	• <Cryptogram> contains the encrypted CVCA key Name (CAR).
	• 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 12” chapter as DV_CERT_12k
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	• The Public Key D.O. in the certificate body does not contain any RSA Modulus field.
	• This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.
	• Reset the chip after this step and restore the preconditions for this test case before the next step is performed.
	3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.
	`‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	• <Cryptogram> contains the encrypted CVCA key Name (CAR)
	• The Certification Authority Reference MUST be used as read from the EF.CVCA file.
	4. 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> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.40 Test case ISO7816_J_40

Test - ID	ISO7816_J_40
Purpose	Test a DV certificate while the Public Key D.O has no public exponent field - Current date not updated
Version	1.2
Profile	RSA, TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification. ‘0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ • <Cryptogram> contains the encrypted CVCA key Name (CAR). • 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 12” chapter as DV_CERT_12l ‘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> • The Public Key D.O. in the certificate body does not contain any RSA public exponent field. • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA. ‘0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’

	• <Cryptogram> contains the encrypted CVCA key Name (CAR) • The Certification Authority Reference MUST be used as read from the EF.CVCA file. 4. 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> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.41 Test case ISO7816_J_41

Test - ID	ISO7816_J_41
Purpose	Test a DV certificate while the Public Key D.O contains an unknown D.O. - Current date not updated
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 MSE Set DST APDU to initiate the certificate verification. ‘0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ • <Cryptogram> contains the encrypted CVCA key Name (CAR). • 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 12” chapter as DV_CERT_12m ‘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> • The Public Key D.O. in the certificate body contains an unknown D.O (tag ‘77’). • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. • Reset the chip after this step and restore the preconditions for this test

	case before the next step is performed. 3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA. ‘0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00’ - <Cryptogram> contains the encrypted CVCA key Name (CAR) - The Certification Authority Reference MUST be used as read from the EF.CVCA file. 4. 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> - This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	1. ’90 00’ in a valid SM response 2. ISO checking error or warning processing ’63 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response

3.6.42 Test case ISO7816_J_42

Test - ID	ISO7816_J_42
Version	Deleted in version 0.8 (Merged with ISO7816_J_41)

3.6.43 Test case ISO7816_J_43

Test - ID	ISO7816_J_43
Purpose	Test the transition CVCA ⇨ IS key
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 IS-Certificate as specified in the “Certificate Set 10”

	chapter as IS_CERT_10. ‘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>
Expected results	1. The eMRTD MUST return status bytes ‘90 00’ in a valid SM response 2. The eMRTD MUST return a ISO checking error or status bytes ’63 00’ in a valid SM response

3.6.44 Test case ISO7816_J_44

Test - ID	ISO7816_J_44
Purpose	Test the transition CVCA ⇨ domestic DV ⇨ CVCA
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 10” chapter as DV_CERT_10a. ‘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 CA-Certificate as specified in the “Certificate Set 10” chapter as LINK_CERT_10. ‘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>
Expected results	1. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 2. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 3. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 4. The eMRTD MUST return status bytes a ISO checking error or status bytes ’63 00’ in a valid SM response.

3.6.45 Test case ISO7816_J_45

Test - ID	ISO7816_J_45
Purpose	Test the transition CVCA ⇨ foreign DV ⇨ CVCA
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 10” chapter as DV_CERT_10b. ‘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 CA-Certificate as specified in the “Certificate Set 10” chapter as LINK_CERT_10. ‘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>

Expected results	1. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 2. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 3. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 4. The eMRTD MUST return status bytes a ISO checking error or status bytes ’63 00’ in a valid SM response.

3.6.46 Test case ISO7816_J_46

Test - ID	ISO7816_J_46
Purpose	Test the transition CVCA ⇨ domestic DV ⇨ domestic DV
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 10” chapter as DV_CERT_10a. ‘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 DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10c. ‘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>
Expected results	1. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 2. The eMRTD MUST return status bytes ’90 00’ in a valid SM response

	3. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 4. The eMRTD MUST return status bytes a ISO checking error or status bytes ’63 00’ in a valid SM response.

3.6.47 Test case ISO7816_J_47

Test - ID	ISO7816_J_47
Purpose	Test the transition CVCA ⇨ domestic DV ⇨ foreign DV
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 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 10” chapter as DV_CERT_10a.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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 <L87> 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 DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10d.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>

Expected results	1. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 2. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 3. The eMRTD MUST return status bytes ’90 00’ in a valid SM response

	4. The eMRTD MUST return status bytes a ISO checking error or status bytes ’63 00’ in a valid SM response.

3.6.48 Test case ISO7816_J_48

Test - ID	ISO7816_J_48
Purpose	Test the transition CVCA ⇨ foreign DV ⇨ domestic DV
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 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 10” chapter as DV_CERT_10b.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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 <L87> 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 DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10c.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>

Expected results	1. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 2. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 3. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 4. The eMRTD MUST return status bytes a ISO checking error or status bytes ’63 00’ in a valid SM response.

3.6.49 Test case ISO7816_J_49

Test - ID	ISO7816_J_49
Purpose	Test the transition CVCA ⇨ foreign DV ⇨ foreign DV
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 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 10” chapter as DV_CERT_10b.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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 <L87> 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 DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10d.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>

Expected results	1. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 2. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 3. The eMRTD MUST return status bytes ’90 00’ in a valid SM response 4. The eMRTD MUST return status bytes a ISO checking error or status bytes ’63 00’ in a valid SM response.

3.6.50 Test case ISO7816_J_50

Test - ID	ISO7816_J_50
Purpose	Test the transition CVCA ⇨ DV ⇨ IS ⇨ foreign DV
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 11” chapter as DV_CERT_11a. ‘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 11” chapter as IS_CERT_11a. ‘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> 5. 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 IS-Certificate sent in step 4 has to be used. 6. Send the appropriate DV-Certificate as specified in the “Certificate Set 11” chapter as DV_CERT_11b. ‘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>
Expected results	1. ’90 00’ in a valid SM response 2. ’90 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response 5. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 6. ISO checking error or ’63 00’ in a valid SM response.

3.6.51 Test case ISO7816_J_51

Test - ID	ISO7816_J_51
Purpose	Test the transition CVCA ⇨ DV ⇨ IS ⇨ domestic DV
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 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 11” chapter as DV_CERT_11a.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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 11” chapter as IS_CERT_11a.

	‘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> 5. 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 IS-Certificate sent in step 4 has to be used. 6. Send the appropriate DV-Certificate as specified in the “Certificate Set 11” chapter as DV_CERT_11c. ‘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>
Expected results	1. ’90 00’ in a valid SM response 2. ’90 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response 5. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 6. ISO checking error or ’63 00’ in a valid SM response.

3.6.52 Test case ISO7816_J_52

Test - ID	ISO7816_J_52
Purpose	Test the transition CVCA ⇨ DV ⇨ IS ⇨ IS
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 11” chapter as DV_CERT_11a. ‘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 11” chapter as IS_CERT_11a. ‘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> 5. 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 IS-Certificate sent in step 4 has to be used. 6. Send the appropriate IS-Certificate as specified in the “Certificate Set 11” chapter as IS_CERT_11b. ‘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>
Expected results	1. ’90 00’ in a valid SM response 2. ’90 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response 5. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 6. ISO checking error or ’63 00’ in a valid SM response.

3.6.53 Test case ISO7816_J_53

Test - ID	ISO7816_J_53

Purpose	Test the transition CVCA ⇨ DV ⇨ IS ⇨ CVCA
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 11” chapter as DV_CERT_11a. ‘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 11” chapter as IS_CERT_11a. ‘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> 5. 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 IS-Certificate sent in step 4 has to be used. 6. Send the appropriate CVCA-Certificate as specified in the “Certificate Set 11” chapter as LINK_CERT_11a. ‘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>
Expected results	1. ’90 00’ in a valid SM response 2. ’90 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response 5. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 6. ISO checking error or ’63 00’ in a valid SM response.

