For Publication on the ICAO Website

TECHNICAL REPORT

Radio Frequency and Protocol Testing

Part 4

Conformity Test for Inspection Systems

DISCLAIMER: All reasonable precautions have been taken by ICAO to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied; nor does it necessarily represent the decisions or policies of ICAO. The responsibility for the interpretation and use of the material contained or referred to in this publication lies with the reader and in no event shall ICAO be liable for damages arising from reliance upon or use of the same. This publication shall not be considered as a substitute for the government policies or decisions relating to information contained in it. This publication contains the collective views of an international group of experts, believed to be reliable and accurately reproduced at the time of printing. Nevertheless, ICAO does not assume any legal liability or responsibility for the accuracy or completeness of the views expressed by the international group of experts.

Version 2.11

March 2018

File: WP-x Appendix A – TR_RF_and_Protocol_Testing_Part 4_V2.11.docx

Author: ISO/IEC JTC1 SC17 WG3/TF4R

Contents

Introduction

An essential element of ICAO compliant MRTDs is the addition of a Secure Contactless Integrated Circuit (SCIC) that will securely hold biometric data of the MRTD bearer within the ICAO defined Logical Data Structure (LDS).

Successful integration of the SCIC into the MRTD and the integration of a PCD into an inspection system depend upon active international cooperation between many companies and organisations.

The MRTD and the inspection system have been specified and designed to operate interoperable across a wide variety of infrastructures worldwide. The risk profile for the MRTD and the inspection system indicate a high impact if that design includes a widespread error or fault. Therefore it is essential that all companies and organisations involved make all reasonable efforts to minimise the probability that this error or fault is undetected before the design is approved and inspection systems are issued.

Information technology — Test methods for inspection systems for machine readable travel documents (MRTD) — Part 4: Test methods for inspection systems

1 Scope

This document specifies a test plan to verify the application part of the inspection system. The tests comprise

- Basic Access Control
- PACE
- Secure Messaging
- Active Authentication
- Chip Authentication v1
- Handling of the LDS including Passive Authentication.

This test plan consists of two separate parts. Layer 6 defines tests for the application protocol data units (APDUs) based on [ISO/IEC 7816-4] sent by the inspection system application and the correct processing of the corresponding MRTD responses. Layer 7 verifies the correct processing of the logical data structure read from the MRTD.

This test plan is designed to be applicable to existing inspection systems in the marketplace. The tests specified herein are technically feasible, especially the functionality of the lower tester, which is the main test tool to verify the reader's application. The test cases are formulated in such a way that they are independent of any specific system design or implementation.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10373-6:2011, *Identification cards — Test methods — Part 6: Proximity cards*

ISO/IEC 9796-2:2010, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

ISO/IEC 3166:2013, *Codes for the representation of names of countries and their subdivisions*

ISO/IEC 19794-5:2005, *Information technology — Biometric data interchange formats — Part 5: Facial image data*

ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ICAO TR - RF and Protocol Testing Part 4 V2.11, Conformity test for inspection systems

ICAO Doc9303-3 Seventh Edition 2015, *International Civil Aviation Organization, Machine Readable Travel Documents, Part 3: Specifications Common to all MRTDs*

ICAO Doc9303-10 Seventh Edition 2015, *International Civil Aviation Organization, Machine Readable Travel Documents, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)*

ICAO Doc9303-11 Seventh Edition 2015, *International Civil Aviation Organization, Machine Readable Travel Documents, Part 11: Security Mechanisms for MRTDs*

ICAO Doc9303-12 Seventh Edition 2015, *International Civil Aviation Organization, Machine Readable Travel Documents, Part 12: Public Key Infrastructure (PKI) for MRTDs*

3 Terms and definitions

3.1 Abbreviations

AA	Active authentication
APDU	Application protocol data unit
BAC	Basic access control
BHT	Biometric header template
BIT	Biometric information template
BIGT	Biometric information group template
CA	Chip Authentication
CAM	Chip Authentication Mapping
CAN	Card Access Number
C-APDU	Command APDU
DGPM	Data Group Presence Map
DH	Diffie-Hellman
DUT	Device under test
EAC	Extended Access Control
ECAD	Encrypted Chip Authentication Data
ECC	Elliptic curve cryptography
ECDH	Elliptic curve Diffie-Hellman
ECDSA	Elliptic curve digital signature algorithm
FIB	Facial information block
FRH	Facial record header
ICAO	International Civil Aviation Organization
IIB	Image information block
IS	Inspection system
LDS	Logical Data Structure
LT	Lower tester

MRZ	Machine readable zone
OID	Object identifier
PA	Passive authentication
PACE	Password Authenticated Connection Establishment
PCD	Proximity coupling device
PICC	Proximity integrated circuit card
R-APDU	Response APDU
RSA	Rivest-Shamir-Adleman
SHA	Secure hash algorithm
SIP	Standard Inspection Procedure
SM	Secure messaging
SOD	Document Security Object
SSC	Send sequence counter
UT	Upper tester

4 Test environment

In order to define an appropriate test setup, this test plan follows the concept of an upper and a lower tester – UT and LT – as specified in [ISO/IEC 10373-6]. These two interfaces are needed because the inspection system initiates and controls the communication sequence. The following figure 1 illustrates this concept.

