

MACHINE READABLE TRAVEL DOCUMENTS



TECHNICAL REPORT

RF PROTOCOL AND APPLICATION TEST STANDARD FOR E-PASSPORT - PART 3

TESTS FOR APPLICATION PROTOCOL AND LOGICAL DATA STRUCTURE

Version: **0.9**

Date – Mar 17, 2006

Published by authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION

File	: WG3TF4_SDXX_RF_protocol_and_application_test_standard_ePP_Part_3.doc
Author	: ISO/JTC1/SC17/WG3/TF4 for ICAO-NTWG

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

Release Control

Release	Date	Description
0.1	23-11-2005	First draft based on the German WG3 TF4 contribution "e-Passport Conformity Testing" version 1.02 presented at TF4 meeting in Paris Nov 21-23, 2005
0.2	21-12-2005	Updated version with new ICAO TR layout.
0.9	17-03-2006	Changes according to resolved comments from the WG3 TF4 meeting in Ottawa, Jan 30 – Feb 02, 2006. The following major changes have been introduced: <ul style="list-style-type: none">• Less restrictive verification of status words• Introduction of profiles to be tested

Release Note:

Release 2006-03-17 is the second working draft of the technical report issued to the SC17 WG3 TF4 for final comments until April 14th, 2006.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

Table of contents

1	INTRODUCTION.....	7
1.1	SCOPE AND PURPOSE.....	7
1.2	ASSUMPTIONS	7
1.3	BUILD-UP OF THE TEST PLAN	7
1.4	TERMINOLOGY.....	7
1.5	GLOSSARY	8
1.6	ABBREVIATIONS.....	8
1.7	REFERENCE DOCUMENTATION	9
2	GENERAL TEST REQUIREMENTS	10
2.1	TEST SETUP	10
2.2	IMPLEMENTATION CONFORMANCE STATEMENT	10
2.3	VERIFICATION OF ISO 7816-4 STATUS WORDS.....	11
3	SECURITY AND COMMAND TESTS.....	12
3.1	UNIT TEST ISO_7816_A – SELECTAPPLICATION COMMAND.....	12
3.1.1	Test Case 7816_A_1	12
3.1.2	Test Case 7816_A_2	12
3.2	UNIT TEST ISO_7816_B – SECURITY CONDITIONS OF A BAC PROTECTED E-PASSPORT	13
3.2.1	Test Case 7816_B_1	13
3.2.2	Test Case 7816_B_2	13
3.2.3	Test Case 7816_B_3.....	13
3.2.4	Test Case 7816_B_4.....	14
3.2.5	Test Case 7816_B_5.....	14
3.2.6	Test Case 7816_B_6.....	14
3.2.7	Test Case 7816_B_7.....	14
3.2.8	Test Case 7816_B_8.....	15
3.2.9	Test Case 7816_B_9.....	15
3.2.10	Test Case 7816_B_10.....	15
3.2.11	Test Case 7816_B_11.....	16
3.2.12	Test Case 7816_B_12.....	16
3.2.13	Test Case 7816_B_13.....	16
3.2.14	Test Case 7816_B_14.....	16
3.2.15	Test Case 7816_B_15.....	17
3.2.16	Test Case 7816_B_16.....	17
3.2.17	Test Case 7816_B_17.....	17
3.2.18	Test Case 7816_B_18.....	17
3.2.19	Test Case 7816_B_19.....	18
3.2.20	Test Case 7816_B_20.....	18
3.2.21	Test Case 7816_B_21.....	18
3.2.22	Test Case 7816_B_22.....	19
3.2.23	Test Case 7816_B_23.....	19
3.2.24	Test Case 7816_B_24.....	19
3.2.25	Test Case 7816_B_25.....	19
3.2.26	Test Case 7816_B_26.....	20
3.2.27	Test Case 7816_B_27.....	20
3.2.28	Test Case 7816_B_28.....	20
3.2.29	Test Case 7816_B_29.....	21
3.2.30	Test Case 7816_B_30.....	21
3.2.31	Test Case 7816_B_31.....	21
3.2.32	Test Case 7816_B_32.....	21
3.2.33	Test Case 7816_B_33.....	22
3.2.34	Test Case 7816_B_34.....	22
3.2.35	Test Case 7816_B_35.....	22
3.2.36	Test Case 7816_B_36.....	23
3.3	UNIT TEST ISO_7816_C – BASIC ACCESS CONTROL.....	23
3.3.1	Test Case 7816_C_1	23
3.3.2	Test Case 7816_C_2	23

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

3.3.3	Test Case 7816_C_3.....	24
3.3.4	Test Case 7816_C_4.....	24
3.3.5	Test Case 7816_C_5.....	24
3.3.6	Test Case 7816_C_6.....	25
3.3.7	Test Case 7816_C_7.....	26
3.3.8	Test Case 7816_C_8.....	26
3.3.9	Test Case 7816_C_9.....	26
3.3.10	Test Case 7816_C_10.....	27
3.3.11	Test Case 7816_C_11.....	27
3.3.12	Test Case 7816_C_12.....	28
3.3.13	Test Case 7816_C_13.....	29
3.3.14	Test Case 7816_C_14.....	29
3.3.15	Test Case 7816_C_15.....	29
3.3.16	Test Case 7816_C_16.....	30
3.3.17	Test Case 7816_C_17.....	30
3.3.18	Test Case 7816_C_18.....	30
3.3.19	Test Case 7816_C_19.....	31
3.3.20	Test Case 7816_C_20.....	31
3.3.21	Test Case 7816_C_21.....	31
3.3.22	Test Case 7816_C_22.....	32
3.3.23	Test Case 7816_C_23.....	32
3.3.24	Test Case 7816_C_24.....	32
3.3.25	Test Case 7816_C_25.....	33
3.3.26	Test Case 7816_C_26.....	33
3.3.27	Test Case 7816_C_27.....	33
3.3.28	Test Case 7816_C_28.....	34
3.3.29	Test Case 7816_C_29.....	34
3.3.30	Test Case 7816_C_30.....	34
3.3.31	Test Case 7816_C_31.....	35
3.3.32	Test Case 7816_C_32.....	35
3.3.33	Test Case 7816_C_33.....	35
3.3.34	Test Case 7816_C_34.....	36
3.3.35	Test Case 7816_C_35.....	36
3.3.36	Test Case 7816_C_36.....	36
3.3.37	Test Case 7816_C_37.....	37
3.4	UNIT TEST ISO_7816_D – SELECTFILE COMMAND.....	37
3.4.1	Test Case 7816_D_1.....	37
3.4.2	Test Case 7816_D_2.....	37
3.4.3	Test Case 7816_D_3.....	38
3.4.4	Test Case 7816_D_4.....	38
3.4.5	Test Case 7816_D_5.....	38
3.4.6	Test Case 7816_D_6.....	38
3.4.7	Test Case 7816_D_7.....	39
3.4.8	Test Case 7816_D_8.....	39
3.4.9	Test Case 7816_D_9.....	39
3.4.10	Test Case 7816_D_10.....	39
3.4.11	Test Case 7816_D_11.....	40
3.4.12	Test Case 7816_D_12.....	40
3.4.13	Test Case 7816_D_13.....	40
3.4.14	Test Case 7816_D_14.....	40
3.4.15	Test Case 7816_D_15.....	41
3.4.16	Test Case 7816_D_16.....	41
3.4.17	Test Case 7816_D_17.....	41
3.4.18	Test Case 7816_D_18.....	41
3.4.19	Test Case 7816_D_19.....	42
3.4.20	Test Case 7816_D_20.....	42
3.4.21	Test Case 7816_D_21.....	42
3.4.22	Test Case 7816_D_22.....	42
3.4.23	Test Case 7816_D_23.....	43
3.5	UNIT TEST ISO_7816_E – READBINARY COMMAND.....	43

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

3.5.1	Test Case 7816_E_1	43
3.5.2	Test Case 7816_E_2	44
3.5.3	Test Case 7816_E_3	44
3.5.4	Test Case 7816_E_4	44
3.5.5	Test Case 7816_E_5	45
3.5.6	Test Case 7816_E_6	45
3.5.7	Test Case 7816_E_7	45
3.5.8	Test Case 7816_E_8	46
3.5.9	Test Case 7816_E_9	46
3.5.10	Test Case 7816_E_10	46
3.5.11	Test Case 7816_E_11	46
3.5.12	Test Case 7816_E_12	47
3.5.13	Test Case 7816_E_13	47
3.5.14	Test Case 7816_E_14	47
3.5.15	Test Case 7816_E_15	47
3.5.16	Test Case 7816_E_16	48
3.5.17	Test Case 7816_E_17	48
3.5.18	Test Case 7816_E_18	48
3.5.19	Test Case 7816_E_19	49
3.5.20	Test Case 7816_E_20	49
3.5.21	Test Case 7816_E_21	49
3.5.22	Test Case 7816_E_22	50
4	LOGICAL DATA STRUCTURE TESTS.....	51
4.1	UNIT TEST LDS_A - TESTS FOR THE EF.COM LDS OBJECT	51
4.1.1	Test Case LDS_A_01	51
4.1.2	Test Case LDS_A_02	51
4.1.3	Test Case LDS_A_03	51
4.1.4	Test Case LDS_A_04	52
4.1.5	Test Case LDS_A_05	52
4.2	UNIT TEST LDS_B - TESTS FOR THE DATAGROUP 1 LDS OBJECT	52
4.2.1	Test Case LDS_B_01	52
4.2.2	Test Case LDS_B_02	53
4.2.3	Test Case LDS_B_03	53
4.2.4	Test Case LDS_B_04	53
4.2.5	Test Case LDS_B_05	54
4.2.6	Test Case LDS_B_06	54
4.2.7	Test Case LDS_B_07	54
4.2.8	Test Case LDS_B_08	55
4.2.9	Test Case LDS_B_09	55
4.2.10	Test Case LDS_B_10	55
4.2.11	Test Case LDS_B_11	56
4.2.12	Test Case LDS_B_12	56
4.2.13	Test Case LDS_B_13	56
4.3	UNIT TEST LDS_C - TESTS FOR THE DATAGROUP 2 LDS OBJECT	56
4.3.1	Test Case LDS_C_01	57
4.3.2	Test Case LDS_C_02	57
4.3.3	Test Case LDS_C_03	57
4.3.4	Test Case LDS_C_04	57
4.3.5	Test Case LDS_C_05	58
4.3.6	Test Case LDS_C_06	58
4.3.7	Test Case LDS_C_07	58
4.3.8	Test Case LDS_C_08	59
4.3.9	Test Case LDS_C_09	59
4.3.10	Test Case LDS_C_10	60
4.3.11	Test Case LDS_C_11	60
4.3.12	Test Case LDS_C_12	61
4.3.13	Test Case LDS_C_13	61
4.4	UNIT TEST LDS_D - TESTS FOR THE DATAGROUP 2 LDS OBJECT	61
4.4.1	Test Case LDS_D_01	61

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

4.4.2	Test Case LDS_D_02.....	62
4.4.3	Test Case LDS_D_03.....	62
4.4.4	Test Case LDS_D_04.....	62
4.4.5	Test Case LDS_D_05.....	63
4.4.6	Test Case LDS_D_06.....	63
4.4.7	Test Case LDS_D_07.....	64

1 Introduction

1.1 Scope and purpose

An essential element of the new ICAO compliant e-Passport is the addition of a Secure Contactless Integrated Circuit (SCIC) that holds securely biometric data of the e-Passport bearer within the ICAO defined Logical Data Structure (LDS).