3.6.54 Test case ISO7816_J_54

Test - ID	ISO7816_J_54
Purpose	Test the transition CVCA ⇨ CVCA ⇨ IS
Version	Has been moved to M_5 in version 1.1

3.6.55 Test case ISO7816_J_55

Test - ID	ISO7816_J_55
Purpose	Test a DV certificate with a wrong Public Key (shorter key length).
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 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 14” chapter as DV_CERT_14b.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	• The key length of this certificate is different to the CVCA public key.
	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 given in the previous DVCA-Certificate sent. 4. Send the appropriate IS-Certificate as specified in the "Certificate Set 14" chapter as IS_CERT_14a. '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>
Expected results	1. '90 00' in a valid SM response 2. ISO checking error or '63 00' in a valid SM response. 3. '90 00' or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. ISO checking error or '63 00' in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.5.56 Test case ISO7816_J_56

Test - ID	ISO7816_J_56
Purpose	Test a IS certificate with a wrong Public Key (shorter key length).
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 CA-Certificate as specified in the "Certificate Set 14" chapter as DV_CERT_14a. '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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'`
	- <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <certificate authority reference>
	- The Certification Holder Reference given in the previous DVCA-Certificate sent.
	4. Send the appropriate IS-Certificate as specified in the “Certificate Set 14” chapter as IS_CERT_14b.
	`'0C 2A 00 BE <Lc> 87 <L87> 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>
	- The key length of this certificate is different to the CVCA and DV certificates public keys.

Expected results	1. ’90 00’ in a valid SM response 2. ’90 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ISO checking error or ’63 00’ in a valid SM response

3.7 Unit ISO7816_K – Terminal Authentication[1]

This unit tests the second part of the terminal authentication process. In this step, the terminal proves the possession of the private key which belongs to the IS certificate.

All test cases of this test unit which require the “Open ePassport Application” procedure MUST be performed twice (one test run with BAC and one with PACE) if the chip supports both protocols. If the chip only supports one of these protocols (BAC or PACE), only one test run has to be performed with the supported protocol used in the “Open ePassport Application” procedure.

3.7.1 Test case ISO7816_K_1

Test - ID	ISO7816_K_1_template
Purpose	Positive test with a valid terminal authentication process
Version	1.2
Profile	see Table 1
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. Use the protocol specified in Table 1. 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.

---

[1] Note that some States have issued MRTDs using a static binding for the combination of PACE and Terminal Authentication. For these MRTDs some test cases of this unit will be replaced by alternative and additional test cases in [R10].

	`‘0C 22 81 B6 <Lc> 87 <L87> 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 <L87> 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 <L87> 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 <L87> 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>
	5. Send the given MSE: Set AT APDU to the eMRTD.
	`‘0C 22 81 A4 <Lc> 87 <L87> 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 as specified in Table 1.

Expected results	1. ’90 00’ in a valid SM response 2. ’90 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response 5. ’90 00’ in a valid SM response 6. ‘<Eight bytes of random data> 90 00’ in an SM response 7. ’90 00’ in a valid SM response

Test – ID	**Profile**	**Precondition**	**Test scenario**

ISO7816_K_1a	TA	Perform BAC with MRZ	7. Send the given external authenticate command to the eMRTD. `‘0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’` - The MRTD chip’s Document number as contain in the MRZ including the check digit MUST be used to build the encrypted terminal signature (S_{PCD}) for the External Authenticate command. <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.
ISO7816_K_1b	TA, PACE	Perform PACE with MRZ or CAN	7. Send the given external authenticate command to the eMRTD. `‘0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’` - The MRTD chip’s ephemeral PACE public key MUST be used to build the encrypted terminal signature (S_{PCD}) for the External Authenticate command. ID_{PICC} = Comp($ehpPK_{PICC}$) <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.

Table 1: Test case ISO7816_K_1

3.7.2 Test case ISO7816_K_2

Test - ID	ISO7816_K_2
Purpose	Test with an invalid certificate reference for the MSE:Set AT command
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <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 > - To generate an invalid certification holder reference, the last character of the holder reference stored inside the IS-Certificate sent in step 4 is changed. 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>’ - <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.
Expected results	1. ’90 00’ in a valid SM response 2. ’90 00’ in a valid SM response 3. ’90 00’ in a valid SM response 4. ’90 00’ in a valid SM response 5. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 6. ‘<Eight bytes of random data> 90 00’ or ISO checking error in an SM response 7. ISO checking error or ‘6300’ in an SM response

3.7.3 Test case ISO7816_K_3

Test - ID	ISO7816_K_3
Version	Deleted in version 0.8 (Identical with ISO7816_L_11)

3.7.4 Test case ISO7816_K_4

Test - ID	ISO7816_K_4
Purpose	Test with a terminal authentication process without secure messaging
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <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.
	`‘00 82 00 00 <Lc> <Terminal generated signature>’`
	- The APDU is sent in plain without SM encoding
	- The signature is 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 as a plain response (without Secure Messaging)

3.7.5 Test case ISO7816_K_5

Test - ID	ISO7816_K_5
Purpose	Test that the effective access rights in a DV-Certificate are ignored
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 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 <L87> 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 AT APDU to the eMRTD.
	`‘0C 22 81 A4 <Lc> 87 <L87> 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 DV-Certificate sent in step 2 has to be used.
	4. Send the given Get Challenge APDU to the eMRTD.
	`‘0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’`
	5. Send the given external authenticate command to the eMRTD.
	`‘0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’`
	• <Cryptogram> contains the encrypted terminal generated signature created with the private key of DV_KEY_01.

Expected results	1. ’90 00’ in an SM response 2. ’90 00’ in an SM response 3. ’90 00’ or ISO checking error in an SM response 4. ‘<Eight bytes of random data> 90 00’ or ISO checking error in an SM response 5. ISO checking error or ‘6300’ in an SM response

3.7.6 Test case ISO7816_K_6

Test - ID	ISO7816_K_6
Purpose	Test that the effective access rights in a CVCA-Certificate are ignored
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 AT APDU to the eMRTD.
	`‘0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	• <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <Certification Holder Reference >
	• The Certification Authority Reference as read from the EF.CVCA file has to be used.
	2. Send the given Get Challenge APDU to the eMRTD.
	`‘0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’`
	3. Send the given external authenticate command to the eMRTD.
	`‘0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’`
	• <Cryptogram> contains the encrypted terminal generated signature created with the private key of CVCA_KEY_00.

Expected results	1. ’90 00’ or ISO checking error in an SM response 2. ‘<Eight bytes of random data> 90 00’ or ISO checking error in an SM response 3. ISO checking error or ‘6300’ in an SM response

3.7.7 Test case ISO7816_K_7

Test - ID	ISO7816_K_7
Purpose	Test the external authenticate command with an invalid class byte
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <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. ‘8C 82 00 00 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ - <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01. - The class byte is set to an invalid value (‘8C’) 8. If the error code in step 7 was returned in a Secure Messaging response, verify that the secure messaging session has not been aborted. If a plain error code was returned, this step is skipped. The Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the session keys derived in step 2 of the preconditions.
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. Note that the behaviour of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. 8. Skipped or ’90 00’ in an SM response

3.7.8 Test case ISO7816_K_8

Test - ID	ISO7816_K_8
Version	Deleted in version 1.1

3.7.9 Test case ISO7816_K_9

Test - ID	ISO7816_K_9
Version	Deleted in version 0.8

3.7.10 Test case ISO7816_K_10

Test - ID	ISO7816_K_10
Purpose	Terminal authentication process with two Get Challenge commands (Using the first challenge)
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <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 a second Get Challenge APDU to the eMRTD. ‘0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’ • If the chip returns a ISO checking error for this second Get Challenge, the remaining steps of this case MUST be skipped. 8. Send the given external authenticate command to the eMRTD. ‘0C 82 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01. • The signature is based on the first challenge received in step 6
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. ‘<Eight bytes of random data> 90 00’ or ISO checking error in an SM response 8. Skipped or ISO checking error or ’63 00’ in an SM response

3.7.11 Test case ISO7816_K_11

Test - ID	ISO7816_K_11
Version	Deleted in version 0.8 (Superseded by ISO7816_K_14)

3.7.12 Test case ISO7816_K_12

Test - ID	ISO7816_K_12
Purpose	Terminal authentication process with short challenge
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 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>
	5. Send the given MSE: Set AT APDU to the eMRTD.
	`‘0C 22 81 A4 <Lc> 87 <L87> 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 07 8E 08 <Checksum> 00’`
	7. If the chip returns a short challenge (only 7 bytes) then send the given external authenticate command to the eMRTD, otherwise skip this step.
	`‘0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’`
	- <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.
	- The signature is based on the short challenge received in step 6