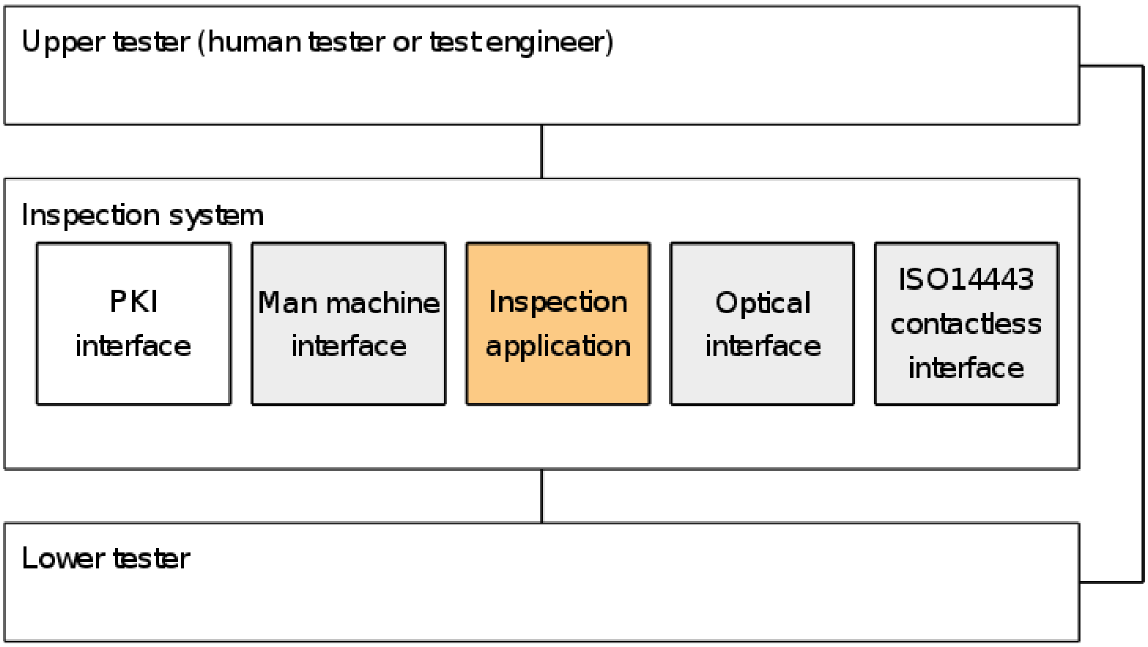

Figure 1: Upper and lower tester of the test environment

Until an upper test interface to trigger the test procedure cannot be assumed, the upper tester is replaced by a human tester – the test engineer. The test engineer manually starts the tests by placing the lower tester in or onto the inspection system.

The lower tester mainly replaces the MRTD. It simulates an MRTD. In order to perform all specified test cases, the lower tester MUST provide the functional elements shown in the following figure 2.

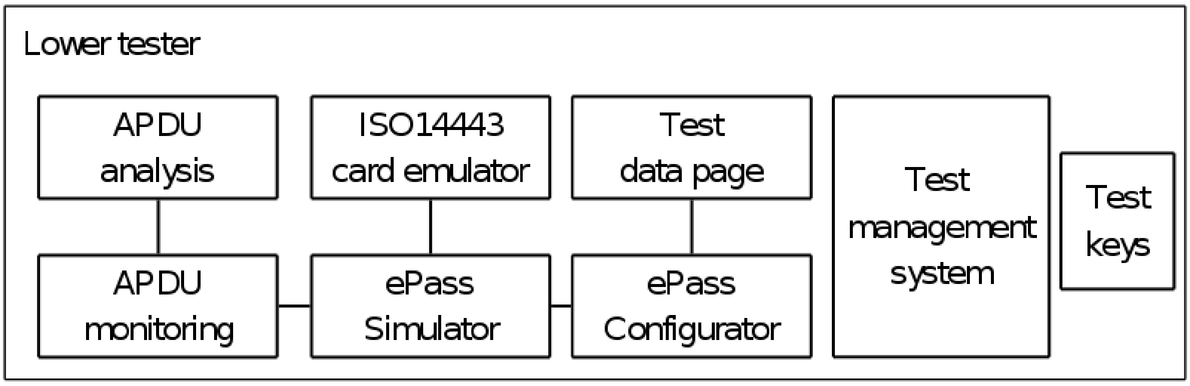

Figure 2: Functional components of the lower tester

First of all, the lower tester MAY provide a test data page that contains the test data specified in this test plan. All information MUST be printed in machine readable format. Especially the MRZ SHALL be printed in OCR-B1 according to [ICAO Doc9303-3]. Moreover, the test data page MAY contain the antenna of the ISO14443 card emulator.

This emulator SHALL be compliant with ISO14443 type A or type B communication. The lower tester SHALL process received C-APDU and return the R-APDU to the inspection system. The ISO14443 card emulator MAY log the communication as specified in [ISO/IEC 10373-6]. It SHOULD be able to process bit rates of 424 bit/sec in both directions. When all steps of a test case are done, the LT stops all communication.

The MRTD simulator simulates the application of a BAC/PACE protected MRTD. It SHALL be capable of processing each C-APDU that it receives. It SHALL support different configurations with respect to the following features:

- Configurable [ISO/IEC 7816-4] file system (number and size of files) to store the data groups
- Large transparent file as specified in [ISO/IEC 7816-4] with size larger than 32k.
- The ISO/IEC 7816-4 application commands defined by [ICAO Doc9303-10].
- BAC and PACE with ISO secure messaging
- Failure simulation as defined in test definitions.

The MRTD configurator sets the configuration of the MRTD simulator according to the data sets defined for each test case. A configuration consists of the layer 6 specifications – the MRTD application profile – and the layer 7 data groups – the MRTD personalization profile.

The lower tester MUST be able to monitor the communication at the application protocol level. It MUST provide appropriate log files of the communication of each test case performed. Moreover, it SHALL be capable of analysing each C-APDU received for correct syntax. The logging itself is only used for further analysis of failures.

The lower tester SHOULD also consist of a test management system to manage and run test cases and test results. The functionality of such a test management system however is not in the scope of this specification.

4.1 Test automation and transfer interface

In general, the test cases will be performed manually. For enhanced testing purpose it is possible to add an optional transfer interface to the test object. The test object MAY provide such a test interface for testing purposes only. It MAY be deactivated for the real products.[1]

5 Implementation conformance statement

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

A tested inspection system SHALL be assigned to the supported profiles in the implementation conformance statement, and a test SHALL only be performed if the inspection system belongs to this profile.

The profile “standard inspection procedure (SIP)” contains the mandatory feature set for compliant inspection systems. Therefore, this profile and its tests are mandatory for all inspection system. To define a better granularity of test cases, the following table shows a list of test profiles.