Successful integration of the SCIC into the e-Passport depends upon active international cooperation between many companies and organizations.

The e-Passport has been specified and designed to operate correctly across a wide variety of reading infrastructures worldwide. The risk profile for the e-Passport indicates a high impact if that design includes a widespread error or fault. Therefore it is essential, that all companies and organizations involved make all reasonable efforts to minimize the probability that this error or fault remains undetected before that design is approved and e-Passports are issued.

This test specification covers the application interface, i.e. the ISO7816 conformance of the e-Passport Chip and the conformance of the LDS.

The ISO7816 conformance tests are restricted to the commands defined in the LDS 1.7 [R1] and PKI 1.1 [R2] specifications. Other commands especially file creation and personalization commands are beyond the scope of this document.

The logical data structure test layer analyses the encoding of the LDS objects stored on an e-Passport. This layer contains several test units, one for each LDS object (DG 1 - 16, EF.COM and EF.SOD). Another test unit verifies the integrity and consistency of the different data structures. The tests specified for this layer can be performed using a regular e-Passport or with given input data from a different source (e.g. file). The test configuration document specifies the source of the data.

1.2 Assumptions

It is assumed that the electrical interface and the underlying transport protocol are functionally tested. Thus, failures introduced by the RF protocol are out of scope of the test cases defined here.

1.3 Build-up of the test plan

The general test methodology is defined in the part 1 of the RF protocol and application test standard for e-Passport.

1.4 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", mean 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.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

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", mean 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.)

1.5 Glossary

1.6 Abbreviations

Abbreviation	
AA	Active authentication
AID	Application identifier
APDU	Application protocol data unit
BAC	basic access control
DF	Dedicated file
DG	Data group
DO	Data object
EAC	Extended access control
EF	Elementary file
FID	File identifier
LDS	Logical data structure
MRZ	Machine-readable zone
OID	Object identifier
PCD	Proximity coupling device
PICC	Proximity integrated circuit card
PKD	Public-key directory
PKI	Public-key infrastructure
RF	Radio frequency
SCIC	Secure contactless integrated circuit
SFI	Short file identifier
SOD	Security data object

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

1.7 Reference documentation

The following documentation served as reference for the Technical Reports and this Supplement:

- [R1] *Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies, version 1.7*
- [R2] *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only access, version 1.1*
- [R3] *RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997*
- [R4] *ICAO Doc 9303 Part 1 Volume 2, 6th edition, 2005.*
- [R5] *ISO/IEC 7816-4:2005. Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange.*
- [R6] *ISO/IEC 19794-5:2005. Information technology -- Biometric data interchange formats -- Part 5: Face image data.*

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

2 General test requirements

The tests in this layer require a fully personalized e-Passport. This means that all mandatory data groups **MUST** be present.

This layer tests all mandatory ISO 7816 commands of the SCIC. There are additional test units for tests for optional features like BAC.

All tests are mandatory unless marked as optional or conditional.

2.1 Test Setup

For setting up these tests, any contactless reader supporting type A and type B protocols can be used. One personalized e-Passport sample is needed for executing the tests.

2.2 Implementation conformance statement

In order to set up the tests properly, an applicant **SHALL** provide the information specified in Table 1 below.

The ICAO specification defines several optional elements which can be supported by an e-Passport. This includes security mechanisms like BAC and AA as well as additional data groups (DG 3 to DG 16). Since these elements are optional, it is not possible to define the corresponding tests as mandatory for each e-Passport. Therefore this document specifies a set of profiles. Each profile covers a specific optional element. A tested e-Passport **MUST** be assigned to the supported profiles in the implementation conformance statement and a test **MUST** only be performed if the e-Passport belongs to this profile. The ICAO profile contains the mandatory feature set for ICAO compliant e-Passports. Therefore this profile and its tests are mandatory for all e-Passports.

Note: There are no profile IDs explicitly defined for DG 14 and DG 15 because these data groups are implicitly covered by the AA and EAC profile.

Table 1: Test precondition table "Information on the product"

Information for test setup	Profile	Applicant declaration
Access control applied <ul style="list-style-type: none">PlaintextBasic Access ControlExtended Access Control (TBD)	Plain BAC EAC	
Read Binary with odd instruction byte supported	OddIns	
e-Passport contains elementary file with LDS Data Group 3	DG3	
e-Passport contains elementary file with LDS Data Group 4	DG4	
e-Passport contains elementary file with LDS Data Group 5	DG5	
e-Passport contains elementary file with LDS Data Group 6	DG6	
e-Passport contains elementary file with LDS Data Group 7	DG7	
e-Passport contains elementary file with LDS Data Group 8	DG8	
e-Passport contains elementary file with LDS Data Group 9	DG9	
e-Passport contains elementary file with LDS Data Group 10	DG10	
e-Passport contains elementary file with LDS Data Group 11	DG11	
e-Passport contains elementary file with LDS Data Group 12	DG12	
e-Passport contains elementary file with LDS Data Group 13	DG13	
e-Passport contains elementary file with LDS Data Group 16	DG16	
Authentication supported		

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

Information for test setup	Profile	Applicant declaration
<ul style="list-style-type: none">Passive AuthenticationActive Authentication	ICAO AA	
MRZ provided with the samples	ICAO	
Country signing certificate	ICAO	
Document signer certificate if not contained in SOD	ICAO	

2.3 Verification of ISO 7816-4 Status Words

For most of test cases defined in this document, the status bytes returned by the e-Passport are not exactly defined in the ICAO specification. In these cases the result analysis uses the scheme defined in the ISO 7816-4 [R5] in order to specify the expected result. It is only checked that the response belongs to the specified category. In cases where the expected result is unambiguously defined in the ICAO specification, the exact value is specified in the test case.

Proprietary status words outside the range of defined ISO status words will be treated as failures in the test cases.

Table 2: ISO 7816-4 status words

Status word category	Valid value range	Process behavior
Normal processing	'90 00'	Process completed
	'61 XX'	
Warning processing	'62 XX'	Process completed
	'63 XX'	
Execution error	'64 XX'	Process aborted
	'65 XX'	
	'66 XX'	
Checking error	'67 XX'	Process aborted
	'68 XX'	
	'69 XX'	
	'6A XX'	
	'6B XX'	
	'6C XX'	
	'6D XX'	
'6E XX'		
'6F XX'		

Note: There's a significant difference between Normal and Warning processing on the one side and Execution and Checking error on the other side. While the first group is returned if the process has been fully completed and may return some additional data, the Process aborted categories are issues if the command could not be performed and therefore no additional data MUST be returned. In all test cases where an Execution or Checking error is expected, it MUST be verified that no data except SM protocol elements (DO 99 / 8E) is returned by the e-Passport.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

3 Security and Command Tests

3.1 Unit Test ISO_7816_A – SelectApplication Command

This Unit covers all tests about the SelectApplication command. The LDS specification requires the selection of the LDS application by its AID. Since the AID is unique, selecting the application should be possible regardless of the previously selected DF or EF. Selecting the LDS Application should also reset the cards security state, but this scenario is tested in the access control unit test.

3.1.1 Test Case 7816_A_1

Purpose	Selecting the LDS Application using the AID (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	LDS application is not selected.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 04 0C 07 A0 00 00 02 47 10 01
Expected Results	1. According to the ICAO recommendation the "return no file information" case is used and there's no le byte present. Therefore no response data except the status bytes is expected. Command MUST return 90 00.
Postconditions	LDS application is selected.

3.1.2 Test Case 7816_A_2

Purpose	Selecting the LDS Application using the AID (robustness tests)
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	LDS application is not selected.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 8F A4 04 0C 07 A0 00 00 02 47 10 01 2. Send the given SelectApplication APDU to the test object. => 00 A4 04 0C 07 A0 00 00 02 47 10 02 3. Send the given SelectApplication APDU to the test object. => 00 A4 84 0C 07 A0 00 00 02 47 10 01 4. Send the given SelectApplication APDU to the test object. => 00 A4 04 8C 07 A0 00 00 02 47 10 01 5. Send the given SelectApplication APDU to the test object. => 00 A4 04 8C 08 A0 00 00 02 47 10 01 6. Send the given SelectApplication APDU twice to the test object. => 00 A4 04 0C 07 A0 00 00 02 47 10 01 => 00 A4 04 0C 07 A0 00 00 02 47 10 01
Expected Results	1. The given APDU has an invalid class byte which is explicitly defined as invalid in ISO 7816-3. Therefore the e-Passport MUST return an ISO checking error. 2. The APDU has an invalid AID which does not belong to LDS application. Therefore, the e-Passport MUST return an ISO checking error. 3. The APDU has an invalid P1 parameter. Therefore, the e-Passport chip MUST return an ISO checking error. 4. The APDU has an invalid P2 parameter. Therefore, the e-Passport chip MUST return an ISO checking error. 5. The APDU has an invalid LC parameter. Therefore, the e-Passport chip

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

	MUST return an ISO checking error. 6. The application MUST be selected successfully even it was already selected before. Therefore, the e-Passport chip MUST return error code 90 00 twice.
Postconditions	LDS application is selected.

3.2 Unit Test ISO_7816_B – Security Conditions of a BAC Protected e-Passport

This Unit tests the security conditions of a BAC protected e-Passport. It MUST not be possible read the content of any present file. The tests in this unit try to access the files with an explicit SelectFile command and ReadBinary command with implicit file selected via short file identifier. Note: Some e-Passports allow selection of a protected file but no read access to this file. This will also be accepted.

The tests in this unit only apply to BAC protected e-Passports (profile BAC).