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. ‘<Seven bytes of random data> 90 00’ or ISO checking error in an SM response 7. Skipped, ISO checking error or warning processing ’63 00’ in an SM response

3.7.13 Test case ISO7816_K_13

Test - ID	ISO7816_K_13
Version	Deleted in version 0.8 (Identical with ISO7816_L_11)

3.7.14 Test case ISO7816_K_14

Test - ID	ISO7816_K_14
Purpose	Check the Terminal authentication – No Get Challenge Performed
Version	1.2
Profile	TA, DG3
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <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 external authenticate command to the eMRTD. ‘0C 82 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> `<Le>`’ - <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01. - The wrong signature is calculated without any challenge. 7. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 3 has NOT been granted. ‘0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’

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. ISO checking error or warning processing ’63 00’ in an SM response. 7. ISO checking error in an SM response

3.7.15 Test case ISO7816_K_15

Test - ID	ISO7816_K_15
Purpose	Check the Terminal authentication – No authentication key selection performed
Version	1.2
Profile	TA, DG3
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L$_{7F4E}$> <certificate body> 5F 37 <L$_{5F37}$> <certificate signature> 5. Send the given Get Challenge APDU to the eMRTD.

	‘0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’ 6. Send the given external authenticate command to the eMRTD. ‘0C 82 00 00 <Lc> 87 <L$_{87}$> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ - If the Get Challenge command in step 5 returns a ISO checking error, the remaining steps of this test case are skipped. - <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01. - The signature is based on the challenge received in step 5. 7. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 3 has NOT been granted. ‘0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’
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. ‘<Eight bytes of random data> 90 00’ or ISO checking error in an SM response 6. Skipped, or ISO checking error or warning processing ’63 00’ in an SM response 7. Skipped, or ISO checking error in an SM response

3.7.16 Test case ISO7816_K_16

Test - ID	ISO7816_K_16
Version	Deleted in version 0.8 (Identical with ISO7816_K_2)

3.7.17 Test case ISO7816_K_17

Test - ID	ISO7816_K_17
Purpose	Check the Terminal authentication – Wrong structure in the MSE Set AT command
Version	1.2
Profile	TA, DG3
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <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 84<L_{84}> <Certification Holder Reference > instead of tag 83 • 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>’ • If the Get Challenge command in step 6 returns a ISO checking error, the remaining step of this test case are skipped. • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01. • The signature is based on the challenge received in step 6. 8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 3 has NOT been granted. ‘0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’

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. ISO checking error in an SM response 6. ‘<Eight bytes of random data> 90 00’ or ISO checking error in an SM response 7. Skipped or ISO checking error or warning processing ’63 00’ in an SM response 8. Skipped or ISO checking error in an SM response

3.7.18 Test case ISO7816_K_18

Test - ID	ISO7816_K_18
Purpose	Check the Terminal authentication – Reset of the access rights in case of Application reset
Version	1.2
Profile	TA, DG3
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <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>’` • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01. • The signature is based on the challenge received in step 6. 8. Reset the chip by switching off the field and switching in on again • Perform the “Open ePassport Application”. • Do NOT perform Chip Authentication • Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 3 has NOT been granted. ‘0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’
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 8. ISO checking error in an SM response

3.7.19 Test case ISO7816_K_19

Test - ID	ISO7816_K_19
Purpose	Check the Terminal Authentication – Passive and optionaly Active Authentication between Chip Authentication and Terminal authentication
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 2. The Chip Authentication mechanism MUST have been performed as well. 3. The Passive Authentication MUST have been performed after CA.

	4. If available, DG15 MAY have been read and verified and Active Authentication have been performed after PA. 5. The Certification Authority Reference MUST has 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 <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <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>`’ - <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01. - The signature is based on the challenge received in step 6.

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

3.7.20 Test case ISO7816_K_20

Test - ID	ISO7816_K_20
Purpose	Test the card to perform Terminal Authentication with invalid PACE binding
Version	1.2
Profile	TA, PACE
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 <L87> 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 <L87> 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 <L87> 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 <L87> 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>
	5. Send the given MSE: Set AT APDU to the eMRTD.
	`‘0C 22 81 A4 <Lc> 87 <L87> 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’`
	- Generate a invalid signature, e.g. modify last byte of the signature by adding 0x01.
	- <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 or SW ’63 00’ in an SM response

3.8 Unit ISO7816_L – Effective Access Conditions

This unit tests evaluation of the effective access conditions which has to done by the chip. The chip has to grant access to sensitive data only if the complete terminal authentication mechanism has been performed. Furthermore the access to the specific data groups depends on the access condition flags encoded in the DV and IS certificate.

All test cases of this test unit which require the “Open ePassport Application” procedure MUST be performed twice (one test run with BAC and one with PACE) if the chip supports both protocols. If the chip only supports one of these protocols (BAC or PACE), only one test run has to be performed with the supported protocol used in the “Open ePassport Application” procedure.

3.8.1 Test case ISO7816_L_1

Test - ID	ISO7816_L_1
Purpose	Positive test with a valid terminal authentication process with access permission for DG 3 if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 3.
Version	1.2
Profile	TA, DG3
Preconditions	1. The "Open ePassport Application" procedure MUST have been

	performed. 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 3” chapter as DV_CERT_3. ‘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> - This DV-Certificate grants access to data group 3 and 4. 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 3” chapter as IS_CERT_3a. ‘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> - This IS-Certificate grants only access to data group 3. 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>’ - <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_03. 8. Send the given READ BINARY (with SFI) command to the eMRTD, to

	verify the access to the data group 3 has been granted. `'0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'`
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 8. ‘<data group 3 content data> 90 00’ in an SM response

3.8.2 Test case ISO7816_L_2

Test - ID	ISO7816_L_2
Purpose	Test that data group 4 cannot be accessed if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 3.
Version	1.2
Profile	TA, DG4
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 3” chapter as DV_CERT_3. '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> - This DV-Certificate grants access to data group 3 and 4. 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 3”

	chapter as IS_CERT_3a. ‘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> • This IS-Certificate grants only access to data group 3. 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>’ • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_03. 8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 4 has NOT been granted. ‘0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’
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 8. ISO checking error in an SM response

3.8.3 Test case ISO7816_L_3

Test - ID	ISO7816_L_3
Purpose	Positive test with a valid terminal authentication process with access permission for DG 4 if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 4.
Version	1.2
Profile	TA, DG4
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 3” chapter as DV_CERT_3 ‘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> - This DV-Certificate grants access to data group 3 and 4. 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 3” chapter as IS_CERT _3b. ‘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> - This IS-Certificate grants only access to data group 4. 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>’ - <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_03. 8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 4 has been granted. ‘0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’

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 8. ‘<data group 4 content data> 90 00’ in an SM response

3.8.4 Test case ISO7816_L_4

Test - ID	ISO7816_L_4
Purpose	Test that data group 3 cannot be accessed if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 4.
Version	1.2
Profile	TA, DG3
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 3” chapter as DV_CERT_3 ‘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> - This DV-Certificate grants access to data group 3 and 4. 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 3” chapter as IS_CERT _3b. ‘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> • This IS-Certificate grants only access to data group 4. 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>’ • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_03. 8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 3 has NOT been granted. ‘0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’
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 8. ISO checking error in an SM response

3.8.5 Test case ISO7816_L_5

Test - ID	ISO7816_L_5
Purpose	Positive test with a valid terminal authentication process for DG 3 if the DV certificate grant access to data group 3 only and the IS certificate enable access to both data 3 and 4.
Version	1.2
Profile	TA, DG3
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 4” chapter as DV_CERT_4 ‘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> • This DV-Certificate grants access to data group 3 only. 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 4” chapter as IS_CERT_4. ‘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> • This IS-Certificate grants access to data group 3 and 4. 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>’ • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_04. 8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 3 has been granted. ‘0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’
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 8. ‘<data group 3 content data> 90 00’ in an SM response

3.8.6 Test case ISO7816_L_6

Test - ID	ISO7816_L_6
Purpose	Test that data group 4 cannot be accessed if the DV certificate grant access to data group 3 only and the IS certificate enable access to both data 3 and 4.
Version	1.2
Profile	TA, DG4
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 4” chapter as DV_CERT_4 ‘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> - This DV-Certificate grants access to data group 3 only. 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 4” chapter as IS_CERT_4. ‘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>