Table 1 — Profiles to be tested for specified inspection system

Profile-ID	***Profile***	***Description***
SIP	Standard inspection procedure	The inspection system is capable of reading MRTDs that are unprotected (plain) or that support BAC/PACE. It verifies the authenticity of the information retrieved from the MRTD using Passive Authentication.
CAM	PACE with Chip Authentication Mapping	The inspection system is capable of performing PACE with Chip Authentication Mapping if the MRTD supports that.
CA	Chip Authentication	The inspection system is able to perform Chip Authentication if the MRTD supports this.
CAN	CAN Support	The inspection system is able to perform the SIP with CAN if MRTD supports this.
AA	Active Authentication	The inspection system performs Active Authentication when available on an MRTD.
AA_B4	Active Authentication including B.4	The inspection system performs Active Authentication including the signature generation scheme specified in [ISO/IEC 9796-2] paragraph B.4.
DG1	Verification of the encoding of DG1	The inspection system performs checks on the ASN-1 encoding of the retrieved data group 1. These checks

[1] See [1] or [2] (Annex 8.1) for possible implementations and details.

Profile-ID	*Profile*	*Description*
		comprise the presence for required tags according to LDS1.7 and the usage of correct lengths in DER.
DG2	Verification of the encoding of DG2	The inspection system performs checks on the ASN-1 encoding of the retrieved data group 2. These checks comprise the presence for required tags according to LDS1.7 and the usage of correct lengths in DER.
ISO19794-5	Verification of ISO/IEC 19794-5 information	The inspection system performs checks on the format of the face image data as specified in [ISO/IEC 19794-5]

The applicant SHALL fill in the following implementation conformance statement.

Table 2 — Implementation conformance table to be filled in by applicants

Information for test setup	**Profile-ID**	**Applicant declaration**
IS supports standard inspection procedure (mandatory)	SIP	
IS supports PACE with CAM	CAM	
IS supports Chip Authentication	CA	
IS supports SIP with CAN	CAN	
IS supports Active Authentication	AA	
IS supports Active Authentication including B.4	AA_B4	
IS performs checks on DG1 contents.	DG1	
IS performs checks on DG2 contents.	DG2	
IS verifies [ISO/IEC 19794-5] information in DG2.	ISO19794-5	

6 Definition of configuration set

While “<” or “0” may be allowed for 43rd digit in 2nd line of MRZ test data according to [ICAO Doc 9303-3], this conformity test uses only “<”.

6.1 Configuration of default plain MRTD

ID		CFG.DFLT.PLAIN
Purpose		This configuration defines a default plain MRTD.
DF.MRTD		Access conditions: select always
	EF.COM	LDS Version 1.7, Unicode version 4.0.0, Data groups present: 61, 75
		Access conditions: read and select always
	EF.SOD	LDS security object containing hash values of DG1 and DG2 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD

		Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit CSCA and DS are based on RSASSA-PSS with SHA256
		Access conditions: read and select always
	EF.DG1	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4
		Access conditions: read and select always
	EF.DG2	Facial Image 2 (see 6.6.2): JPEG2000 of Erika Mustermann
		Access conditions: read and select always
Data page MRZ		P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4

6.2 Configuration of default BAC protected MRTD

ID		CFG.DFLT.BAC
Purpose		This configuration defines a default BAC protected MRTD.
DF.MRTD		Access conditions: select always
	EF.COM	LDS Version 1.7, Unicode version 4.0.0, Data groups present: 61, 75
		Access conditions: read and select with BAC
	EF.SOD	LDS security object containing hash values of DG1 and DG2 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with BAC
	EF.DG1	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4
		Access conditions: read and select with BAC
	EF.DG2	Facial Image 2 (see 6.6.2): JPEG2000 of Erika Mustermann
		Access conditions: read and select with BAC
Data page MRZ		P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4

6.3 Configuration of default PACE protected MRTD

ID	CFG.DFLT.PACE
Purpose	This configuration defines a default PACE protected MRTD.
EF.CardAccess	one PACEInfo: protocol: id-PACE-ECDH-GM-3DES-CBC-CBC version: 2 parameterId: 13

		Access conditions: read and select always
DF.MRTD		Access conditions: select with PACE
	EF.COM	LDS Version 1.7, Unicode version 4.0.0, Data groups present: 61, 75, 6E
		Access conditions: read and select with PACE
	EF.SOD	LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

	EF.DG1	`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<`
		`C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4`

		Access conditions: read and select with PACE
	EF.DG2	Facial Image 2 (see 6.6.2): JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE
	EF.DG14	Content of EF.CardAccess
		Access conditions: read and select with PACE

Data page MRZ		`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<`
		`C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4`

6.4 Configuration of default PACE and AA MRTD

ID		CFG.DFLT.PACEAA
Purpose		This configuration defines a default PACE protected MRTD with Active Authentication.
EF.CardAccess		one PACEInfo: protocol: id-PACE-ECDH-GM-3DES-CBC-CBC version: 2 parameterId: 13
		Access conditions: read and select always
DF.MRTD		Access conditions: select with PACE
	EF.COM	LDS Version 1.7, Unicode version 4.0.0, Data groups present: 61, 6E, 6F, 75
		Access conditions: read and select with PACE
	EF.SOD	LDS security object containing hash values of DG1, DG2, DG14 and DG15 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

	EF.DG1	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4
		Access conditions: read and select with PACE
	EF.DG2	Facial image 2 (see 6.6.2): JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE
	EF.DG14	Content of EF.CardAccess
		Access conditions: read and select with PACE
	EF.DG15	Signature algorithm: RSA with SHA1
		Access conditions: read and select with PACE
Data page MRZ		P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4