3.2.1 Test Case 7816_B_1

Purpose	Accessing the EF.COM file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 1E
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.2 Test Case 7816_B_2

Purpose	Accessing the EF.SOD file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 1D
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.3 Test Case 7816_B_3

Purpose	Accessing the EF.DG1 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 01

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.4 Test Case 7816_B_4

Purpose	Accessing the EF.DG2 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 02
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.5 Test Case 7816_B_5

Purpose	Accessing the EF.DG3 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG3
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 03
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.6 Test Case 7816_B_6

Purpose	Accessing the EF.DG4 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG4
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 04
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.7 Test Case 7816_B_7

Purpose	Accessing the EF.DG5 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG5
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

	NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 05
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.8 Test Case 7816_B_8

Purpose	Accessing the EF.DG6 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG6
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 06
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.9 Test Case 7816_B_9

Purpose	Accessing the EF.DG7 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG7
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 07
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.10 Test Case 7816_B_10

Purpose	Accessing the EF.DG8 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG8
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 08
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

3.2.11 Test Case 7816_B_11

Purpose	Accessing the EF.DG9 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG9
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 09
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.12 Test Case 7816_B_12

Purpose	Accessing the EF.DG10 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG10
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 0A
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.13 Test Case 7816_B_13

Purpose	Accessing the EF.DG11 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG11
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 0B
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.14 Test Case 7816_B_14

Purpose	Accessing the EF.DG12 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG12
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 0C
Expected Results	1. The e-Passport MUST return error code 69 82.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

Postconditions	Conditions remain unchanged.
----------------	------------------------------

3.2.15 Test Case 7816_B_15

Purpose	Accessing the EF.DG13 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG13
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 0D
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.16 Test Case 7816_B_16

Purpose	Accessing the EF.DG14 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, EAC
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 0E
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.17 Test Case 7816_B_17

Purpose	Accessing the EF.DG15 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, AA
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 0F
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.18 Test Case 7816_B_18

Purpose	Accessing the EF.DG16 file with explicit file selection.
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG16
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

Test scenario	1. Send the given SelectApplication APDU to the test object. => 00 A4 02 0C 02 01 10
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.19 Test Case 7816_B_19

Purpose	Accessing the EF.COM file with implicit file selection. (ReadBinary with SFI)
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 9E 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.20 Test Case 7816_B_20

Purpose	Accessing the EF.SOD file with implicit file selection. (ReadBinary with SFI)
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 9D 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.21 Test Case 7816_B_21

Purpose	Accessing the EF.DG1 file with implicit file selection. (ReadBinary with SFI)
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 81 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

3.2.22 Test Case 7816_B_22

Purpose	Accessing the EF.DG2 file with implicit file selection. (ReadBinary with SFI)
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 82 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.23 Test Case 7816_B_23

Purpose	Accessing the EF.DG3 file with implicit file selection. (ReadBinary with SFI).
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG3
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 83 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.24 Test Case 7816_B_24

Purpose	Accessing the EF.DG4 file with implicit file selection. (ReadBinary with SFI).
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG4
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 84 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.25 Test Case 7816_B_25

Purpose	Accessing the EF.DG5 file with implicit file selection. (ReadBinary with SFI).
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG5
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 85 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.26 Test Case 7816_B_26

Purpose	Accessing the EF.DG6 file with implicit file selection. (ReadBinary with SFI).
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG6
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 86 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.27 Test Case 7816_B_27

Purpose	Accessing the EF.DG7 file with implicit file selection. (ReadBinary with SFI).
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG7
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 87 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.28 Test Case 7816_B_28

Purpose	Accessing the EF.DG8 file with implicit file selection. (ReadBinary with SFI).
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG8
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 88 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

3.2.29 Test Case 7816_B_29

Purpose	Accessing the EF.DG93 file with implicit file selection. (ReadBinary with SFI).
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG9
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 89 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.30 Test Case 7816_B_30

Purpose	Accessing the EF.DG10 file with implicit file selection. (ReadBinary with SFI).
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG10
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 8A 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.31 Test Case 7816_B_31

Purpose	Accessing the EF.DG11 file with implicit file selection. (ReadBinary with SFI).
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG11
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 8B 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.32 Test Case 7816_B_32

Purpose	Accessing the EF.DG12 file with implicit file selection. (ReadBinary with SFI).
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG12
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 8C 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.33 Test Case 7816_B_33

Purpose	Accessing the EF.DG13 file with implicit file selection. (ReadBinary with SFI).
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG13
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 8D 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.34 Test Case 7816_B_34

Purpose	Accessing the EF.DG14 file with implicit file selection. (ReadBinary with SFI).
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, EAC
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 8E 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.2.35 Test Case 7816_B_35

Purpose	Accessing the EF.DG15 file with implicit file selection. (ReadBinary with SFI).
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, AA
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 8F 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

3.2.36 Test Case 7816_B_36

Purpose	Accessing the EF.DG16 file with implicit file selection. (ReadBinary with SFI).
References	ICAO LDS 1.7 [R1] ICAO PKI 1.1 [R2]
Profile	BAC, DG16
Preconditions	The LDS application MUST be selected before and the BAC protocol MUST NOT be active.
Test scenario	1. Send the ReadBinary APDU to the test object. => 00 B0 90 00 00
Expected Results	1. Since read access is prohibited without BAC, the e-Passport MUST NOT return any data. The e-Passport MUST return error code 69 82.
Postconditions	Conditions remain unchanged.

3.3 Unit Test ISO_7816_C – Basic Access Control

This unit checks the BAC implementation of the e-Passport. The complete BAC access mechanism is tested, including robustness tests with invalid input data.

Since the tests in this unit apply to BAC protected e-Passports, they are only mandatory for e-Passports complying with the BAC profile.

3.3.1 Test Case 7816_C_1

Purpose	This function verifies the GetChallenge command (positive test)
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST NOT be active.
Test scenario	1. Send the given GetChallenge APDU to the test object. => 00 84 00 00 08 2. Send the same GetChallenge APDU to the test object. => 00 84 00 00 08
Expected Results	1. The e-Passport MUST return 8 random bytes and a 90 00 status word. 2. The e-Passport MUST return 8 different random bytes and a 90 00 status word.
Postconditions	Conditions remain unchanged.

3.3.2 Test Case 7816_C_2

Purpose	This test checks the response to the MutualAuthenticate command (positive test).
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST NOT be active.
Test scenario	1. Send the given GetChallenge APDU to the test object. => 00 84 00 00 08 2. Send the MutualAuthenticate APDU to the test object. The <data> MUST be calculated from the given MRZ data and the challenge returned in step 1. => 00 82 00 00 28 <data> 28
Expected Results	1. The e-Passport MUST return 8 random bytes and a 90 00 status word. 2. The response from the e-Passport MUST be verified as specified in [R2].

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

	The response status word MUST be 90 00.
Postconditions	BAC MUST be active.

3.3.3 Test Case 7816_C_3

Purpose	This test checks the authentication failure response to the MutualAuthenticate command
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST NOT be active.
Test scenario	<ol style="list-style-type: none">1. Send the given GetChallenge APDU to the test object. => 00 84 00 00 082. Send the MutualAuthenticate APDU to the test object.. Same as 7816_C_2, but for the <data> calculation data from a different MRZ MUST be used. To achieve this, the document number MUST be increment by 1 before the <data> is calculated. => 00 82 00 00 28 <data> 28
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 8 random bytes and a 90 00 status word.2. The e-Passport MUST respond with an ISO warning status word.
Postconditions	Conditions remain unchanged.

3.3.4 Test Case 7816_C_4

Purpose	This test checks the authentication failure response to the MutualAuthenticate command
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST NOT be active.
Test scenario	<ol style="list-style-type: none">1. Send the given GetChallenge APDU to the test object. => 00 84 00 00 082. Send the given GetChallenge APDU to the test object. => 00 84 00 00 083. Send the MutualAuthenticate APDU to the test object. Same as 7816_C_2, but for the <data> calculation the byte from the first challenge MUST be used. => 00 82 00 00 28 <data> 28
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 8 random bytes and a 90 00 status word.2. The e-Passport MUST return 8 random bytes and a 90 00 status word.3. The e-Passport MUST respond with an ISO warning status word.
Postconditions	Conditions remain unchanged.

3.3.5 Test Case 7816_C_5

Purpose	This test checks the response for the MutualAuthenticate command (robustness test)
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST NOT be active.
Test scenario	<ol style="list-style-type: none">1. Send the given GetChallenge APDU to the test object. => 00 84 00 00 08

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

	<ol style="list-style-type: none"> 2. Send the MutualAuthenticate APDU to the test object. The <data> MUST be calculated from the given MRZ data and the challenge returned in step 1. The class byte is set to a wrong value. => 8F 82 00 00 28 <data> 28 3. Send the given GetChallenge APDU to the test object. => 00 84 00 00 08 4. Send the MutualAuthenticate APDU to the test object. The <data> MUST be calculated from the given MRZ data and the challenge returned in step 1. The P1 byte is set to a wrong value. => 00 82 60 00 28 <data> 28 5. Send the given GetChallenge APDU to the test object. => 00 84 00 00 08 6. Send the MutualAuthenticate APDU to the test object. The <data> MUST be calculated from the given MRZ data and the challenge returned in step 1. The P2 byte is set to a wrong value. => 00 82 00 60 28 <data> 28 7. Send the given GetChallenge APDU to the test object. => 00 84 00 00 08 8. Send the MutualAuthenticate APDU to the test object. The <data> MUST be calculated from the given MRZ data and the challenge returned in step 1. The LC byte is set to a wrong value. => 00 82 00 00 29 <data> 28
Expected Results	<ol style="list-style-type: none"> 1. The e-Passport MUST return 8 random bytes and a 90 00 status byte. 2. The e-Passport MUST respond with an ISO checking error. 3. The e-Passport MUST return 8 random bytes and a 90 00 status byte. 4. The e-Passport MUST respond with an ISO checking error. 5. The e-Passport MUST return 8 random bytes and a 90 00 status byte. 6. The e-Passport MUST respond with an ISO checking error. 7. The e-Passport MUST return 8 random bytes and a 90 00 status byte. 8. The e-Passport MUST respond with an ISO checking error.
Postconditions	Conditions remain unchanged.

3.3.6 Test Case 7816_C_6

Purpose	This test checks the response for the MutualAuthenticate command with a corrupted MAC.
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST NOT be active.
Test scenario	<ol style="list-style-type: none"> 1. Send the given GetChallenge APDU to the test object. => 00 84 00 00 08 2. Send the MutualAuthenticate APDU to the test object. The <data> MUST be calculated from the given MRZ data and the challenge returned in step 1. In the calculated MAC the very last byte is incremented by one. => 00 82 00 00 28 <data> 28
Expected Results	<ol style="list-style-type: none"> 1. The e-Passport MUST return 8 random bytes and a 90 00 status byte. 2. The e-Passport MUST respond with an ISO checking error.
Postconditions	Conditions remain unchanged.

Note: this test case differs from test case ISO17816_C_4. In this test case, only the MAC is manipulated but the cryptogram is valid.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

3.3.7 Test Case 7816_C_7

Test case deleted because the GetChallenge command using secure messaging is not defined. The test case may added again when the EAC specification is finalized.

3.3.8 Test Case 7816_C_8

Purpose	This test checks the Secure Messaging coding of a ReadBinary (B0) with SFI (positive tests)
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given ReadBinary (SFI) APDU encoded as a valid SM APDU to the test object. => 0C B0 9E 00 0D 97 01 06 8E 08 <checksum> 002. Search for the cryptogram DO encoded in tag 87 and decrypt it with current session key.3. Search for the cryptographic checksum DO encoded in tag 8E and verify it with current session key.4. Search for the status word DO encoded in tag 99 and verify status word received.
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The response of step 1 MUST contain the read data in a valid cryptogram encoded in tag 87.3. The response of step 1 MUST contain a valid cryptographic checksum encoded in tag 8E.4. The response of step 1 MUST contain a status word encoded in tag 99 that equals the received status word of the secured response.
Postconditions	Conditions unchanged.