	- This IS-Certificate grants access to data group 3 and 4. 5. Send the given MSE: Set AT APDU to the eMRTD. `‘0C 22 81 A4 <Lc> 87 <L87> 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’` - <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_04. 8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 4 has NOT been granted. `‘0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’`
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 8. ISO checking error in an SM response

3.8.7 Test case ISO7816_L_7

Test - ID	ISO7816_L_7
Purpose	Positive test with a valid terminal authentication process for DG 4 if the DV certificate grant access to data group 4 only and the IS certificate enables access to both data 3 and 4.
Version	1.2
Profile	TA, DG4
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 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 5” chapter as DV_CERT_5 ‘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> - This DV-Certificate grants access to data group 4 only. 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 5” chapter as IS_CERT_5. ‘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> - This IS-Certificate grants access to data group 3 and 4. 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>’ - <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_05. 8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 4 has been granted. ‘0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’
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 8. ‘<data group 4 content data> 90 00’ in an SM response

3.8.8 Test case ISO7816_L_8

Test - ID	ISO7816_L_8
Purpose	Test that data group 3 cannot be accessed if the DV certificate grants access to data group 4 only and the IS certificate enables access to both data group 3 and 4.
Version	1.2
Profile	TA, DG3
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 5” chapter as DV_CERT_5 ‘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> - This DV-Certificate grants access to data group 4 only. 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 5” chapter as IS_CERT_5. ‘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> - This IS-Certificate grants access to data group 3 and 4. 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>’ • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_05. 8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 3 has NOT been granted. ‘0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’
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 8. ISO checking error in an SM response

3.8.9 Test case ISO7816_L_9

Test - ID	ISO7816_L_9
Purpose	This test verifies that a successful certificate chain validation without external authenticate does not enable the access to the sensitive data in data group 3.
Version	1.2
Profile	TA, DG3
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 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 <L87> 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>
	5. Send the given MSE: Set AT APDU to the eMRTD.
	`‘0C 22 81 A4 <LC> 87 <L87> 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 READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 3 has NOT been granted.
	`‘0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’`

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

3.8.10 Test case ISO7816_L_10

Test - ID	ISO7816_L_10
Purpose	This test verifies that a successful certificate chain validation without external authenticate does not enable the access to the sensitive data in data group 4
Version	1.2
Profile	TA, DG4
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed.

	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 <L87> 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 <L87> 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 <L87> 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 <L87> 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>
	5. Send the given MSE: Set AT APDU to the eMRTD.
	`‘0C 22 81 A4 <LC> 87 <L87> 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 READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 4 has NOT been granted.
	`‘0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’`

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.

3.8.11 Test case ISO7816_L_11

Test - ID	ISO7816_L_11
Purpose	Test with a failed external authenticate command does not enable the access to the sensitive data in data group 3.
Version	1.2
Profile	TA, DG3
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L$_{7F4E}$> <certificate body> 5F 37 <L$_{5F37}$> <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>’ - <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01. - The last byte of the signature is changed to make it invalid 8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 3 has NOT been granted. ‘0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’
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 or warning processing ’63 00’ in an SM response 8. ISO checking error in an SM response

3.8.12 Test case ISO7816_L_12

Test - ID	ISO7816_L_12
Purpose	Test with a failed external authenticate command does not enable the access to the sensitive data in data group 4.
Version	1.2
Profile	TA, DG4
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L_{7F4E}> <certificate body>
	5F 37 <L_{5F37}> <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>’`
	- <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.
	- The last byte of the signature is changed to make it invalid
	8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the data group 4 has NOT been granted.
	`‘0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’`

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 or warning processing ’63 00’ in an SM response 8. ISO checking error in an SM response

3.8.13 Test case ISO7816_L_13

Test - ID	ISO7816_L_13

Purpose	Test that the chip rejects to fall back to BAC secure messaging after terminal has been authenticated as extended inspection system
Version	1.4
Profile	TA
Preconditions	1. The LDS application MUST have been selected. 2. The BAC mechanism MUST have been performed. 3. The Chip Authentication mechanism MUST have been performed as well. 4. 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 <L87> 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 <L87> 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 <L87> 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 <L87> 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>
	5. Send the given MSE: Set AT APDU to the eMRTD.
	`‘0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the following encrypted data objects
	83 <L83> <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 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’`
	- <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.
	8. Send the given Get Challenge APDU to the eMRTD.

	‘0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’ 9. Send the mutual authenticate command for BAC authentication to the eMRTD. ‘0C 82 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 97 01 28 8E 08 <Checksum> <Le>’ - <Cryptogram> contains the encrypted terminal generated authentication token
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 8. ‘<Eight bytes of random data> 90 00’ or ISO checking error in an SM response 9. If step 8 returned an ISO checking error this step MAY be skipped. Else an ISO checking error in an SM response (chip rejects re-authentication with BAC to maintain the security of the trusted channel after terminal authentication) is expected.

3.8.14 Test case ISO7816_L_14

Test - ID	ISO7816_L_14
Purpose	Test that the chip rejects a second PACE run or reset extended access rights after successful second PACE run.
Version	1.4
Profile	TA, PACE
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. PACE 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 <L87> 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>
	5. Send the given MSE: Set AT APDU to the eMRTD.
	`‘0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the following encrypted data objects
	83 <L83> <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 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’`
	- <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.
	8. Select the MF by sending the given Select APDU to the eMRTD:
	`‘0C A4 00 00 0D 97 01 00 8E 08 <Checksum> 00’`
	9. Under SM, Perform a second run of the “Open ePassport Application” procedure with PACE.
	10. Use new SM keys from second PACE run. Send the READ BINARY (with SFI) command to the eMRTD to verify the access to data group 3 has NOT been granted.
	`‘0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the encrypted terminal generated authentication token

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 8. ’90 00’ in an SM response, or ISO checking error, or ISO checking error in a SM response. If this step returns an ISO checking error the next test steps SHALL be skipped. 9. Successful run of “Open ePassport Application” procedure or ISO checking error. If “Open ePassport Application” procedure fails, the next steps SHALL be skipped. 10. ISO checking error in a SM response (chip MUST reject access to data group 3 since access condition from previous Terminal Authentication MUST be reset)

3.9 Unit ISO7816_M – Update mechanism

This unit contains all test cases which update the chips persistent memory. Therefore these tests can be performed only once with a combination of a distinct sample and set of certificates. To reproduce this test unit, a new set with future certificate dates has to be created or a different test object has to be used.

3.9.1 Test case ISO7816_M_1

Test - ID	ISO7816_M_1
Purpose	Test the “Current Date” update mechanism with a new domestic IS certificate.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 <L87> 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 6” as DV_CERT_6
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	• The DV certificate is marked as a domestic certificate
	3. Send the given MSE: Set DST APDU to the eMRTD.
	`‘0C 22 81 B6 <Lc> 87 <L87> 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 6” as IS_CERT_6a.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	• This certificate has an advanced effective date. Since the DV

	certificate was marked as a domestic one, the chip MUST update the current date.
	- Reset the chip after this step and restore the preconditions for this test case before the next step is performed.
	5. Send the given MSE: Set DST APDU to the eMRTD.
	`‘0C 22 81 B6 <Lc> 87 <L87> 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
	6. Send the appropriate DV-Certificate as specified in the “Certificate Set 6” as DV_CERT_6
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	- The DV certificate is marked as a domestic certificate
	7. Send the given MSE: Set DST APDU to the eMRTD.
	`‘0C 22 81 B6 <Lc> 87 <L87> 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 6 has to be used.
	8. Send the appropriate IS-Certificate as specified in the “Certificate Set 6” as IS_CERT_6b.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	- This certificate has an expiry date BEFORE the effective of the IS certificate used in step 4. Therefore this certificate MUST be rejected.

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. ’90 00’ in an SM response. 7. ’90 00’ in an SM response. 8. ISO checking error or ‘6300’ in an SM response. This certificate MUST no longer be valid, since the current date of the chip has been updated.