6.5 Configuration of default EAC MRTD

ID		CFG.DFLT.EAC
Purpose		This configuration defines a default PACE protected MRTD with Chip Authentication as part of EAC.
EF.CardAccess		one PACEInfo: protocol: id-PACE-ECDH-GM-3DES-CBC-CBC version: 2 parameterId: 13
		Access conditions: read and select always
DF.MRTD		Access conditions: select with PACE
	EF.COM	LDS Version 1.7, Unicode version 4.0.0, Data groups present: 61, 6E, 6F, 75
		Access conditions: read and select with PACE
	EF.SOD	LDS security object containing hash values of DG1, DG2, DG14 and DG15 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE
	EF.DG1	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4
		Access conditions: read and select with PACE
	EF.DG2	Facial image 2 (see 6.6.2): JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE
	EF.DG14	Key agreement algorithm: id-CA-ECDH-3DES-CBC-CBC Key reference: none
		Access conditions: read and select with PACE

	EF.DG15	Signature algorithm: RSA with SHA1
		Access conditions: read and select with PACE
Data page MRZ		P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4

6.6 Configuration of default PACE-CAM protected MRTD

ID		CFG.DFLT.PACE.CAM
Purpose		This configuration defines a PACE-CAM protected MRTD.
EF.CardAccess		Two PACEInfos: protocol: id-PACE-ECDH-GM-3DES-CBC-CBC protocol: id-PACE-ECDH-CAM-AES-CBC-CMAC-128
		Access conditions: read and select always
EF.CardSecurity		SecurityInfo containing - ChipAuthenticationPublicKeyInfo as required for PACE-CAM, - SecurityInfos contained in EF.CardAccess
		Access conditions: read and select with PACE
DF.MRTD		Access conditions: select with PACE
	EF.COM	LDS Version 1.7, Unicode version 4.0.0, Data groups present: 61, 75, 6E
		Access conditions: read and select with PACE
	EF.SOD	LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE
	EF.DG1	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4
		Access conditions: read and select with PACE
	EF.DG2	Facial Image 2 (see 6.6.2): JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE
	EF.DG14	Content of EF.CardAccess
		Access conditions: read and select with PACE
Data page MRZ		P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4

6.7 Definition of biometric data

6.7.1 Facial image 1

Facial Image 1: JPEG of Erika Mustermann

Biometric Header Template

- Biometric type '00 00 02'
- Format owner '01 01'
- Format type '00 08'

The CBEFF header SHALL not contain further tags.

Biometric data block

- Number of feature points set to 0
- Gender set to unspecified, value '00'
- Eye colour set to unspecified, value '00'
- Hair colour set to unspecified, value '00'
- Feature mask set to unspecified, value '00 00 00'
- Expression set to unspecified, value '00'
- Pose angles set to unspecified, value '00'
- Pose angles uncertainties set to unspecified, value '00'
- Face image type set to "full frontal" encoded as "01"
- Image data type set to "JPEG" encoded as "00"
- Height and width set to the actual value of the JPEG image

6.7.2 Facial image 2

Facial Image 2: JPEG2000 of Erika Mustermann

Biometric Header Template

- Biometric type '00 00 02'
- Format owner '01 01'
- Format type '00 08'

The CBEFF header SHALL not contain further tags.

Biometric data block

- Number of feature points set to 0
- Gender set to unspecified, value '00'
- Eye colour set to unspecified, value '00'
- Hair colour set to unspecified, value '00'
- Feature mask set to unspecified, value '00 00 00'
- Expression set to unspecified, value '00'
- Pose angles set to unspecified, value '00'
- Pose angles uncertainties set to unspecified, value '00'
- Face image type set to "full frontal" encoded as '01'

- Image data type set to "JPEG2000" encoded as '01'
- Height and width set to the actual value of the JPEG2000 image

6.7.3 Facial image 3

Facial Image 3: JPEG2000 of Erika Mustermann

As facial image 2 but with a higher resolution so that the size of the image is greater than 32 KBytes.

6.7.4 Facial image 4

Facial Image 4: JPEG2000 of Erika Mustermann

As facial image 2 but with the JPEG2000 image including header is cut to the first 200 bytes image.

6.7.5 Facial image 5

Facial Image 5: JPEG2000 of Erika Mustermann

As facial image 2 but with 2 additional feature points for the middle of the eyes.

7 Layer 6 tests (Application protocol tests)

7.1 Unit ISO7816_A: Test of Application Selection

7.1.1 ISO7816_A_01: Positive test with unprotected MRTD

Test - ID	ISO7816_A_01
Purpose	This test verifies that the test object can successfully read an unprotected MRTD. Perform standard inspection procedure and read data groups from the lower tester.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PLAIN is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

7.1.2 ISO7816_A_02: Positive test with BAC MRTD

Test - ID	ISO7816_A_02
Purpose	This test verifies that the test object can successfully read a BAC protected MRTD. Perform standard inspection procedure and read data groups from the lower tester.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC is loaded into the LT. • IS is „ready“.

Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

7.1.3 ISO7816_A_03: Positive test with PACE MRTD

Test - ID	ISO7816_A_03
Purpose	This test verifies that the test object can successfully read a PACE protected MRTD. Perform standard inspection procedure and read data groups from the lower tester.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

7.1.4 ISO7816_A_04: Application selection failure (BAC)

Test - ID	ISO7816_A_04
Purpose	This test verifies that the test object recognizes BAC MRTDs which contain an invalid ICAO AID.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC is loaded into the LT with the following modification: The installed ICAO application has an invalid AID (e.g. 'A0 00 00 02 47 10 0**F**') • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. The LT does have an installed ICAO application with an invalid AID (e.g. 'A0 00 00 02 47 10 0**F**'). It responds with the checking error '6A 82'; application is not found.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

7.1.5 ISO7816_A_05: Application selection failure (PACE)

Test - ID	ISO7816_A_05
Purpose	This test verifies that the test object recognizes PACE MRTDs which contain an invalid ICAO AID.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT with the

	following modification: The installed ICAO application has an invalid AID (e.g. 'A0 00 00 02 47 10 0**F**') • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. The LT does have an installed ICAO application with an invalid AID (e.g. 'A0 00 00 02 47 10 0**F**'). It responds with the checking error '6A 82'; application is not found.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