3.3.9 Test Case 7816_C_9

Purpose	This test checks the Secure Messaging coding of a ReadBinary (B1) with SFI (positive tests)
References	ICAO PKI 1.1 [R2]
Profile	BAC, OddIns
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given ReadBinary (SFI) APDU encoded as a valid SM APDU to the test object. The offset (0) MUST be encoded in a DO 54, which is then encrypted in a SM 85 object. => 0C B1 9E 00 17 85 08 <cryptogram> 97 01 06 8E 08 <checksum> 002. Search for the cryptogram DO encoded in tag 85 and decrypt it with current session key.3. Search for the cryptographic checksum DO encoded in tag 8E and verify it with current session key.4. Search for the status word DO encoded in tag 99 and verify status word received.
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The response of step 1 MUST contain the read data in a valid cryptogram encoded in tag 85. The data MUST be encapsulated in a tag 53 object.3. The response of step 1 MUST contain a valid cryptographic checksum encoded in tag 8E.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

	4. The response of step 1 MUST contain a status word encoded in tag 99 that equals the received status word of the secured response.
Postconditions	Conditions unchanged.

3.3.10 Test Case 7816_C_10

Purpose	This test checks the Secure Messaging coding of a SelectFile and ReadBinary (B0) w/o SFI (positive tests)
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given SelectFile APDU encoded as a valid SM APDU to the test object. => 0C A4 02 0C 15 87 09 01 <cryptogram> 8E 08 <checksum> 002. Search for the status word DO encoded in tag 99 and verify status word received.3. Search for the cryptographic checksum DO encoded in tag 8E and verify it with current session key.4. Send the given ReadBinary APDU encoded as a valid SM APDU to the test object. => 0C B0 00 00 0D 97 01 06 8E 08 <checksum> 005. Search for the cryptogram DO encoded in tag 87 and decrypt it with current session key.6. Search for the status word DO encoded in tag 99 and verify status word received.7. Search for the cryptographic checksum DO encoded in tag 8E and verify it with current session key.8. Search for further DO.
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status byte.2. The response of step 1 MUST contain a status word encoded in tag 99 that MUST equal the received status word of the secured response.3. The response of step 1 MUST contain a valid cryptographic checksum encoded in tag 8E.4. The e-Passport MUST return 90 00 status byte.5. The response of step 4 MUST contain the read data in a valid cryptogram encoded in tag 87.6. The response of step 4 MUST contain a status word encoded in tag 99 that equals the received status word of the secured response.7. The response of step 4 MUST contain a valid cryptographic checksum encoded in tag 8E.8. The response MUST NOT contain any further data but the trailing status word.
Postconditions	Conditions unchanged.

3.3.11 Test Case 7816_C_11

Purpose	This test checks the Secure Messaging coding of a SelectFile and ReadBinary (B1) w/o SFI (positive tests)
References	ICAO PKI 1.1 [R2]
Profile	BAC, OddIns
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given SelectFile APDU encoded as a valid SM APDU to the test

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

	<p>object. => 0C A4 02 0C 15 87 09 01 <cryptogram> 8E 08 <checksum> 00</p> <ol style="list-style-type: none"> Search for the cryptographic checksum DO encoded in tag 8E and verify it with current session key. Search for the status word DO encoded in tag 99 and verify status word received. Send the given ReadBinary APDU encoded as a valid SM APDU to the test object. The offset (0) MUST be encoded in a DO 54, which is then encrypted in a SM 85 object. => 0C B1 00 00 17 85 08 <cryptogram> 97 01 06 8E 08 <checksum> 00 Search for the cryptogram DO encoded in tag 85 and decrypt it with current session key. Search for the cryptographic checksum DO encoded in tag 8E and verify it with current session key. Search for the status word DO encoded in tag 99 and verify status word received. Search for further DO.
Expected Results	<ol style="list-style-type: none"> The e-Passport MUST return 90 00 status word. The response of step 1 MUST contain a valid cryptographic checksum encoded in tag 8E. The response of step 1 MAY contain a status word encoded in tag 99 that MUST equal the received status word of the secured response. The e-Passport MUST return 90 00 status byte. The response of step 4 MUST contain the read data in a valid cryptogram encoded in tag 85. The data MUST be encapsulated in a tag 53 object. The response of step 4 MUST contain a valid cryptographic checksum encoded in tag 8E. The response of step 4 MUST contain a status word encoded in tag 99 that equals the received status word of the secured response. The response MUST NOT contain any further data but the trailing status word.
Postconditions	Conditions unchanged.

3.3.12 Test Case 7816_C_12

Purpose	The test verifies the Secure Messaging handling while BAC is active for the SelectFile Command (checksum missing)
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none"> Send the given SelectFile APDU encoded as a SM APDU but without the checksum SM object to the test object. => 0C A4 02 0C 0B 87 09 01 <cryptogram> 00 To verify that the error in step 1 has terminated the SM session, send a valid SM APDU (ReadBinary) to the e-Passport. => 0C B0 9E 00 0D 97 01 06 8E 08 <checksum> 00
Expected Results	<ol style="list-style-type: none"> The e-Passport MUST return error code 69 87. Since the session keys are no longer valid, the e-Passport MUST return an ISO checking error.
Postconditions	BAC MUST NOT be active.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

3.3.13 Test Case 7816_C_13

Purpose	The test verifies the Secure Messaging handling while BAC is active for the SelectFile Command (checksum corrupted)
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given SelectFile APDU encoded as a valid SM APDU to the test object. The last byte of the checksum is incremented by one. => 0C A4 02 0C 15 87 09 01 <cryptogram> 8E 08 <corrupted checksum> 002. To verify that the error in step 1 has terminated the SM session, send a valid SM APDU (ReadBinary) to the e-Passport. => 0C B0 9E 00 0D 97 01 06 8E 08 <checksum> 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return error code 69 88.2. Since the session keys are no longer valid, the e-Passport MUST return an ISO checking error.
Postconditions	BAC MUST NOT be active.

3.3.14 Test Case 7816_C_14

Purpose	The tests verifies the Secure Messaging handling while BAC is active for the SelectFile Command (bad send sequence counter)
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given SelectFile APDU encoded as a valid SM APDU to the test object. During the coding of the SM APDU the SendSequenceCounter is not incremented. => 0C A4 02 0C 15 87 09 01 <cryptogram> 8E 08 <corrupted checksum> 002. To verify that the error in step 1 has terminated the SM session, send a valid SM APDU (ReadBinary) to the e-Passport. => 0C B0 9E 00 0D 97 01 06 8E 08 <checksum> 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return error code 69 88.2. Since the session keys are no longer valid, the e-Passport MUST return an ISO checking error.
Postconditions	BAC MUST NOT be active.

3.3.15 Test Case 7816_C_15

Purpose	The test verifies the Secure Messaging handling while BAC is active for the SelectFile Command (invalid class byte)
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given SelectFile APDU encoded as a SM APDU to the test object. The class byte is set to 00. => 00 A4 02 0C 15 87 09 01 <cryptogram> 8E 08 <checksum> 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

3.3.16 Test Case 7816_C_16

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the SelectFile Command.
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	1. Send the given SelectFile APDU as a plain unprotected APDU to the test object. => 00 A4 02 0C 02 01 1E
Expected Results	1. The e-Passport MUST return error code 69 82.
Postconditions	Undefined with respect to BAC.

3.3.17 Test Case 7816_C_17

Purpose	The test verifies the Secure Messaging handling while BAC is active for the ReadBinary Command (checksum missing).
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	1. Send the given ReadBinary APDU encoded as a SM APDU but without the checksum SM object to the test object. => 0C B0 9E 00 03 97 01 06 00 2. To verify that the error in step 1 has terminated the SM session, send a valid SM APDU (ReadBinary) to the e-Passport. => 0C B0 9E 00 0D 97 01 06 8E 08 <checksum> 00
Expected Results	1. The e-Passport MUST return error code 69 87. 2. Since the session keys are no longer valid, the e-Passport MUST return an ISO checking error.
Postconditions	BAC MUST NOT be active.

3.3.18 Test Case 7816_C_18

Purpose	The test verifies the Secure Messaging handling while BAC is active for the ReadBinary Command (checksum corrupted).
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	1. Send the given ReadBinary APDU encoded as a valid SM APDU to the test object. The last byte of the checksum is incremented by one. => 0C B0 00 00 0D 97 01 06 8E 08 <checksum> 00 2. To verify that the error in step 1 has terminated the SM session, send a valid SM APDU (GetChallenge) to the e-Passport. => 0C B0 9E 00 0D 97 01 06 8E 08 <checksum> 00
Expected Results	1. The e-Passport MUST return error code 69 88. 2. Since the session keys are no longer valid, the e-Passport MUST return an ISO checking error.
Postconditions	BAC MUST NOT be active.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

3.3.19 Test Case 7816_C_19

Purpose	The test verifies the Secure Messaging handling while BAC is active for the ReadBinary Command (invalid class byte).
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	1. Send the given ReadBinary APDU encoded as a SM APDU to the test object. The class byte is set to 00. => 00 B0 00 00 0D 97 01 06 8E 08 <checksum> 00
Expected Results	1. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.3.20 Test Case 7816_C_20

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.COM)
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	1. Send the given "Read Binary (SFI)" APDU for EF.COM encoded as a valid SM APDU to the test object. => 0C B0 9E 00 0D 97 01 06 8E 08 <checksum> 00 2. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word. 2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.3.21 Test Case 7816_C_21

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.SOD)
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	1. Send the given "Read Binary (SFI)" APDU for EF.SOD encoded as a valid SM APDU to the test object. => 0C B0 9D 00 0D 97 01 06 8E 08 <checksum> 00 2. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word. 2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

3.3.22 Test Case 7816_C_22

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG1)
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given "Read Binary (SFI)" APDU for EF.DG1 encoded as a valid SM APDU to the test object. => 0C B0 81 00 0D 97 01 06 8E 08 <checksum> 002. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.3.23 Test Case 7816_C_23

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG2)
References	ICAO PKI 1.1 [R2]
Profile	BAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given "Read Binary (SFI)" APDU for EF.DG2 encoded as a valid SM APDU to the test object. => 0C B0 82 00 0D 97 01 06 8E 08 <checksum> 002. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.3.24 Test Case 7816_C_24

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG3)
References	ICAO PKI 1.1 [R2]
Profile	BAC, DG3
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given "Read Binary (SFI)" APDU for EF.DG3 encoded as a valid SM APDU to the test object. => 0C B0 83 00 0D 97 01 06 8E 08 <checksum> 002. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

3.3.25 Test Case 7816_C_25

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG4)
References	ICAO PKI 1.1 [R2]
Profile	BAC, DG4
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given "Read Binary (SFI)" APDU for EF.DG4 encoded as a valid SM APDU to the test object. => 0C B0 84 00 0D 97 01 06 8E 08 <checksum> 002. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.3.26 Test Case 7816_C_26