3.9.2 Test case ISO7816_M_2

Test - ID	ISO7816_M_2

Purpose	Test the “Current Date” update mechanism with a new DV certificate.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 6” as DV_CERT_6a ‘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> - The DV certificate has an advanced effective data. beyond the expiration date of DV_CERT_6 - Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 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 Authority Reference MUST be used as read from the EF.CVCA file 4. Send the appropriate DV-Certificate as specified in the “Certificate Set 6” as DV_CERT_6. ‘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> - This certificate has an expiration date before the effective date that was set in step 2. Therefore, this certificate SHALL be rejected
Expected results	1. ’90 00’ in an SM response 2. ’90 00’ in an SM response. 3. ’90 00’ in an SM response. 4. ISO checking error or ‘6300’ in an SM response. This certificate MUST no longer be valid, since the current date of the chip has been updated.

3.9.3 Test case ISO7816_M_3

Test - ID	ISO7816_M_3
Purpose	Test the “Trust Point” update mechanism with a new link certificate.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 link certificate as specified in the “Certificate Set 7” as LINK_CERT_7. The ePassport MUST update the trust point with this new certificate. ‘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. Power down the field or remove the passport from the reader, so that the chip looses all temporary information. This is done to prove, that the new trust point has been stored in persistent memory. - Power up the chip - Reestablish the preconditions - Read the EF.CVCA as exactly 36 bytes, using the SELECT and READ BINARY command ‘0C A4 02 0C 15 87 09 01 <Cryptogram> 8E 08 <Checksum> 00’ The cryptogram contains the encrypted fileID of the EF.CVCA file <fid.EF.CVCA>’ ’0C B0 00 00 0D 97 01 24 8E 08 <Checksum> 00’ - Check that EF.CVCA file contains now two trust points and verify that the new trust point is at the first position and the previous one has been moved to the second position. - Any remaining bytes of the EF.CVCA content MUST be filled with ‘00’. 4. 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 the SECOND trust

	point as read from the EF.CVCA file. 5. Send the appropriate DV-Certificate as specified in the “Certificate Set 7” as DV_CERT_7a. ‘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> - Since the previous trust point is still valid, the certificate MUST be verified successfully. - Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 6. 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 the FIRST trust point as read from the EF.CVCA file. 7. Send the appropriate DV-Certificate as specified in the “Certificate Set 7” as DV_CERT_7b. ‘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> - Since the effective date of this certificate is after the expiration date of the original trust point, the chip MUST update the current date and MUST also disable the original trust point. - Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 8. 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> - Use the original Certification Authority Reference (same as in step 4). 9. Send the appropriate DV-Certificate as specified in the “Certificate Set 7” as DV_CERT_7a. ‘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> - Since the trust point has been disabled, the certificate verification MUST fail.
Expected results	1. ’90 00’ in an SM response 2. ’90 00’ in an SM response. 3. true

	4. ’90 00’ in an SM response 5. ’90 00’ in an SM response 6. ’90 00’ in an SM response 7. ’90 00’ in an SM response 8. ’90 00’ or ISO checking error in an SM response 9. ISO checking error or ‘6300’ in an SM response. This certificate MUST no longer be valid, since the current date of the chip has been updated.

3.9.4 Test case ISO7816_M_4

Test - ID	ISO7816_M_4
Purpose	Test the “Trust Point” update mechanism with two link certificates.
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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). 4. This test case can only be done AFTER ISO7816_M_3 has been performed.

Test scenario	1. Send the given MSE: Set DST APDU to the eMRTD.
	`‘0C 22 81 B6 <Lc> 87 <L87> 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 the FIRST trust point as read from the EF.CVCA file.
	2. Send the appropriate link certificate as specified in the “Certificate Set 8” as LINK_CERT_8. The ePassport MUST update the trust point with this new certificate.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	• <Cryptogram> contains the following encrypted data objects
	83 <L$_{83}$> <certificate reference>
	• The Certification Reference MUST be used as specified in the Link certificate used in step 2.
	4. Send the appropriate link certificate as specified in the “Certificate Set 8” as LINK_CERT_9. The ePassport MUST update the trust point with this new certificate.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	5. Send the given MSE: Set DST APDU to the eMRTD.
	`‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
	- <Cryptogram> contains the following encrypted data objects
	83 <L_{83}> <certificate authority reference>
	- The Certification Reference MUST be used as specified in the second Link certificate used in step 4.
	6. Send the appropriate DV-Certificate as specified in the “Certificate Set 8” as DV_CERT_9.
	`‘0C 2A 00 BE <Lc> 87 <L87> 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>
	7. Read the EF.CVCA as exactly 36 bytes, using the SELECT and READ BINARY command
	- `‘0C A4 02 0C 15 87 09 01 <Cryptogram> 8E 08 <Checksum> 00’`
	The cryptogram contains the encrypted fileID of the EF.CVCA file <fid.EF.CVCA>
	- `’0C B0 00 00 0D 97 01 24 8E 08 <Checksum> 00’`
	- Verify the EF.CVCA file that both new trust points are present. The previous trust point from the LINK_CERT_7 MUST be gone.
	- The remaining (three) bytes of the EF.CVCA content MUST be padded with ‘00’.

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. ’90 00’ in an SM response 7. true

3.9.5 Test case ISO7816_M_5

Test - ID	ISO7816_M_5
Purpose	Test the transition CVCA ⇨ CVCA ⇨ IS
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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 (Primary trust point). 2. Send the appropriate CVCA-Certificate as specified in the “Certificate Set 11” chapter as LINK_CERT_11b. ‘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 new CVCA-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 11” chapter as IS_CERT_11c. ‘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>
Expected results	1. ’90 00’ in an SM response 2. ’90 00’ in an SM response 3. ’90 00’ in an SM response 4. ISO checking error or ’63 00’ in an SM response

3.9.6 Test case ISO7816_M_6

Test - ID	ISO7816_M_6
Purpose	Test sanity of the EF.CVCA
Version	1.2
Profile	TA
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed.
Test scenario	1. Send the given SELECT APDU to the eMRTD. ‘0C A4 02 0C 15 87 09 01 <Cryptogram> 8E 08 <Checksum> 00’ • The cryptogram contains the encrypted fileID of the EF.CVCA file <fid.EF.CVCA>’

	2. Send the given READ BINARY APDU to the eMRTD trying to read 36 bytes. `’0C B0 00 00 0D 97 01 24 8E 08 <Checksum> 00’` 3. The EF.CVCA MUST contain two trust points 4. The remaining (six) bytes of the EF.CVCA content MUST be padded with ‘00’ 5. Send another READ BINARY APDU to the MRTD trying to read another byte at offset 36 `’0C B0 00 24 0D 97 01 01 8E 08 <Checksum> 00’`
Expected results	1. ’90 00’ in an SM response 2. Exactly **36** bytes of content data and’90 00’ in an SM response 3. true 4. true 5. ISO checking error in an SM response

3.10 Unit ISO7816_N – Migration policies

This unit covers all tests about the migration policies. This mechanism is used for the import of new CVCA key with new TA algorithm in post issuance phase.

The purpose of this unit is to ensure the migration policy(ies) claimed by the manufacturer can be implemented.

This unit has to be performed once for each possible migration scenario indicated by the passport provider. After the algorithm has been updated, the full test specification has to be repeated based on this new algorithm.

3.10.1 Test case ISO7816_N_1

Test - ID	ISO7816_N_1
Purpose	Test mechanism migration according to the manufacturer’s implementation statement.
Version	1.2
Profile	TA, MIG
Preconditions	1. The "Open ePassport Application" procedure MUST have been performed. 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). 4. This test case can only be done AFTER ISO7816_M_5 has been performed.
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 the FIRST trust point as read from the EF.CVCA file.

	2. Send the appropriate link certificate with the updated mechanism as defined in “Certificate Set 13” as LINK_CERT_13. The ePassport MUST update the trust point with this new certificate. ‘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 reference> - The Certification Reference MUST be used as specified in the Link certificate used in step 2. - The chip MUST be able to use the updated cryptographic algorithms as introduced by the link certificate in step 2. 4. Send the appropriate DV certificate as specified in the “Certificate Set 13” as.DV_CERT_13. ‘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> 5. 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 Reference MUST be used as specified in the DV certifcate used in step 4. 6. Send the appropriate IS-Certificate as specified in the “Certificate Set 13” as IS_CERT_13 ‘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>
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. ’90 00’ in an SM response

4 Tests for layer 7 (LDS)

4.1 Unit LDS_E – Data group 14

This unit covers all tests about the coding of the data group 14 containing the public key information required for the chip authentication mechanism.