7.2 Unit ISO7816_B: Test of Basic Access Control

7.2.1 ISO7816_B_01: Mutual authentication MAC failure

Test - ID	ISO7816_B_01
Purpose	This test verifies that an inspection system recognized an authentication failure of an MRTD (internal authentication). Perform standard inspection procedure and read BAC protected data groups from the lower tester. The test object SHALL NOT read the data groups.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC is loaded into the LT. • Modification: the MUTUAL AUTHENTICATE command SHALL use a manipulated K_{MAC} – last byte of the K_{MAC} increased by 2 – to compute the MAC for the response. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. The LT introduces a failure in the response of the MUTUAL AUTHENTICATE command. The MAC returned in the response APDU has an incorrect value. MAC verification in the IS MUST fail.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

7.2.2 ISO7816_B_02: Mutual authentication encryption failure

Test - ID	ISO7816_B_02
Purpose	This test verifies that an inspection system recognized an authentication failure of an MRTD (internal authentication). Perform standard inspection procedure and read BAC protected data groups from the lower tester. The test object SHALL NOT read the data groups.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC is loaded into the LT. • Modification: the MUTUAL AUTHENTICATE command SHALL use a manipulated K_{ENC} – last byte of the K_{ENC} increased by 2 – to compute the cryptogram for the response. • IS is „ready“.

Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. The LT introduces a failure in the response of the MUTUAL AUTHENTICATE command. The cryptogram returned in the response APDU has an incorrect value. The IS can't successfully verify that this cryptogram contains the challenge RND.IFD sent by the IS.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

7.2.3 ISO7816_B_03: Mutual authentication failure

Test - ID	ISO7816_B_03
Purpose	This test verifies that an inspection system recognizes an authentication failure of an MRTD (external authentication). Perform standard inspection procedure and read BAC protected data groups from the lower tester. The test object SHALL NOT read the data groups.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC is loaded into the LT. • The BAC keys K_{ENC} and K_{MAC} SHALL generated from manipulated DG1 data. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. The LT uses wrong BAC keys. The MUTUAL AUTHENTICATE command detects an authentication failure and returns warning processing SW '63 00' (Authentication failure)
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

7.2.4 Positive test with BAC MRTD and three line MRZ

Test - ID	ISO7816_B_04
Purpose	This test verifies that the test object can successfully read a BAC protected MRTD with a three line MRZ. Perform standard inspection procedure and read data groups from the lower tester.
Version	2.11
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG. BAC.ISO7816.B04 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID	CFG.BAC.ISO7816.B04
Purpose	This configuration is based on CFG.DFLT.BAC. The following files are

	modified as specified below. The MRZ includes three lines.
Data page MRZ	P<D<<C11T002JM4<<<<<<<<<<<<<<< 9608122F2310314D<<<<<<<<<<<<<4 MUSTERMANN<<ERIKA<<<<<<<<<<<<<
EF.DG1	EF.DG1 must be encoded as TD1 size MRZ.

7.3 Unit ISO7816_C: Test of PACE protocol

This unit checks the PACE implementation of an Inspection System. An Inspection System that support PACE and BAC SHOULD always first try to perform PACE (see [ICAO Doc9303-11]).

Note: According to [ICAO Doc9303-11] states MUST NOT implement PACE without implementing BAC if interoperability is required. Inspection systems which are able to perform PACE SHALL be able perform this test unit with "PACE only profile". Therefore, to ensure that PACE will be performed, the LT SHALL deny the selection of the eMRTD-Application in all test cases by returning SW '69 82' until PACE performed successful. Starting January 1st 2018 eMRTDs that implement PACE, but not BAC, are compliant to [ICAO Doc9303-11].

By default the test cases in this unit will be performed with MRZ, but the test lab can choose to use the CAN if entering the MRZ is difficult (e.g. mobile readers).

The vendor of inspection systems supporting PACE-CAM must provide a way to perform PACE-CAM explicitly. This function is needed to force the inspection system to use PACE-CAM and must be used in all test cases using PACE-CAM (profile: CAM).

7.3.1 ISO7816_C_01: Correct execution of PACE protocol

Test - ID	ISO7816_C_01_template
Purpose	Check correct execution of PACE protocol in the terminal. The test is executed with CAN and/or MRZ.
Version	2.11
References	[ICAO Doc9303-11]
Profile	See Table 3
Preconditions	• Configuration profile CFG.DFLT.PACE (in case of ISO7816_C_01c: CFG.PACE.ISO7816.C01) is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	1. - 2. MSE:Set AT command contains DO83 with value as defined in Table 3. DO80 contains valid PACE protocol OID as provided in EF.CardAccess. The inspection procedure SHALL be successful.

Table 3 — Test case ISO7816_C_01

Test- ID	***Profiles***	***Password***	***<DO83>***

ISO7816_C_01a	SIP	Use PACE with MRZ	'01'
ISO7816_C_01b	SIP, CAN	Use PACE with CAN	'02'
ISO7816_C_01c	SIP	Use PACE with three line MRZ as specified in the following table	‘01’

ID	CFG.PACE.ISO7816.C01
Purpose	This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The MRZ includes three lines.
Data page MRZ	P<D<<C11T002JM4<<<<<<<<<<<<<<< 9608122F2310314D<<<<<<<<<<<<<4 MUSTERMANN<<ERIKA<<<<<<<<<<<<<
EF.DG1	EF.DG1 must be encoded as TD1 or TD2 MRZ: ISO7816_C_01a: TD2 ISO7816_C_01b: TD2 ISO7816_C_01c: TD1

7.3.2 ISO7816_C_02: Check supported standardized Domain Parameters with Generic Mapping

Test - ID	ISO7816_C_02_template
Purpose	Check correct execution of PACE protocol in the test object. The test has to be executed for each PACE Domain Parameters in table 4. This test case is only rated as a PASS if all passes are completed successfully. The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • In EF.CardAccess use exact one PACEInfo with standardized domain parameter and protocol as defined in Table 4. Don't use a PACEDomainParameterInfo within EF.CardAccess. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	1. - 2. MSE:Set AT command contains DO83 with value '01' or '02'. DO80 contains valid PACE protocol OID as provided in EF.CardAccess. The inspection procedure SHALL be successful.