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG5)
References	ICAO PKI 1.1 [R2]
Profile	BAC, DG5
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given "Read Binary (SFI)" APDU for EF.DG5 encoded as a valid SM APDU to the test object. => 0C B0 85 00 0D 97 01 06 8E 08 <checksum> 002. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.3.27 Test Case 7816_C_27

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG6)
References	ICAO PKI 1.1 [R2]
Profile	BAC, DG6
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given "Read Binary (SFI)" APDU for EF.DG6 encoded as a valid SM APDU to the test object. => 0C B0 86 00 0D 97 01 06 8E 08 <checksum> 002. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

3.3.28 Test Case 7816_C_28

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG8)
References	ICAO PKI 1.1 [R2]
Profile	BAC, DG7
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">Send the given "Read Binary (SFI)" APDU for EF.DG7 encoded as a valid SM APDU to the test object. => 0C B0 87 00 0D 97 01 06 8E 08 <checksum> 00Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">The e-Passport MUST return 90 00 status word.The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.3.29 Test Case 7816_C_29

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG8)
References	ICAO PKI 1.1 [R2]
Profile	BAC, DG8
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">Send the given "Read Binary (SFI)" APDU for EF.DG8 encoded as a valid SM APDU to the test object. => 0C B0 88 00 0D 97 01 06 8E 08 <checksum> 00Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">The e-Passport MUST return 90 00 status word.The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.3.30 Test Case 7816_C_30

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG9)
References	ICAO PKI 1.1 [R2]
Profile	BAC, DG9
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">Send the given "Read Binary (SFI)" APDU for EF.DG9 encoded as a valid SM APDU to the test object. => 0C B0 89 00 0D 97 01 06 8E 08 <checksum> 00Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">The e-Passport MUST return 90 00 status word.The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

3.3.31 Test Case 7816_C_31

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG10)
References	ICAO PKI 1.1 [R2]
Profile	BAC, DG10
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given "Read Binary (SFI)" APDU for EF.DG10 encoded as a valid SM APDU to the test object. => 0C B0 8A 00 0D 97 01 06 8E 08 <checksum> 002. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.3.32 Test Case 7816_C_32

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG11)
References	ICAO PKI 1.1 [R2]
Profile	BAC, DG11
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given "Read Binary (SFI)" APDU for EF.DG11 encoded as a valid SM APDU to the test object. => 0C B0 8B 00 0D 97 01 06 8E 08 <checksum> 002. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.3.33 Test Case 7816_C_33

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG12)
References	ICAO PKI 1.1 [R2]
Profile	BAC, DG12
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given "Read Binary (SFI)" APDU for EF.DG12 encoded as a valid SM APDU to the test object. => 0C B0 8C 00 0D 97 01 06 8E 08 <checksum> 002. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

3.3.34 Test Case 7816_C_34

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG13)
References	ICAO PKI 1.1 [R2]
Profile	BAC, DG13
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given "Read Binary (SFI)" APDU for EF.DG13 encoded as a valid SM APDU to the test object. => 0C B0 8D 00 0D 97 01 06 8E 08 <checksum> 002. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.3.35 Test Case 7816_C_35

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG14)
References	ICAO PKI 1.1 [R2]
Profile	BAC, EAC
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given "Read Binary (SFI)" APDU for EF.DG14 encoded as a valid SM APDU to the test object. => 0C B0 8E 00 0D 97 01 06 8E 08 <checksum> 002. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.3.36 Test Case 7816_C_36

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG15)
References	ICAO PKI 1.1 [R2]
Profile	BAC, AA
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given "Read Binary (SFI)" APDU for EF.DG15 encoded as a valid SM APDU to the test object. => 0C B0 8F 00 0D 97 01 06 8E 08 <checksum> 002. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

3.3.37 Test Case 7816_C_37

Purpose	The test verifies the enforcement of Secure Messaging while BAC is active for the ReadBinary Command. (EF.DG16)
References	ICAO PKI 1.1 [R2]
Profile	BAC, DG16
Preconditions	The LDS application MUST be selected and BAC MUST be active.
Test scenario	<ol style="list-style-type: none">1. Send the given "Read Binary (SFI)" APDU for EF.DG16 encoded as a valid SM APDU to the test object. => 0C B0 90 00 0D 97 01 06 8E 08 <checksum> 002. Send the given ReadBinary APDU as a plain unprotected APDU to the test object. => 00 B0 00 00 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.4 Unit Test ISO_7816_D – SelectFile Command

This unit verifies the implementation of the SelectFile command.

If the Passport is BAC protected, the BAC MUST be active as tested in 7816_C_2. In this case all APDUs MUST be encoded for Secure Messaging and the e-Passport response MUST be decoded again.

The tests in this unit do not explicitly test the Secure Messaging implementation; this is handled by unit 7816_C. Therefore, the tests in this unit also apply to unprotected e-Passports.

3.4.1 Test Case 7816_D_1

Purpose	This function verifies the SelectFile (EF.COM) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	<ol style="list-style-type: none">1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 1E
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.2 Test Case 7816_D_2

Purpose	This function checks robustness of the SelectFile command (robustness test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	<ol style="list-style-type: none">1. Send the given SelectFile APDU to the test object. The class tag is set to the invalid value of 8F. => 8F A4 02 0C 02 01 1E

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

Expected Results	1. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.4.3 Test Case 7816_D_3

Purpose	This function checks robustness of the SelectFile command (Invalid parameter P1).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. The parameter P1 is set to the invalid value of 12. => 00 A4 12 0C 02 01 1E
Expected Results	1. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.4.4 Test Case 7816_D_4

Purpose	This function checks robustness of the SelectFile command (Invalid parameter P2).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. The parameter P2 is set to the invalid value of 1C. => 00 A4 02 1C 02 01 1E
Expected Results	1. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.4.5 Test Case 7816_D_5

Purpose	This function checks robustness of the SelectFile command (Invalid Lc).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. The parameter Lc is set to 03. => 00 A4 02 0C 03 01 1E
Expected Results	1. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.4.6 Test Case 7816_D_6

Purpose	This function verifies the SelectFile (EF.SOD) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 1D
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.7 Test Case 7816_D_7

Purpose	This function verifies the SelectFile (EF.DG1) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 01
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.8 Test Case 7816_D_8

Purpose	This function verifies the SelectFile (EF.DG2) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 02
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.9 Test Case 7816_D_9

Purpose	This function verifies the SelectFile (EF.DG3) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG3
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 03
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.10 Test Case 7816_D_10

Purpose	This function verifies the SelectFile (EF.DG4) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	BAC, DG4
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

	protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 04
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.11 Test Case 7816_D_11

Purpose	This function verifies the SelectFile (EF.DG5) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG5
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 05
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.12 Test Case 7816_D_12

Purpose	This function verifies the SelectFile (EF.DG6) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG6
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 06
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.13 Test Case 7816_D_13

Purpose	This function verifies the SelectFile (EF.DG7) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG7
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 07
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.14 Test Case 7816_D_14

Purpose	This function verifies the SelectFile (EF.DG8) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG8
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 08
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.15 Test Case 7816_D_15

Purpose	This function verifies the SelectFile (EF.DG9) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG9
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 09
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.16 Test Case 7816_D_16

Purpose	This function verifies the SelectFile (EF.DG10) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG10
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 0A
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.17 Test Case 7816_D_17

Purpose	This function verifies the SelectFile (EF.DG11) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG11
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 0B
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.18 Test Case 7816_D_18

Purpose	This function verifies the SelectFile (EF.DG12) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG12
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 0C
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.19 Test Case 7816_D_19

Purpose	This function verifies the SelectFile (EF.DG13) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG13
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 0D
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.20 Test Case 7816_D_20

Purpose	This function verifies the SelectFile (EF.DG14) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	BAC, EAC
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 0E
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.21 Test Case 7816_D_21

Purpose	This function verifies the SelectFile (EF.DG15) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, AA
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 0F
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.22 Test Case 7816_D_22

Purpose	This function verifies the SelectFile (EF.DG16) command (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG16
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

	=> 00 A4 02 0C 02 01 10
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

3.4.23 Test Case 7816_D_23

Purpose	This function verifies the SelectFile command when the file to be selected does not exist.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 02 00
Expected Results	1. The e-Passport MUST return an ISO checking error.
Postconditions	Conditions remain unchanged.

3.5 Unit Test ISO_7816_E – ReadBinary Command

This unit verifies the implementation of the ReadBinary command.

If the Passport is BAC protected, the BAC MUST be active as tested in 7816_C_2. In this case all APDUs MUST be encoded for Secure Messaging and the e-Passport response MUST be decoded again. The tests in this unit do not explicitly test the Secure Messaging implementation; this is handled by unit 7816_C. Therefore, the tests in this unit also apply to unprotected e-Passports.

Note for BAC profile: For ReadBinary command in Secure Messaging mode, there is no clear definition in the ISO specification in case that the Le byte in DO 97 object equals zero. Therefore, the Le byte in the DO 97 object should be set to 'E0' in all test cases specified in this unit.

3.5.1 Test Case 7816_E_1

Purpose	This function verifies the ReadBinary command (w/o SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport.
Test scenario	1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 1E 2. Send the ReadBinary APDU to the test object, this will read the first bytes of the EF.COM => 00 B0 00 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word. 2. The e-Passport MUST return 90 00 status word.
Postconditions	Conditions remain unchanged.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

3.5.2 Test Case 7816_E_2

Purpose	Test the robustness of the ReadBinary command (w/o SFI) (invalid class byte).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. The SelectFile command is implicitly tested in this test case; so it is required that the test object has previously passed the SelectFile Test 7816_D_1, otherwise this test will fail.
Test scenario	<ol style="list-style-type: none">1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 1E2. Send the ReadBinary APDU to the test object. The class byte is set to the invalid value of FF. => 8F B0 00 00 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.5.3 Test Case 7816_E_3

Purpose	Test the robustness of the ReadBinary command (w/o SFI) (offset beyond EOF).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. The SelectFile command is implicitly tested in this test case; so it is required that the test object has previously passed the SelectFile Test 7816_D_1, otherwise this test will fail.
Test scenario	<ol style="list-style-type: none">1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 1E2. Send the ReadBinary APDU to the test object. The offset is beyond the end of the EF.COM file. Note: Since the actual file on the e-Passport could be larger than necessary, the e-Passport may return valid data in this case. If this happens, the test may have to be repeated with an appropriated offset. => 00 B0 7F FF 00
Expected Results	<ol style="list-style-type: none">1. The e-Passport MUST return 90 00 status word.2. The e-Passport MUST return an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.5.4 Test Case 7816_E_4

Purpose	Test the robustness of the ReadBinary command (w/o SFI) (Le beyond EOF).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. The SelectFile command is implicitly tested in this test case; so it is required that the test object has previously passed the SelectFile Test 7816_D_1, otherwise this test will fail.
Test scenario	<ol style="list-style-type: none">1. Send the given SelectFile APDU to the test object. => 00 A4 02 0C 02 01 1E2. Send the ReadBinary APDU to the test object. The Le Byte requests more data than available in the EF.COM file Note: Since the actual file on the e-

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

	Passport could be larger than necessary, the e-Passport may return valid data in this case. If this happens, the test may have to be repeated with an appropriated offset. => 00 B0 00 00 E0
Expected Results	1. The e-Passport MUST return 90 00 status word. 2. The e-Passport MUST return an ISO warning status word or an ISO checking error.
Postconditions	Undefined with respect to BAC.