If the data group 14 contains multiple instances of the same element type (ChipAuthentication, ChipAuthenticationPublicKeyInfo, TerminalAuthenticationInfo), the corresponding test cases have to be performed for each element. A test case is only rated as a PASS if all passes of a test case are performed without any failure, so that all test runs for one test case lead to a single result.

4.1.1 Test case LDS_E_1

Test - ID	LDS_E_1
Purpose	Test the LDS tag of the data group 14 object
Version	0.6
Profile	CA_KAT, CA_ATGA
Preconditions	1. Data group 14 MUST have been read from the eMRTD
Test scenario	1. Verify the hex value of the very first byte of the data group 14 content. It MUST contain the LDS tag for this data group. 2. The tag is followed by an ASN.1 style encoded length of the data group 14 object. This length MUST be encoded correctly according to the ASN.1 specification. 3. The encoded length MUST NOT exceed the overall length of the read to group object.
Expected results	1. ’6E’ 2. true 3. true

4.1.2 Test case LDS_E_2

Test - ID	LDS_E_2
Purpose	Test the ASN.1 encoding of the ChipAuthenticationPublicKeyInfos
Version	1.11
Profile	CA_KAT, CA_ATGA
Preconditions	1. Data group 14 MUST have been read from the eMRTD
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 at least one ChipAuthenticationPublicKeyInfo element with one of the protocol OID defined in the EAC specification (id-PK-DH or id-PK-ECDH). The test LDS_E_3 MUST be performed for each ChipAuthenticationPublicKeyInfo element which has such an OID. 3. If at least one ChipAuthenticationInfo element (with 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) is present, there MUST be at least one ChipAuthenticationInfo element with the version element set to 1. 4. If at least one TerminalAuthenticationInfo element (with OID id-TA) is present, there MUST be at least one TerminalAuthenticationInfo element (with OID id-TA) with the version element set to 1. 5. There MUST be no SecurityInfo element specifying a specific TA protocol like id-TA-RSA. Only the generic identifier id-TA MUST be used inside the data group 14 security info.
Expected results	1. true 2. true 3. true 4. true 5. true

4.1.3 Test case LDS_E_3

Test - ID	LDS_E_3
Purpose	Test the ASN.1 encoding of the ChipAuthenticationPublicKeyInfo
Version	1.12
Profile	CA_KAT, CA_ATGA
Preconditions	1. Data group 14 MUST have been read from the eMRTD 2. The data group 14 is parsed and this test is repeated for each ChipAuthenticationPublicKeyInfo element containing the OID (id-PK-DH or id-PK-ECDH) as defined in the EAC specification (see LDS_E_2).
Test scenario	1. The ChipAuthenticationPublicKeyInfo element must follow the ASN.1 syntax definition in the EAC specification [R2] and [R11]. 2. The presence of the key reference in the ChipAuthenticationPublicKeyInfo MUST be coherent with the ICS 3. The algorithm identifier MUST match to the Key agreement protocol and be one of the following: • DHKeyAgreement (OID: 1.2.840.113549.1.3.1) • ecPublicKey (OID: 1.2.840.10045.2.1) 4. The parameters MUST follow PKCS #3 (DH) or KAEG specification (ECDH). For DH verify that • $0 < g < p$, that is both should be positive and g should be less than p. • If private value length l is present, verify that $l > 0$ and $2^{l-1} < p$. In case of ECDH verify that

	- prime $p > 2$ - curve parameter $0 \leq a < p$ - curve parameter $0 \leq b < p$ - $4a^3 + 27b^2 \neq 0$ - base point G is on the curve, with both coordinates in range $0 \dots p - 1$ - Cofactor $f > 0$ - order r of base point $r > 0$, $r \neq p$ - $r * f \leq 2p$ 5. The public key value MUST follow PKCS#3 (DH) or BSI TR03111 specification (ECDH) For DH verify that - $0 < y < p$ For ECDH verify that - public point Y is on the curve, with both coordinates in range $0 \dots p - 1$
Expected results	1. true 2. true 3. true 4. true 5. true

4.1.4 Test case LDS_E_4

Test - ID	LDS_E_4
Purpose	Test the ASN.1 encoding of the ChipAuthenticationInfo
Version	1.11
Profile	CA_KAT, CA_ATGA
Preconditions	1. Data group 14 MUST have been read from the eMRTD 2. The data group 14 is parsed and this test is repeated for each ChipAuthenticationInfo element containing the OID (CA-DH-3DES-CBC-CBC or CA-ECDH-3DES-CBC-CBC) as defined in the EAC specification (see LDS_E_2) and the version element set to 1.
Test scenario	1. The ChipAuthenticationInfo element must follow the ASN.1 syntax definition in the EAC specification [R2] and [R11]. 2. The presence of the key reference in the ChipAuthenticationInfo MUST be coherent with the ICS 3. If the key reference is present in the ChipAuthenticationInfo element, there MUST be also on ChipAuthenticationPublicKeyInfo element with this key reference.
Expected results	1. true 2. true 3. true

4.1.5 Test case LDS_E_5

Test - ID	LDS_E_5
Purpose	Test the ASN.1 encoding of the TerminalAuthenticationInfo
Version	1.11
Profile	CA_KAT, CA_ATGA
Preconditions	1. Data group 14 MUST have been read from the eMRTD 2. The data group 14 is parsed and this test is repeated for each TerminalAuthenticationInfo element containing the OID id-TA as defined in the EAC specification (see LDS_E_2) and the version element set to 1.
Test scenario	1. The TerminalAuthenticationInfo element must follow the ASN.1 syntax definition in the EAC specification [R2] and [R11]. 2. If the fileID element is present, it MUST be encoded as a OCTET STRING, not as an INTEGER 3. If the fileID element is present and if it contains a sfid element, it MUST be encoded as a OCTET STRING, not as an INTEGER.
Expected results	1. true 2. true 3. true

4.2 Unit LDS_F – EF.CVCA

This unit covers all tests about the coding of the EF.CVCA file containing the trust point for the certificate verification process.

4.2.1 Test case LDS_F_1

Test - ID	LDS_F_1
Purpose	Test the content of the EF.CVCA file
Version	1.11
Profile	TA
Preconditions	1. The EF.CVCA file MUST have been read from the eMRTD
Test scenario	1. The size of the EF.CVCA file MUST be exactly 36 bytes. 2. The EF.CVCA file MUST contain at least one at most two Certificate Authority Reference objects. 3. Each object MUST start with the tag ‘42’ 4. The encoded object length of each object MUST NOT exceed 16 bytes. 5. Any remaining bytes of the EF.CVCA content MUST be padded with ‘00’.
Expected results	1. true 2. true 3. true 4. true 5. true

4.3 Unit LDS_G – Data group 3

This unit includes all test cases concerning the DG 3 element (fingerprint). As the purpose of this test specification is not to test biometrics, only the general DG3 header (as defined in [R1]) is tested to ensure minimum conformance.

Test cases LDS_G_05 to LDS_G_10 MUST are repeated for each instance of Biometric Information Template present in the DG3.

A test case is only rated as a PASS if all passes of a test case are performed without any failure, so that all test runs for one test case lead to a single result.

4.3.1 Test case LDS_G_1

Test - ID	LDS_G_1
Purpose	This test checks the template tag; the encoded DG 3 element starts with.
Version	0.6
Profile	DG3
Preconditions	1. Encoded EF.DG3 object in binary format as read from the eMRTD.
Test scenario	1. Check the very first byte of the EF.DG3 element
Expected results	1. First byte MUST be ‘63’

4.3.2 Test case LDS_G_2

Test - ID	LDS_G_2
Purpose	This test checks the encoding of DG3 length bytes.
Version	0.6
Profile	DG3
Preconditions	1. Encoded EF.DG3 object in binary format as read from the eMRTD.
Test scenario	1. Analyze the encoding of the bytes that follow the template tag 2. Verify the length of the DG3
Expected results	1. The bytes that follow the template tag MUST contain a valid length encoding (According to ASN.1 encoding rules). 2. The encoded length MUST match the size of the DG3 value bytes.