Table 4 — Test case ISO7816_C_02

Test - ID	***Domain Parameter***	***parameterId***	***Mapping***	***Protocol***

Test - ID	*Domain Parameter*	*parameterId*	*Mapping*	*Protocol*
ISO7816_C_02a	1024-bit MODP Group with 160-bit Prime Order Subgroup	0	GM	id-PACE-DH-GM-3DES-CBC-CBC
ISO7816_C_02b	2048-bit MODP Group with 224-bit Prime Order Subgroup	1	GM	id-PACE-DH-GM-3DES-CBC-CBC
ISO7816_C_02c	2048-bit MODP Group with 256-bit Prime Order Subgroup	2	GM	id-PACE-DH-GM-3DES-CBC-CBC
ISO7816_C_02d	NIST P-192 (secp192r1)	8	GM	id-PACE-ECDH-GM-3DES-CBC-CBC
ISO7816_C_02e	NIST P-224 (secp224r1)	10	GM	id-PACE-ECDH-GM-3DES-CBC-CBC
ISO7816_C_02f	NIST P-256 (secp256r1)	12	GM	id-PACE-ECDH-GM-3DES-CBC-CBC
ISO7816_C_02g	NIST P-384 (secp384r1)	15	GM	id-PACE-ECDH-GM-3DES-CBC-CBC
ISO7816_C_02h	NIST P-521 (secp521r1)	18	GM	id-PACE-ECDH-GM-3DES-CBC-CBC
ISO7816_C_02i	BrainpoolP192r1	9	GM	id-PACE-ECDH-GM-3DES-CBC-CBC
ISO7816_C_02j	BrainpoolP224r1	11	GM	id-PACE-ECDH-GM-3DES-CBC-CBC
ISO7816_C_02k	BrainpoolP256r1	13	GM	id-PACE-ECDH-GM-3DES-CBC-CBC
ISO7816_C_02l	BrainpoolP320r1	14	GM	id-PACE-ECDH-GM-3DES-CBC-CBC
ISO7816_C_02m	BrainpoolP384r1	16	GM	id-PACE-ECDH-GM-3DES-CBC-CBC
ISO7816_C_02n	BrainpoolP512r1	17	GM	id-PACE-ECDH-GM-3DES-CBC-CBC

7.3.3 ISO7816_C_03: Check supported standardized Domain Parameters with Integrated Mapping

Test - ID	ISO7816_C_03_template
Purpose	Check correct execution of PACE protocol in the test object. The test has to be executed for each PACE Domain Parameters in table 5. This test case is only rated as a PASS if all passes are completed successfully. The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP

Preconditions	- Configuration profile CFG.DFLT.PACE is loaded into the LT. - In EF.CardAccess use exact one PACEInfo with standardized domain parameter and protocol as defined in Table 5. Don't use a PACEDomainParameterInfo within EF.CardAccess. - Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	1. - 2. MSE:Set AT command contains DO83 with value '01' or '02'. DO80 contains valid PACE protocol OID as provided in EF.CardAccess. The inspection procedure SHALL be successful.

Table 5 — Test case ISO7816_C03

Test - ID	***Domain Parameter***	***parameterId***	***Mapping***	***Protocol***
ISO7816_C_03a	1024-bit MODP Group with 160-bit Prime Order Subgroup	0	IM	id-PACE-DH-IM-3DES-CBC-CBC
ISO7816_C_03b	2048-bit MODP Group with 224-bit Prime Order Subgroup	1	IM	id-PACE-DH-IM-3DES-CBC-CBC
ISO7816_C_03c	2048-bit MODP Group with 256-bit Prime Order Subgroup	2	IM	id-PACE-DH-IM-3DES-CBC-CBC
ISO7816_C_03d	NIST P-192 (secp192r1)	8	IM	id-PACE-ECDH-IM-3DES-CBC-CBC
ISO7816_C_03e	NIST P-256 (secp256r1)	12	IM	id-PACE-ECDH-IM-3DES-CBC-CBC
ISO7816_C_03f	NIST P-384 (secp384r1)	15	IM	id-PACE-ECDH-IM-3DES-CBC-CBC
ISO7816_C_03g	NIST P-521 (secp521r1)	18	IM	id-PACE-ECDH-IM-3DES-CBC-CBC
ISO7816_C_03h	BrainpoolP192r1	9	IM	id-PACE-ECDH-IM-3DES-CBC-CBC
ISO7816_C_03i	BrainpoolP224r1	11	IM	id-PACE-ECDH-IM-3DES-CBC-CBC
ISO7816_C_03j	BrainpoolP256r1	13	IM	id-PACE-ECDH-IM-3DES-CBC-CBC
ISO7816_C_03k	BrainpoolP320r1	14	IM	id-PACE-ECDH-IM-3DES-CBC-CBC
ISO7816_C_03l	BrainpoolP384r1	16	IM	id-PACE-ECDH-IM-3DES-CBC-CBC
ISO7816_C_03m	BrainpoolP512r1	17	IM	id-PACE-ECDH-IM-3DES-CBC-CBC

7.3.4 ISO7816_C_04: Check supported algorithms

Test - ID	ISO7816_C_04_template
Purpose	Check correct execution of PACE protocol in the test object. The test has to be executed for each PACE algorithm specified in [ICAO Doc9303-11]. This test case is only rated as a PASS if all passes are completed successfully. The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP, *(CAM)*
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • If IS supports profile CAM use two PACEInfo (one for PACE-CAM and one for PACE-GM/PACE-IM) with standardized domain parameter in EF.CardAccess. Else use only one PACEInfo for PACE-GM/PACE-IM. Don't use a PACEDomainParameterInfo within EF.CardAccess. Use the OID from Table 6 as protocol in PACEInfo. The DomainParameters SHALL be consistent with the used algorithm (DH or ECDH) and SHOULD be the same for each test run that uses the same algorithm (DH or ECDH) • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	1. - 2. MSE:Set AT command contains DO83 with value '01' or '02'. DO80 contains valid PACE protocol OID as provided in EF.CardAccess. The inspection procedure SHALL be successful. **If EF.CardAccess contains PACEInfo for PACE-CAM but the IS selects PACE-GM or PACE-IM, the result of this test case is inconclusive.**