3.5.5 Test Case 7816_E_5

Purpose	This function verifies the ReadBinary command (EF.COM SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.COM. => 00 B0 9E 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.COM MUST be selected.

3.5.6 Test Case 7816_E_6

Purpose	This function verifies the ReadBinary command (EF.SOD SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.SOD. => 00 B0 9D 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.SOD MUST be selected.

3.5.7 Test Case 7816_E_7

Purpose	This function verifies the ReadBinary command (EF.DG1 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG1. => 00 B0 81 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG1 MUST be selected.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

3.5.8 Test Case 7816_E_8

Purpose	This function verifies the ReadBinary command (EF.DG2 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG2. => 00 B0 82 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG2 MUST be selected.

3.5.9 Test Case 7816_E_9

Purpose	This function verifies the ReadBinary command (EF.DG3 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG3
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG3. => 00 B0 83 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG3 MUST be selected.

3.5.10 Test Case 7816_E_10

Purpose	This function verifies the ReadBinary command (EF.DG4 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG4
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG3. => 00 B0 84 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG4 MUST be selected.

3.5.11 Test Case 7816_E_11

Purpose	This function verifies the ReadBinary command (EF.DG5 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG5
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG5. => 00 B0 85 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

Postconditions	EF.DG5 MUST be selected.
----------------	--------------------------

3.5.12 Test Case 7816_E_12

Purpose	This function verifies the ReadBinary command (EF.DG6 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG6
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG6. => 00 B0 86 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG6 MUST be selected.

3.5.13 Test Case 7816_E_13

Purpose	This function verifies the ReadBinary command (EF.DG7 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG7
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG7. => 00 B0 87 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG7 MUST be selected.

3.5.14 Test Case 7816_E_14

Purpose	This function verifies the ReadBinary command (EF.DG8 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG8
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG8. => 00 B0 88 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG8 MUST be selected.

3.5.15 Test Case 7816_E_15

Purpose	This function verifies the ReadBinary command (EF.DG9 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG9
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

	(256 bytes at maximum) of the EF.DG9. => 00 B0 89 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG9 MUST be selected.

3.5.16 Test Case 7816_E_16

Purpose	This function verifies the ReadBinary command (EF.DG10 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG10
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG10. => 00 B0 8A 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG10 MUST be selected.

3.5.17 Test Case 7816_E_17

Purpose	This function verifies the ReadBinary command (EF.DG11 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG11
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG11. => 00 B0 8B 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG11 MUST be selected.

3.5.18 Test Case 7816_E_18

Purpose	This function verifies the ReadBinary command (EF.DG12 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG12
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG12. => 00 B0 8C 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG12 MUST be selected.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

3.5.19 Test Case 7816_E_19

Purpose	This function verifies the ReadBinary command (EF.DG13 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG13
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG13. => 00 B0 8D 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG13 MUST be selected.

3.5.20 Test Case 7816_E_20

Purpose	This function verifies the ReadBinary command (EF.DG14 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, EAC
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG14. => 00 B0 8E 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG14 MUST be selected.

3.5.21 Test Case 7816_E_21

Purpose	This function verifies the ReadBinary command (EF.DG15 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, AA
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG15. => 00 B0 8F 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG15 MUST be selected.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

3.5.22 Test Case 7816_E_22

Purpose	This function verifies the ReadBinary command (EF.DG16 SFI) (positive test).
References	ICAO LDS 1.7 [R1]
Profile	ICAO, DG16
Preconditions	The LDS application MUST be selected and BAC MUST be active if BAC protected e-Passport. An EF MUST NOT be selected.
Test scenario	1. Send the ReadBinary APDU to the test object, this will read the first bytes (256 bytes at maximum) of the EF.DG16. => 00 B0 90 00 00
Expected Results	1. The e-Passport MUST return 90 00 status word.
Postconditions	EF.DG16 MUST be selected.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

4 Logical Data Structure Tests

The logical data structure test layer analyses the encoding of the LDS objects stored on an e-Passport. This layer contains several test units, one for each LDS object (DG 1 - 16, EF.COM and EF.SOD). Another test unit verifies the integrity and consistency of the different data structures. The tests specified in this layer can be performed using a regular e-Passport or with given input data from a different source (e.g. file). The test configuration document specifies the source of the data.

4.1 Unit Test LDS_A - Tests for the EF.COM LDS Object

This unit includes all test cases concerning the EF.COM element. The general LDS header encoding is tested as well as the referred LDS and Unicode version numbers. The consistency of the data group list with respect to the available data group objects is checked in a different test unit.

4.1.1 Test Case LDS_A_01

Purpose	This test checks the template tag; the encoded LDS element starts with.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.COM object in binary format as read from the e-Passport.
Test scenario	1. Check the very first byte of the EF.COM element
Expected Results	1. First byte MUST be "60"
Postconditions	None

4.1.2 Test Case LDS_A_02

Purpose	This test checks the encoding of LDS element length.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.COM object in binary format as read from the e-Passport.
Test scenario	1. Analyze the encoding of the bytes that follow the template tag 2. Verify the length of the given LDS object
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 given LDS object.
Postconditions	None

4.1.3 Test Case LDS_A_03

Purpose	This test checks the LDS version referred by the EF.COM element
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.COM object in binary format as read from the e-Passport.
Test scenario	1. Search for configured tag "5F01" 2. Verify the length of the tag "5F01" 3. Verify the length of LDS version DE. 4. Verify the LDS version.
Expected Results	1. Tag MUST be present. 2. The bytes that follow the tag MUST contain a valid length encoding.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

	3. Length MUST be 4. 4. The specified LDS version MUST be "30 31 30 37"
Postconditions	None

4.1.4 Test Case LDS_A_04

Purpose	This test checks the Unicode version referred by the EF.COM element
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.COM object in binary format as read from the e-Passport.
Test scenario	1. Search for configured tag "5F36" 2. Verify the length of the tag "5F36" 3. Verify the length of the Unicode version DE. 4. Verify the Unicode version.
Expected Results	1. Tag MUST be present. 2. The bytes that follow the tag MUST contain a valid length encoding. 3. The length MUST be 6. 4. The specified Unicode version MUST be "30 34 30 30 30 30".
Postconditions	None

4.1.5 Test Case LDS_A_05

Purpose	This test checks the Unicode version referred by the EF.COM element
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.COM object in binary format as read from the e-Passport.
Test scenario	1. Search for configured tag "5C" 2. Verify the length of the tag "5C" 3. Verify if mandatory data groups are present. 4. Verify the validity of present data groups.
Expected Results	1. Tag MUST be present. 2. The bytes that follow the tag MUST contain a valid length encoding 3. The list MUST at least contain the tags for the mandatory data groups "61", "75". 4. The list MUST contain only valid data group tags as specified in [R1], i.e. "61", "75", "63", "76", "65", "66", "67", "68", "69", "6A", "6B", "6C", "6D", "6E", "6F", "70"
Postconditions	None

4.2 Unit Test LDS_B - Tests for the DataGroup 1 LDS object

This unit includes all test cases concerning the DG 1 element (MRZ). The general LDS header encoding is tested as well as the MRZ elements and the calculation of the check digits.

4.2.1 Test Case LDS_B_01

Purpose	This test checks the template tag; the encoded LDS element starts with.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG1 object in binary format as read from the e-Passport.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

Test scenario	1. Check the very first byte of the EF.DG1 element
Expected Results	1. First byte MUST be "61"
Postconditions	None

4.2.2 Test Case LDS_B_02

Purpose	This test checks the encoding of LDS element length.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG1 object in binary format as read from the e-Passport.
Test scenario	1. Analyze the encoding of the bytes that follow the template tag 2. Verify the length of the given LDS object
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 given LDS object.
Postconditions	None

4.2.3 Test Case LDS_B_03

Purpose	This test checks the encoding of the MRZ data object.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG1 object in binary format as read from the e-Passport.
Test scenario	1. Verify the length of the tag "5F1F" 2. Verify that the length encoding is correct. 3. Verify that the encoded length equals the remaining size of DG1.
Expected Results	1. The first bytes of the LDS element data MUST be the tag for the MRZ data object. 2. The bytes that follow the MRZ data object tag MUST contain a valid length encoding (According to ASN.1 encoding rules). 3. The encoded length MUST match the remaining size of the given DG1 object.
Postconditions	None

4.2.4 Test Case LDS_B_04

Purpose	This test checks the encoding of the document type.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG1 object in binary format as read from the e-Passport.
Test scenario	1. Analyze the first two characters of the MRZ.
Expected Results	1. The document type encoded in the Data Group 1 object MUST be as defined in [R4], "P<", "I<".
Postconditions	None

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

4.2.5 Test Case LDS_B_05

Purpose	This test checks the encoding of the issuing state element of the MRZ.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG1 object in binary format as read from the e-Passport.
Test scenario	1. Analyze the next three characters of the MRZ.
Expected Results	1. The issuing state element MUST be encoded as defined in [R4]. AFG, ALB, DZA, ASM, AND, AGO, AIA, ATA, ATG, ARG, ARM, ABW, AUS, AUT, AZE, BHS, BHR, BGD, BRB, BLR, BEL, BLZ, BEN, BMU, BTN, BOL, BIH, BWA, BVT, BRA, IOT, BRN, BGR, BFA, BDI, KHM, CMR, CAN, CPV, CYM, CAF, TCD, CHL, CHN, CXR, CCK, COL, COM, COG, COK, CRI, CIV, HRV, CUB, CYP, CZE, PRK, COD, DNK, DJI, DMA, DOM, TLS, ECU, EGY, SLV, GNQ, ERI, EST, ETH, FLK, FRO, FJI, FIN, FRA, FXX, GUF, PYF, ATF, GAB, GMB, GEO, D<<. GHA, GIB, GRC, GRL, GRD, GLP, GUM, GTM, GIN, GNB, GUY, HTI, HMD, VAT, HND, HKG, HUN, ISL, IND, IDN, IRN, IRQ, IRL, ISR, ITA, JAM, JPN, JOR, KAZ, KEN, KIR, KWT, KGZ, LAO, LVA, LBN, LSO, LBR, LBY, LIE, LTU, LUX, MAC, MDG, MWI, MYS, MDV, MLI, MLT, MHL, MTQ, MRT, MUS, MYT, MEX, FSM, MCO, MNG, MSR, MAR, MOZ, MMR, NAM, NRU, NPL, NLD, ANT, NTZ, NCL, NZL, NIC, NER, NGA, NIU, NFK, MNP, NOR, OMN, PAK, PLW, PAN, PNG, PSE, PRY, PER, PHL, PCN, POL, PRT, PRI, QAT, MDA, KOR, REU, ROU, RUS, RWA, SHN, KNA, LCA, SPM, VCT, WSM, SMR, STP, SAU, SEN, SYC, SLE, SGP, SVK, SVN, SLB, SOM, ZAF, SGS, ESP, LKA, SDN, SUR, SJM, SWZ, SWE, CHE, SYR, TWN, TJK, THA, MKD, TGO, TKL, TON, TTO.
Postconditions	None