4.3.3 Test case LDS_G_3

Test - ID	LDS_G_3
Purpose	This test checks the encoding of the Biometric Information Group Template (BIGT).
Version	1.12
Profile	DG3
Preconditions	1. Encoded EF.DG3 object in binary format as read from the eMRTD.
Test scenario	1. Check that the first tag in the DG 3 value is the BIGT tag.

	2. Verify the length of the BIGT . 3. Verify that the BIGT is the only information in the DG3.
Expected results	1. Tag MUST be ‘7F 61’. 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The encoded length MUST match the number of remaining bytes of the DG 3 data element, except if the BIGT contains no BITs (no fingerprints). In this case the BIGT MAY be followed by a DO 53 containing random data to prevent the static hash value.

4.3.4 Test case LDS_G_4

Test - ID	LDS_G_4
Purpose	This test checks the encoding of the number of instances stored in the Biometric Information Group Template (BIGT).
Version	0.6
Profile	DG3
Preconditions	1. Encoded EF.DG3 object in binary format as read from the eMRTD.
Test scenario	1. Check the first tag inside the BIGT. 2. Verify the length of the “number of instances” data object. 3. Verify the value of the “number of instances” data object.
Expected results	1. Tag MUST be ‘02’. 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The number of instances MUST match the actual number of encoded Biometric Information Templates (tag 7F 60).

4.3.5 Test case LDS_G_5

Test - ID	LDS_G_5
Purpose	This test checks the encoding of the Biometric Information Template (BIT).
Version	0.6
Profile	DG3
Preconditions	1. Encoded EF.DG3 object in binary format as read from the eMRTD. 2. This test MUST be repeated for each instance of BIT
Test scenario	1. Check the tag of the BIT. 2. Verify the length of the BIT data object. 3. Verify that the encoded length match the size of the BIT.
Expected results	1. Tag MUST be ‘7F 60’. 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The encoded length MUST match the effective length of the encoded BIT

4.3.6 Test case LDS_G_6

Test - ID	LDS_G_6

Purpose	This test checks the encoding of the Biometric Header Template (BHT).
Version	0.6
Profile	DG3
Preconditions	1. Encoded EF.DG3 object in binary format as read from the eMRTD. 2. This test MUST be repeated for each instance of BIT
Test scenario	1. Check the tag of the BHT 2. Verify the length of the BHT data object. 3. Verify that the encoded length match the size of the BHT.
Expected results	1. Tag MUST be ‘A1’. 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The encoded length MUST match the effective length of the encoded BHT

4.3.7 Test case LDS_G_7

Test - ID	LDS_G_7
Purpose	This test checks the presence/encoding of the CBEFF element "format owner".
Version	1.1
Profile	DG3
Preconditions	1. Encoded EF.DG3 object in binary format as read from the eMRTD. 2. The tested CBEFF element is part of the BHT located in LDS_G_06. 3. This test MUST be repeated for each instance of BIT
Test scenario	1. Check the presence of the “format owner” tag. 2. Verify the length of the “format owner” data object. 3. Check the length of the “format owner” value. 4. Verify the “format owner” value.
Expected results	1. Tag MUST be ‘87’. 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The length of the value field MUST be 2 bytes. 4. The value of the format owner MUST be a registered CBEFF owner. It MUST be ‘01 01’ for the first instance of BIT. All registered format owner can be found at www.ibia.org.

4.3.8 Test case LDS_G_8

Test - ID	LDS_G_8
Purpose	This test checks the presence/encoding of the CBEFF element "format type".
Version	1.1
Profile	DG3
Preconditions	1. Encoded EF.DG3 object in binary format as read from the eMRTD. 2. The tested CBEFF element is part of biometric header template located in LDS_G_06. 3. This test MUST be repeated for each instance of BIT
Test scenario	1. Check the presence of the “format type” tag. 2. Verify the length of the “format type” data object. 3. Check the length of the “format type” value.

	4. Verify the “format type” value.
Expected results	1. Tag MUST be ‘88’. 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The length of the value field MUST be 2 bytes. 4. The value of the format type MUST be a registered CBEFF type. It MUST be ‘0007’ for the first instance of BIT. All registered format types can be found at www.ibia.org.

4.3.9 Test case LDS_G_9

Test - ID	LDS_G_9
Purpose	This test checks the presence/encoding of the CBEFF element "biometric subtype".
Version	1.1
Profile	DG3
Preconditions	1. Encoded EF.DG3 object in binary format as read from the eMRTD. 2. The tested CBEFF element is part of biometric header template located in LDS_G_06. 3. This test MUST be repeated for each instance of BIT
Test scenario	1. Check the presence of the “biometric subtype” tag. 2. Verify the length of the “biometric subtype” data object. 3. Check the length of the “biometric subtype” value. 4. Verify the “biometric subtype” value.
Expected results	1. Tag MUST be ‘82’. 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The length of the value field MUST be 1 byte. 4. The value of the format type MUST be a registered CBEFF biometric subtype. The values for the biometric subtype are defined in ISO 19785-3.

4.3.10 Test case LDS_G_10

Test - ID	LDS_G_10
Purpose	This test checks the encoding of the Biometric Data Block (BDB) tag.
Version	0.6
Profile	DG3
Preconditions	1. Encoded EF.DG3 object in binary format as read from the eMRTD. 2. The BDB is part of the biometric information template tested in LDS_G_05. 3. This test MUST be repeated for each instance of BIT
Test scenario	1. Check the presence of the BDB tag. 2. Verify the length of the BDB. 3. Verify that the encoded length match the size of encoded BDB
Expected results	1. Tag MUST be ‘5F 2E’ or ‘7F 2E’ 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The encoded length MUST match the effective length of the encoded BDB

4.3.11 Test case LDS_G_11

Test - ID	LDS_G_11
Purpose	This test verifies the consistency between the CBEFF format type and the BDB format identifier of the BIT
Version	0.8
Profile	DG3
Preconditions	• Encoded EF.DG3 object in binary format as read from the eMRTD. • The BDB is part of the biometric information template tested in LDS_G_05. • This test MUST be repeated for each instance of BIT”
Test scenario	1. Check the first four bytes of the BDB
Expected results	1. The value MUST be ’46 49 52 00’ (‘F’ ‘I’ ‘R’ 0x0).

4.4 Unit LDS_H – Data group 4

This unit includes all test cases concerning the DG 4 element (Iris). As the purpose of this test specification is not to test biometrics, only the general DG4 header (as defined in [R1]) is tested to ensure minimum conformance.

Test cases LDS_H_5 to LDS_H_10 MUST are repeated for each instance of Biometric Information Template present in the DG4.

A test case is only rated as a PASS if all passes of a test case are performed without any failure, so that all test runs for one test case lead to a single result.

4.4.1 Test case LDS_H_1

Test - ID	LDS_H_1
Purpose	This test checks the template tag; the encoded DG 4 element starts with.
Version	0.6
Profile	DG4
Preconditions	Encoded EF.DG4 object in binary format as read from the eMRTD.
Test scenario	1. Check the very first byte of the EF.DG4 element
Expected results	1. First byte MUST be ‘76’

4.4.2 Test case LDS_H_2

Test - ID	LDS_H_2
Purpose	This test checks the encoding of DG4 length bytes.
Version	0.6
Profile	DG4
Preconditions	Encoded EF.DG4 object in binary format as read from the eMRTD.
Test scenario	1. Analyze the encoding of the bytes that follow the template tag 2. Verify the length of the DG4
Expected results	1. The bytes that follow the template tag MUST contain a valid length encoding (According to ASN.1 encoding rules).

	2. The encoded length MUST match the size of the DG4 value bytes

4.4.3 Test case LDS_H_3

Test - ID	LDS_H_3
Purpose	This test checks the encoding of the Biometric Information Group Template (BIGT).
Version	1.12
Profile	DG4
Preconditions	Encoded EF.DG4 object in binary format as read from the eMRTD.
Test scenario	1. Check that the first tag in the DG 4 value is the BIGT tag. 2. Verify the length of the BIGT. 3. Verify that the BIGT is the only information in the DG 4.
Expected results	1. Tag MUST be '7F 61'. 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The encoded length MUST match the number of remaining bytes of the DG 4 data element, except if the BIGT contains no BITs (no iris images). In this case the BIGT MAY be followed by a DO 53 containing random data to prevent the static hash value.