Table 6 — Test case ISO7816_C_04

Test - ID	***Algorithm OID***
ISO7816_C_04a	id-PACE-DH-GM-3DES-CBC-CBC
ISO7816_C_04b	id-PACE-DH-GM-AES-CBC-CMAC-128
ISO7816_C_04c	id-PACE-DH-GM-AES-CBC-CMAC-192
ISO7816_C_04d	id-PACE-DH-GM-AES-CBC-CMAC-256
ISO7816_C_04e	id-PACE-DH-IM-3DES-CBC-CBC
ISO7816_C_04f	id-PACE-DH-IM-AES-CBC-CMAC-128
ISO7816_C_04g	id-PACE-DH-IM-AES-CBC-CMAC-192
ISO7816_C_04h	id-PACE-DH-IM-AES-CBC-CMAC-256
ISO7816_C_04i	id-PACE-ECDH-GM-3DES-CBC-CBC
ISO7816_C_04j	id-PACE-ECDH-GM-AES-CBC-CMAC-128
ISO7816_C_04k	id-PACE-ECDH-GM-AES-CBC-CMAC-192
ISO7816_C_04l	id-PACE-ECDH-GM-AES-CBC-CMAC-256

Test - ID	*Algorithm OID*
ISO7816_C_04m	id-PACE-ECDH-IM-3DES-CBC-CBC
ISO7816_C_04n	id-PACE-ECDH-IM-AES-CBC-CMAC-128
ISO7816_C_04o	id-PACE-ECDH-IM-AES-CBC-CMAC-192
ISO7816_C_04p	id-PACE-ECDH-IM-AES-CBC-CMAC-256
ISO7816_C_04q	id-PACE-ECDH-CAM-AES-CBC-CMAC-128 (only applicable if IS supports profile CAM)
ISO7816_C_04r	id-PACE-ECDH-CAM-AES-CBC-CMAC-192 (only applicable if IS supports profile CAM)
ISO7816_C_04s	id-PACE-ECDH-CAM-AES-CBC-CMAC-256 (only applicable if IS supports profile CAM)

7.3.5 ISO7816_C_05: PACE with additional entries in SecurityInfos

Test – ID	ISO7816_C_05
Purpose	Positive test with PACE with additional entries in SecurityInfos which should be ignored by the IS.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Use exact one PACEInfo with standardized domain parameter in EF.CardAccess. Don't use a PACEDomainParameterInfo within EF.CardAccess. **Use additional incorrect SecurityInfo entry:** protocol: id-PACE version: 2 parameterId: none. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	1. - 2. MSE:Set AT command contains DO83 with value '01' or '02'. DO80 contains valid PACE protocol OID as provided in EF.CardAccess. The inspection procedure SHALL be successful.

7.3.6 ISO7816_C_06: Check selection of standardized Domain Parameters and algorithms

Test - ID	ISO7816_C_06
Purpose	Check correct execution of PACE protocol in the test object, if LT supports several algorithms for PACE. The test is executed with the MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP

Preconditions	- Configuration profile CFG.DFLT.PACE is loaded into the LT with following modifications: - Use three different PACEInfo objects in EF.CardAccess with different algorithms and different standardized domain parameters. The algorithms and domain parameters are free to choose for each test run but MUST be valid parameters as described in [ICAO Doc9303-11]. Don't use PACEDomainParameterInfo objects within EF.CardAccess. - Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01' or '02' DO84 with parameterId from one of the PACEInfo objects The inspection procedure SHALL be successful.

7.3.7 ISO7816_C_07: EF.CardAccess contains two PACEInfo and PACEDomainParameterInfo

Test - ID	ISO7816_C_07
Purpose	Positive test with EF.CardAccess containing two PACEInfo and one PACEDomainParameterInfo. Check that IS can handle two different PACE parameters and perform one possible option.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	- Configuration profile CFG.DFLT.PACE is loaded into the LT with following modifications: - Use two different PACEInfo objects and one PACEDomainParameterInfo object in EF.CardAccess with different algorithms in PACEInfo. Use one standardized domain parameter identifier (parameterId: between 0 and 2, 8 and 18) in the first PACEInfo. In the second PACEInfo the parameterID SHALL indicate proprietary domain parameters (parameterID above 31). The PACEDomainParameterInfo object MUST contain valid parameters. The algorithms and domain parameters MUST be valid parameters as described in [ICAO Doc9303-11]. - Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID DO83 with value '01' for MRZ or '02' for CAN usage DO84 with parameterId from one of the PACEInfo objects The inspection procedure SHALL be successful.

7.3.8 ISO7816_C_08: Abort PACE because of SW error code (MSE:Set AT)

Test - ID	ISO7816_C_08_template
Purpose	Check that test object aborts the PACE protocol when LT returns an error code to the command MSE: Set AT. The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. The LT returns the SW as defined in Table 7 in the response to the MSE:Set AT command. The verification in the test object MUST fail.
Expected results	1. - 2. The inspection procedure MUST be aborted because of SW as defined in Table 7 in response APDU to MSE:Set AT command.

Table 7 — Test case ISO7816_C_08

Test - ID	***Response SW to MSE:Set AT***
ISO7816_C_08a	6A 80
ISO7816_C_08b	6A 88
ISO7816_C_08c	6F 00

7.3.9 ISO7816_C_09: Error on the nonce – Value modification after first General Authenticate

Test – ID	ISO7816_C_09
Purpose	Negative test: Error on the nonce – Value modification after first General Authenticate
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. The LT returns a wrong encrypted nonce (e.g. by incrementing last byte of transmitted nonce by 1 modulo 256) (DO80) in the response to the first General Authenticate command but uses the correct nonce for itself. The LT returns SW '63 00' in response to the General Authenticate (step 4 mutual authentication) command.
Expected results	1. -

	2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST be aborted because of SW '63 00' in response APDU to the General Authenticate (step 4 mutual authentication) command.