4.2.6 Test Case LDS_B_06

Purpose	This test checks the encoding of the holder name of the MRZ.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG1 object in binary format as read from the e-Passport.
Test scenario	1. Check that the holder name is not empty. 2. Check that the holder name contains only uppercase character
Expected Results	1. Holder name MUST NOT be empty. 2. Holder name MUST only contain uppercase letters.
Postconditions	None

4.2.7 Test Case LDS_B_07

Purpose	This test checks the validity of the document number.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG1 object in binary format as read from the e-Passport.
Test scenario	1. Check that the document number is not empty. 2. Check the document number check digit.
Expected Results	1. Document number MUST NOT be empty. 2. Document number check digit MUST be valid.
Postconditions	None

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

4.2.8 Test Case LDS_B_08

Purpose	This test checks the validity of the document number.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG1 object in binary format as read from the e-Passport.
Test scenario	1. Analyze the issuing state element.
Expected Results	1. The issuing state element MUST be encoded as defined in [R4]. AFG, ALB, DZA, ASM, AND, AGO, AIA, ATA, ATG, ARG, ARM, ABW, AUS, AUT, AZE, BHS, BHR, BGD, BRB, BLR, BEL, BLZ, BEN, BMU, BTN, BOL, BIH, BWA, BVT, BRA, IOT, BRN, BGR, BFA, BDI, KHM, CMR, CAN, CPV, CYM, CAF, TCD, CHL, CHN, CXR, CCK, COL, COM, COG, COK, CRI, CIV, HRV, CUB, CYP, CZE, PRK, COD, DNK, DJI, DMA, DOM, TLS, ECU, EGY, SLV, GNQ, ERI, EST, ETH, FLK, FRO, FJI, FIN, FRA, FXX, GUF, PYF, ATF, GAB, GMB, GEO, D<<. GHA, GIB, GRC, GRL, GRD, GLP, GUM, GTM, GIN, GNB, GUY, HTI, HMD, VAT, HND, HKG, HUN, ISL, IND, IDN, IRN, IRQ, IRL, ISR, ITA, JAM, JPN, JOR, KAZ, KEN, KIR, KWT, KGZ, LAO, LVA, LBN, LSO, LBR, LBY, LIE, LTU, LUX, MAC, MDG, MWI, MYS, MDV, MLI, MLT, MHL, MTQ, MRT, MUS, MYT, MEX, FSM, MCO, MNG, MSR, MAR, MOZ, MMR, NAM, NRU, NPL, NLD, ANT, NTZ, NCL, NZL, NIC, NER, NGA, NIU, NFK, MNP, NOR, OMN, PAK, PLW, PAN, PNG, PSE, PRY, PER, PHL, PCN, POL, PRT, PRI, QAT, MDA, KOR, REU, ROU, RUS, RWA, SHN, KNA, LCA, SPM, VCT, WSM, SMR, STP, SAU, SEN, SYC, SLE, SGP, SVK, SVN, SLB, SOM, ZAF, SGS, ESP, LKA, SDN, SUR, SJM, SWZ, SWE, CHE, SYR, TWN, TJK, THA, MKD, TGO, TKL, TON, TTO.
Postconditions	None

4.2.9 Test Case LDS_B_09

Purpose	This test checks the validity of the date of birth.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG1 object in binary format as read from the e-Passport.
Test scenario	1. Check that the date of birth element contains a valid date. 2. Check the date of birth check digit.
Expected Results	1. The date of birth MUST be reasonable. It MUST specify an existing day and it SHOULD be in the past. 2. The date of birth check digit MUST be valid.
Postconditions	None

4.2.10 Test Case LDS_B_10

Purpose	This test checks the encoding of the sex element.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG1 object in binary format as read from the e-Passport.
Test scenario	1. Check the encoded sex.
Expected Results	1. The character of the sex element MUST be “F”, “M”, or “U”.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

Postconditions	None
----------------	------

4.2.11 Test Case LDS_B_11

Purpose	This test checks the validity of the date of expiry.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG1 object in binary format as read from the e-Passport.
Test scenario	1. Check that the date of expiry element contains a valid date. 2. Check the date of expiry check digit.
Expected Results	1. The date of expiry MUST specify an existing day. 2. The date of expiry check digit MUST be valid.
Postconditions	None

4.2.12 Test Case LDS_B_12

Purpose	This test checks the optional data.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG1 object in binary format as read from the e-Passport.
Test scenario	1. Check the optional data check digit.
Expected Results	1. The optional data check digit MUST be valid.
Postconditions	None

4.2.13 Test Case LDS_B_13

Purpose	This test checks the composite check digit.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG1 object in binary format as read from the e-Passport.
Test scenario	1. Check the composite check digit.
Expected Results	1. The composite check digit MUST be valid.
Postconditions	None

4.3 Unit Test LDS_C - Tests for the DataGroup 2 LDS object

This unit includes all test cases concerning the DG 2 element (Face). The general LDS header encoding is tested as well as the CBEFF encoded biometric template and ISO 19794 coding [R6] of the biometric object itself. Since the CBEFF and the ISO specification allow a very high degree of freedom, this unit contains tests for the mandatory elements as specified in the LDS.

There are some additional (optional) tests that verify the encoding optional elements. The general rule for this optional test is: if an optional element is present, it MUST be encoded according to the corresponding specification, otherwise the test fails.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

4.3.1 Test Case LDS_C_01

Purpose	This test checks the template tag; the encoded DataGroup 2 element starts with.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG2 object in binary format as read from the e-Passport.
Test scenario	1. Check the very first byte of the EF.DG2 element
Expected Results	1. First byte MUST be "75"
Postconditions	None

4.3.2 Test Case LDS_C_02

Purpose	This test checks the encoding of LDS element length.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG2 object in binary format as read from the e-Passport.
Test scenario	1. Analyze the encoding of the bytes that follow the template tag 2. Verify the length of the given LDS object
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 given LDS object.
Postconditions	None

4.3.3 Test Case LDS_C_03

Purpose	This test checks the encoding of the Biometric Information Group Template.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG2 object in binary format as read from the e-Passport.
Test scenario	1. Check the first tag in the DG 2 data. 2. Verify the length of the DG 2 data. 3. Verify that the encoded length is less than size of DG 2.
Expected Results	1. Tag MUST be "7F61". 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). 3. The encoded length MUST not exceed the remaining bytes of the DG 2 data element.
Postconditions	None

4.3.4 Test Case LDS_C_04

Purpose	This test checks the encoding of the number of instances stored in the Biometric Information Group Template.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG2 object in binary format as read from the e-Passport.
Test scenario	1. Check the first tag inside the group template 2. Verify the length of the "number of instances" data object. 3. Verify that the encoded length is less than rest of size of DG 2.
Expected Results	1. Tag MUST be "02".

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

	<ol style="list-style-type: none">This element MUST have a valid encoded length (According to ASN.1 encoding rules).The number of instances MUST be 1.
Postconditions	None

4.3.5 Test Case LDS_C_05

Purpose	This test checks the encoding of the first biometric information template.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG2 object in binary format as read from the e-Passport.
Test scenario	<ol style="list-style-type: none">Check the tag of the biometric information template.Verify the length of the “biometric information template” data object.Verify that the encoded length is less than rest of size of DG 2.
Expected Results	<ol style="list-style-type: none">Tag MUST be “7F60”.This element MUST have a valid encoded length (According to ASN.1 encoding rules).The encoded length MUST not exceed the remaining bytes of the DG 2 element.
Postconditions	None

4.3.6 Test Case LDS_C_06

Purpose	This test checks the encoding of the biometric header template tag.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG2 object in binary format as read from the e-Passport.
Test scenario	<ol style="list-style-type: none">Check the presence of the biometric header template tag with the configured tag.Verify the length of the “biometric header template” data object.Verify that the encoded length is less than rest of size of DG 2.
Expected Results	<ol style="list-style-type: none">Tag MUST be “A1”.This element MUST have a valid encoded length (According to ASN.1 encoding rules).The encoded length MUST not exceed the remaining bytes of the DG 2 element.
Postconditions	None

4.3.7 Test Case LDS_C_07

Purpose	This test checks the presence/encoding of the CBEFF element "format owner".
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG2 object in binary format as read from the e-Passport. The tested CBEFF element is part of biometric header template located in LDS_C_06.
Test scenario	<ol style="list-style-type: none">Check the presence of the “format owner” tag.Verify the length of the “format owner” data object.Check the length of the “format owner” value.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

	4. Verify the “format owner” value.
Expected Results	<ol style="list-style-type: none">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”.
Postconditions	None

4.3.8 Test Case LDS_C_08

Purpose	This test checks the presence/encoding of the CBEFF element "format type".
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG2 object in binary format as read from the e-Passport. The tested CBEFF element is part of biometric header template located in LDS_C_06.
Test scenario	<ol style="list-style-type: none">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	<ol style="list-style-type: none">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 “00 08”.
Postconditions	None

4.3.9 Test Case LDS_C_09

Purpose	This test checks the encoding of the biometric data object tag.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.DG2 object in binary format as read from the e-Passport. The biometric data object is part of the biometric information template tested in LDS_C_05.
Test scenario	<ol style="list-style-type: none">1. Check the presence of the biometric data object tag.2. Verify the length of the biometric data object.3. Verify that the encoded length is less than rest of size of DG 2.
Expected Results	<ol style="list-style-type: none">1. Tag MUST be “5F2E”2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).3. The encoded length MUST not exceed the remaining bytes of the DG 2 element.
Postconditions	None

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

4.3.10 Test Case LDS_C_10

Purpose	This test checks the encoding of the facial header block.
References	ICAO LDS 1.7 [R1] ISO 19794-4 [R6]
Profile	ICAO
Preconditions	Encoded EF.DG2 object in binary format as read from the e-Passport. The biometric data object is part of the biometric data object tested in LDS_C_09.
Test scenario	<ol style="list-style-type: none">1. Check the first 4 bytes of the header block (Format identifier)2. Check the next 4 bytes of the header block (Version number)3. Check the record length element.4. Check the Number of Facial Images element.
Expected Results	<ol style="list-style-type: none">1. The format identifier MUST be "46 41 43 00".2. The version number MUST be "30 31 30 00".3. The length MUST not exceed the remaining bytes of the DG2 element and MUST match the encoded length of the biometric data object.4. The number of facial images MUST at least be 1.
Postconditions	None