4.4.4 Test case LDS_H_4

Test - ID	LDS_H_4
Purpose	This test checks the encoding of the number of instances stored in the Biometric Information Group Template (BIGT).
Version	0.6
Profile	DG4
Preconditions	Encoded EF.DG4 object in binary format as read from the eMRTD.
Test scenario	1. Check the first tag inside the BIGT. 2. Verify the length of the "number of instances" data object. 3. Verify the value of the "number of instances" data object.
Expected results	1. Tag MUST be '02'. 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The number of instances MUST match the actual number of encoded Biometrics Information Templates (tag 7F 60).

4.4.5 Test case LDS_H_5

Test - ID	LDS_H_5
Purpose	This test checks the encoding of the Biometric Information Template (BIT).
Version	0.6
Profile	DG4
Preconditions	- Encoded EF.DG4 object in binary format as read from the eMRTD - This test MUST be repeated for each instance of BIT

Test scenario	1. Check the tag of the BIT. 2. Verify the length of the BIT data object. 3. Verify that the encoded length match the effective size of the BIT.
Expected results	1. Tag MUST be ‘7F 60’. 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The encoded length MUST match the length of the encoded BIT

4.4.6 Test case LDS_H_6

Test - ID	LDS_H_6
Purpose	This test checks the encoding of the Biometric Header Template (BHT).
Version	0.6
Profile	DG4
Preconditions	• Encoded EF.DG4 object in binary format as read from the eMRTD. • This test MUST be repeated for each instance of BIT
Test scenario	1. Check the tag of the BHT. 2. Verify the length of the BHT data object. 3. Verify that the encoded length match the size of the BHT
Expected results	1. Tag MUST be ‘A1’. 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The encoded length MUST match the effective length of the encoded BHT

4.4.7 Test case LDS_H_7

Test - ID	LDS_H_7
Purpose	This test checks the presence/encoding of the CBEFF element "format owner".
Version	1.1
Profile	DG4
Preconditions	• Encoded EF.DG4 object in binary format as read from the eMRTD. • The tested CBEFF element is part of biometric header template located in LDS_H_06. • This test MUST be repeated for each instance of BIT
Test scenario	1. Check the presence of the “format owner” tag. 2. Verify the length of the “format owner” data object. 3. Check the length of the “format owner” value. 4. Verify the “format owner” value.
Expected results	1. Tag MUST be ‘87’. 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The length of the value field MUST be 2 bytes. 4. The value of the format owner MUST be a registered CBEFF owner. It MUST be ‘01 01’ for the first instance of BIT. All registered format owner can be found at www.ibia.org.

4.4.8 Test case LDS_H_8

Test - ID	LDS_H_8
Purpose	This test checks the presence/encoding of the CBEFF element "format type".
Version	1.1
Profile	DG4
Preconditions	• Encoded EF.DG4 object in binary format as read from the eMRTD. • The tested CBEFF element is part of biometric header template located in LDS_H_06. • This test MUST be repeated for each instance of BIT
Test scenario	1. Check the presence of the “format type” tag. 2. Verify the length of the “format type” data object. 3. Check the length of the “format type” value. 4. Verify the “format type” value.
Expected results	1. Tag MUST be ‘88’. 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The length of the value field MUST be 2 bytes. 4. The value of the format type MUST be a registered CBEFF type. It MUST be ‘0009’ or ‘000B’ for the first instance of BIT. All registered format types can be found at www.ibia.org.

4.4.9 Test case LDS_H_9

Test - ID	LDS_H_9
Purpose	This test checks the presence/encoding of the CBEFF element "biometric subtype". Note that the biometric subtype element is optional for data group 4. Therefore this test case is only performed if the biometric subtype element is present.
Version	1.1
Profile	DG4
Preconditions	• Encoded EF.DG4 object in binary format as read from the eMRTD. • The tested CBEFF element is part of biometric header template located in LDS_H_06. • This test MUST be repeated for each instance of BIT
Test scenario	1. Check the presence of the “biometric subtype” tag. 2. Verify the length of the “biometric subtype” data object. 3. Check the length of the “biometric subtype” value. 4. Verify the “biometric subtype” value.
Expected results	1. Tag MUST be ‘82’. 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The length of the value field MUST be 1 byte. 4. The value of the format type MUST be a registered CBEFF biometric subtype. The values for the biometric subtype are defined in ISO 19785-3.

4.4.10 Test case LDS_H_10

Test - ID	LDS_H_10
Purpose	This test checks the encoding of the Biometric Data Block (BDB) tag.
Version	0.6
Profile	DG4
Preconditions	• Encoded EF.DG4 object in binary format as read from the eMRTD. • The BDB is part of the biometric information template tested in LDS_H_05. • This test MUST be repeated for each instance of BIT
Test scenario	1. Check the presence of the BDB tag. 2. Verify the length of the BDB. 3. Verify that the encoded length match the size of encoded BDB
Expected results	1. Tag MUST be ‘5F 2E’ or ‘7F 2E’ 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The encoded length MUST match the effective length of the encoded BDB

4.4.11 Test case LDS_H_11

Test - ID	LDS_H_11
Purpose	This test verifies the consistency between the CBEFF format type and the BDB format identifier of the BIT
Version	1.0
Profile	DG4
Preconditions	• Encoded EF.DG4 object in binary format as read from the eMRTD. • The BDB is part of the biometric information template tested in LDS_H_05. • This test MUST be repeated for each instance of BIT”
Test scenario	1. Check the first four bytes of the BDB
Expected results	1. The value MUST be ’49 49 52 00’ ('I' 'I' 'R' 0x00).

Annex A Implementation conformance statement

In order to set up the tests properly, an applicant SHALL provide the information specified in this annex. Some tests defined in this document are depending on the supported functionality of the passport. The test results will only cover the function declared in this statement.

A.1 Supported profiles

Tests which require functions not supported by the provided ePassport will be skipped during the tests. Please specify the profiles supported by the provided sample. For details on the profiles please refer to section 2.2.

Table 2: Supported profiles

Profile	**Applicant declaration**
Password Authenticated Connection Establishment	
Chip Authentication	
Chip Authentication with MSE:Set AT & General Authenticate for 3DES algorithm support	
Diffie-Hellman	
Elliptic Curve Diffie-Hellman	
Explicit key selection supported	
Invalid key ID for explicit key selection (required for Test case ISO7816_I_14 and Test case ISO7816_II_13 of explicit key selection is supported)	
Terminal Authentication	
ECDSA algorithm	
RSA algorithm	
Migration of the crypto system	
Certificate date validation	
For Terminal Authentication based on ECDSA algorithm, include domain parameter in link certificate (LINK_CERT_7, LINK_CERT_8, LINK_CERT_9, LINK_CERT_11)	
Command APDU to send to the eMRTD to verify the chip's ability to still require Secured Messaging. If not provided `'00 B0 81 00 00'` will be used. This command has to be send as SM protected command.	

A.2 Supported cryptographic algorithm

The applicant of the passport under test SHALL declare the cryptosystem (signature algorithm and hash algorithm) used to perform the Terminal Authentication.

Table 3: Supported cryptographic algorithm

Signature algorithm	**Key size (incl. curve name for ECDSA)**	**Hash algorithm**

A.3 Cryptosystem migration policy

If the eMRTD under test supports the migration to another cryptosystem, the applicant SHALL provide the list of supported target(s) cryptosystem(s) (signature algorithm and hash algorithm).

Note: For each target algorithm specified in this table, the test unit ISO7816_N has to be performed. Afterward, the fully test set has to be repeated for each new algorithm.

Table 4: Targets cryptosystems table

Signature algorithm	Key size (incl. curve name for ECDSA)	Hash algorithm

A.4 CVCA trust point information

For the preparation of the certificate sets defined in 2.4, the applicant has to provide some information about the current trust point stored inside the ePassport EF.CVCA file. Alternatively the application can provide a CVCA certificate containing these information.

Table 5: Trust point information

Information	Applicant declaration (value)
Primary trust point CAR	
Primary trust point “Effective date”	
Primary trust point “Expiration date” Note that for the test scenarios covered by this test plan the time span between “Effective date” and “Expiration date” must be at least 2 month, otherwise some tests will fail.	