4.3.11 Test Case LDS_C_11

Purpose	This test checks the encoding of the facial information block. This test is mandatory for the first facial information block and should be repeated for further optional facial images.
References	ICAO LDS 1.7 [R1] ISO 19794-4 [R6]
Profile	ICAO
Preconditions	Encoded EF.DG2 object in binary format as read from the e-Passport.
Test scenario	<ol style="list-style-type: none">1. Check the Facial Record Data Length.2. Check the number of facial feature points.3. Check the gender element.4. Check the eye colour element.5. Check the hair colour element.6. Check Pose Angle - Yaw.7. Check Pose Angle - Pitch.8. Check Pose Angle - Roll.9. Check Pose Angle Uncertainty - Yaw.10. Check Pose Angle Uncertainty - Pitch.11. Check Pose Angle Uncertainty - Roll.
Expected Results	<ol style="list-style-type: none">1. The Facial Record Data Length MUST be at least 32 bytes and MUST not exceed the remaining size of the biometric data object.2. The size of the feature point structures (8 * number of facial feature points) MUST not exceed the remaining size of the biometric data object3. The gender MUST be encoded as "00", "01", "02", or "FF".4. The eye colour MUST be encoded as "00", "01", "02", "03", "04", "05", "06", "07", or "FF".5. The hair colour MUST be encoded as "00", "01", "02", "03", "04", "05", "06", "07", or "FF".6. The Pose Angle - Yaw MUST be equal or less than 181.7. The Pose Angle - Pitch MUST be equal or less than 181.8. The Pose Angle - Roll MUST be equal or less than 181.9. The Pose Angle Uncertainty - Yaw MUST be equal or less than 181.10. The Pose Angle Uncertainty - Pitch MUST be equal or less than 181.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

	11. The Pose Angle Uncertainty - Roll MUST be equal or less than 181.
Postconditions	None

4.3.12 Test Case LDS_C_12

Purpose	This test checks the encoding of the facial feature points. It is conditional and applies only if there are feature points encoded. This test should be repeated for every present feature point. See LDS_C_11 for the number of feature points.
References	ICAO LDS 1.7 [R1] ISO 19794-4 [R6]
Profile	ICAO
Preconditions	Encoded EF.DG2 object in binary format as read from the e-Passport.
Test scenario	1. Check the feature point type.
Expected Results	1. The feature point type MUST be 1.
Postconditions	None

4.3.13 Test Case LDS_C_13

Purpose	This test checks the encoding of the image information block. This test is mandatory for the first image information block and should be repeated for further optional facial images.
References	ICAO LDS 1.7 [R1] ISO 19794-4 [R6]
Profile	ICAO
Preconditions	Encoded EF.DG2 object in binary format as read from the e-Passport.
Test scenario	1. Check the face image type. 2. Check the image data type.
Expected Results	1. The face image type MUST be encoded as "00", "01", or "02". 2. The image data type MUST be encoded as "00" or "01".
Postconditions	None

4.4 Unit Test LDS_D - Tests for the DataGroup 2 LDS object

This unit includes all test cases concerning the EF.SOD element. The general LDS header encoding is tested as well as the contained CMS (PKCS#7) signed content object.

In order verify the signing certificate signature the corresponding country signing certificate is needed. For the verification of the LDS security object, the binary data group objects and the EF.COM is needed as read from the e-Passport.

4.4.1 Test Case LDS_D_01

Purpose	This test checks the template tag; the encoded DataGroup 2 element starts with.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.SOD object in binary format as read from the e-Passport.
Test scenario	1. Check the very first byte of the EF.SOD element.
Expected Results	1. First byte MUST be "77".
Postconditions	None

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

4.4.2 Test Case LDS_D_02

Purpose	This test checks the encoding of LDS element length.
References	ICAO LDS 1.7 [R1]
Profile	ICAO
Preconditions	Encoded EF.SOD object in binary format as read from the e-Passport.
Test scenario	<ol style="list-style-type: none">1. Analyze the encoding of the bytes that follow the template tag2. Verify the length of the given LDS object
Expected Results	<ol style="list-style-type: none">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 given LDS object.
Postconditions	None

4.4.3 Test Case LDS_D_03

Purpose	This test checks the ASN#1 encoding of a PKCS#7 signedData object.
References	ICAO PKI 1.1 [R2]
Profile	ICAO
Preconditions	Encoded EF.SOD object in binary format as read from the e-Passport.
Test scenario	<ol style="list-style-type: none">1. Check that the element has a sound ASN.1 structure.
Expected Results	<ol style="list-style-type: none">1. The PKCS#7 signed data object included as the value in the LDS true template MUST be encoded according to the DER format.
Postconditions	None

4.4.4 Test Case LDS_D_04

Purpose	This test checks the value that is encoded into the signedData element.
References	ICAO PKI 1.1 [R2]
Profile	ICAO
Preconditions	Encoded EF.SOD object in binary format as read from the e-Passport.
Test scenario	<ol style="list-style-type: none">1. Check the SignedData version value.2. Check the digestAlgorithms list.3. Check the eContentType.4. Check the certificates list.
Expected Results	<ol style="list-style-type: none">1. The version number MUST be 3.2. All OIDs MUST be valid. This list SHOULD contain all used digestAlgorithms in this signedData container. It MUST contain only digestAlgorithms specified in the PKI report:<ul style="list-style-type: none">1.3.14.3.2.26 (SHA1)2.16.840.1.101.3.4.2.1 (SHA-2 256)2.16.840.1.101.3.4.2.2 (SHA-2 384)2.16.840.1.101.3.4.2.3 (SHA-2 512)2.16.840.1.101.3.4.2.4 (SHA-2 224)3. The eContentType MUST have OID id-icao-ldsSecurityObject.4. According to the PKI Report; the certificate list MAY contain the Document Signer Certificate. If this is the case, the Document Signer Certificate is tested in LDS_D_7. Other certificates SHOULD NOT be included in this list.
Postconditions	None

RF protocol and application test standard for e-Passport - part 3

Version : 0.9
Date : Mar 17, 2006

4.4.5 Test Case LDS_D_05

Purpose	This test checks the SignerInfo element of the signedData structure. The signedData Structure MUST at least contain one signer info. If there is more than one signer info, although this is not recommended in the PKI report, this test MUST be repeated for each element.
References	ICAO PKI 1.1 [R2]
Profile	ICAO
Preconditions	Encoded EF.SOD object in binary format as read from the e-Passport.
Test scenario	<ol style="list-style-type: none">1. Check the signer info version value.2. Check the choice of the sid element.3. Check if the certificate identified in the sid is included in the signed data certificates list or available in the PKD.4. Check the digestAlgorithm identifier.5. Check the signedAttrs element.6. Check the MessageDigest Attribute.7. Check the SigningTime attribute if present.8. Check the signatureAlgorithm element.9. Check the signature element. It is verified with the signer certificates public key and the hash value produced over the signedAttributes.
Expected Results	<ol style="list-style-type: none">1. The version number MUST be 1 or 3.2. The choice of the sid element MUST match the signer info version value. (Version 1 if issuerandSerialNumber is used and 3 if subjectKeyIdentifier is used).3. Certificate MUST be available.4. The digestAlgorithmID MUST be included in the algorithm list.5. The signed attributes list MUST contain the MessageDigest attribute.6. The value of the message digest attribute MUST match the hash value of the eContent element. (Using the digestAlgorithm specified above)7. If there's a SigningTime attribute present, the signing time MUST be within the validity period of the signing certificate.8. The signature algorithm MUST refer to an algorithm specified in [R2]: RSA, DSA, or ECDSA.9. The signature MUST be valid.
Postconditions	None

4.4.6 Test Case LDS_D_06

Purpose	This test checks the LDS Security Object stored as eContent in the signedData Object. The LDS Security Object is stored as the eContent element in the signedData Structure.
References	ICAO PKI 1.1 [R2]
Profile	ICAO
Preconditions	Encoded EF.SOD object in binary format as read from the e-Passport. For the data group hash verification this test needs also the binary data group objects as read from the e-Passport.
Test scenario	<ol style="list-style-type: none">1. Check the ASN.1 encoding of the LDS Security Object.2. Check the security object version element.3. Check the digestAlgorithm identifier.4. Check the DataGroupHash Sequence.5. Check the dataGroup numbers in the DataGroup Hash Sequence.6. Check the dataGroup numbers in the DataGroup Hash Sequence.7. Check the dataGroup hash values in the Hash Sequence. Compare the hash

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

	value with the corresponding data group binary objects.
Expected Results	<ol style="list-style-type: none"> 1. The object MUST be encoded according to the DER syntax. 2. The version number MUST be 0. 3. The digestAlgorithm identifier MUST be one of the algorithms specified in [R2]: SHA1, SHA-224, SHA-256, SHA-384, and SHA-512. 4. The Sequence MUST contain at least 2 entries for DG 1 and 2. 5. The Sequence MUST contain a hash value for all present data groups. There MUST be no additional hash value for non-existing data groups. 6. The referred dataGroups MUST match the DataGroup list in the EF.COM. 7. All hash values MUST be valid.
Postconditions	None

4.4.7 Test Case LDS_D_07

Purpose	This test checks the signing certificate used to verify the EF.SOD object. The certificate can be read from the SOD object or MUST be retrieved from the PKD.
References	ICAO PKI 1.1 [R2]
Profile	ICAO
Preconditions	Encoded EF.SOD object in binary format as read from the e-Passport. For the verification of the signing certificate signature, the country signing certificate is required.
Test scenario	<ol style="list-style-type: none"> 1. Check the ASN.1 encoding of the signing certificate. 2. Check the signing certificate version element. 3. Check the signature element. 4. Check the certificates validity period element. 5. Check the certificates issuer element. 6. Check the subjectPublicKeyInfo element. 7. Check the AuthorityKeyIdentifier extension in the signing certificate. 8. Check that the SubjectKeyIdentifier extension of the country signing certificate matches the AuthorityKeyIdentifier of the signing certificate. 9. Check the keyUsage extension of the signing certificate. 10. Check the signatureAlgorithm element. 11. Verify the signatureValue of the signing certificate with the public key of the country signing certificate.
Expected Results	<ol style="list-style-type: none"> 1. The object MUST be encoded according to the DER syntax. 2. The version MUST be v3 (Value for v3 is 2). 3. The algorithm specified here MUST match the OID in the signatureAlgorithm field. 4. It MUST use UTC time until 2049 from the on GeneralisedTime. NOTE: It is not necessary that the certificate is still valid; it MUST only have been valid at signing time, which is tested in LDS_D_5. 5. The issuer MUST match the subject of the provided country signing certificate. 6. This element MUST refer to an algorithm specified in [R2]: RSA, ECDSA, or DSA. 7. This extension MUST be present and MUST contain a keyIdentifier value. 8. AuthorityKeyIdentifier MUST match the SubjectKeyIdentifier of the country signing certificate. 9. The keyUsage extension MUST be 1. 10. The signatureAlgorithm element MUST be one of the algorithms specified in [R2]: RSA, ECDSA, or DSA. 11. The certificate signature MUST be valid.

RF protocol and application test standard for e-Passport - part 3

Version : 0.9

Date : Mar 17, 2006

Postconditions	None
----------------	------