7.3.10 ISO7816_C_10: Error on General Authenticate step 1 command

Test – ID	ISO7816_C_10_template
Purpose	Negative test: Error on General Authenticate step 1command
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. The LT returns the SW as defined in Table 8 in response to the General Authenticate (step 1) command.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST be aborted because of the SW as defined in Table 8 in response APDU to General Authenticate (step 1) command.

Table 8 — Test case ISO7816_C_10

Test - ID	***Response SW to General Authenticate step 1***
ISO7816_C_10a	6A 80
ISO7816_C_10b	6F 00

7.3.11 ISO7816_C_11: Error on General Authenticate step 1 command – Bad Tag (use 90h instead of 80h)

Test – ID	ISO7816_C_11
Purpose	Negative test : Error on General Authenticate step 1command – Bad Tag (use 90h instead of 80h)
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.

Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. When LT receives command General Authenticate step 1, LT returns incorrect Tag (90h instead of 80h) for the encrypted nonce in response APDU back to the test object.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST fail after receiving the response APDU to General Authenticate command step 1.

7.3.12 ISO7816_C_12: Error on General Authenticate step 2 command

Test – ID	ISO7816_C_12_template
Purpose	Negative test: Error on General Authenticate step 2command
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. When LT receives command General Authenticate step 2, LT returns the SW as defined in Table 9 in response APDU back to the test object.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST be aborted because of the SW as defined in Table 9 in response APDU to General Authenticate (step 2) command.

Table 9 — Test case ISO7816_C_12

Test - ID	*Response SW to General Authenticate step 2*
ISO7816_C_12a	6A 80
ISO7816_C_12b	6F 00

7.3.13 ISO7816_C_13: Error on General Authenticate step 2 command – Bad Tag (use 92h instead of 82h)

Test – ID	ISO7816_C_13
Purpose	Negative test : Error on General Authenticate step 2 command – Bad Tag (use 92h instead of 82h)

Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. When LT receives command General Authenticate step 2, LT returns incorrect Tag (92h instead of 82h) for the mapping data in response APDU back to the test object.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST fail after receiving the response APDU to General Authenticate command step 2.

7.3.14 ISO7816_C_14: Abort PACE because of error in GA step 2 (GM)

Test - ID	ISO7816_C_14
Purpose	Check that test object aborts PACE when LT transmits incorrect data for mapping function in answer to command GENERAL AUTHENTICATE (step 2) when using generic mapping The test is executed with the MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. When LT receives command GENERAL AUTHENTICATE (Step 2) with Mapping Data (DO81) from the test object, LT sends incorrect (incremented by 1) Mapping data (DO82) in the response APDU back to the test object. It is accepted that the test object aborts protocol execution after receiving the incorrect mapping data. The return codes in the response APDUs of all commands apart from General Authenticate (Step 4) are positive (SW '90 00'). The return code in the response APDU to General Authenticate (Step 4) (if this message is sent) is an error code indicating that the authentication has failed.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01 for MRZ or '02' for CAN usage The inspection procedure MUST fail. The command APDUs for GENERAL AUTHENTICATE step 3 and 4 MAY missing if test object aborts PACE after GENERAL AUTHENTICATE step 2.

7.3.15 ISO7816_C_15: Abort PACE because of error in GA step 2 (IM)

Test - ID	ISO7816_C_15
Purpose	Check that test object aborts PACE when LT transmits incorrect data for mapping function in answer to command GENERAL AUTHENTICATE (step 2) when using integrated mapping. The test is executed with the MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Modification: In EF.CardAccess use one PACEInfo with following parameters: protocol: id-PACE-ECDH-IM-3DES-CBC-CBC version: 2 parameterId: 13 • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. When LT receives command GENERAL AUTHENTICATE (Step 2) with Mapping Data (DO81) from the test object, LT sends incorrect Mapping data (DO82) in the response APDU back to the test object. R-APDU should be: 7C <L7C> 82 08 11 22 33 44 55 66 77 88 90 00 It is accepted that the test object aborts protocol execution after receiving the incorrect mapping data. The return codes in the response APDUs of all commands apart from General Authenticate (Step 4) are positive (SW '90 00'). The return code in the response APDU to General Authenticate (Step 4) (if this message is sent) is an error code indicating that the authentication has failed.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01 for MRZ or '02' for CAN usage The inspection procedure MUST fail. The command APDUs for GENERAL AUTHENTICATE step 3 and 4 MAY missing if test object aborts PACE after GENERAL AUTHENTICATE step 2.

7.3.16 ISO7816_C_16: Error on General Authenticate step 2 command – error on mapping data – All ECDH Public key components

Test – ID	ISO7816_C_16
Purpose	Negative test: Error on General Authenticate step 2 command – error on mapping data – All ECDH Public key components
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP

Preconditions	- Configuration profile CFG.DFLT.PACE is loaded into the LT. - Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. When LT receives command GENERAL AUTHENTICATE (Step 2) with Mapping Data (DO81) from the test object, LT sends incorrect Mapping data (DO82) in the response APDU back to the test object. Mapping data contains the concatenation of the following objects in the given order: Tag 06: OID Tag 81: Prime Tag 82: Coefficient a Tag 83: Coefficient b Tag 84: Base point Tag 85: Order Tag 86: Public point Tag 87: Cofactor It is accepted that the test object aborts protocol execution after receiving the incorrect mapping data. The return codes in the response APDUs of all commands apart from General Authenticate (Step 4) are positive (SW '90 00'). The return code in the response APDU to General Authenticate (Step 4) (if this message is sent) is an error code indicating that the authentication has failed.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST fail. The command APDUs for GENERAL AUTHENTICATE step 3 and 4 MAY missing if test object aborts PACE after GENERAL AUTHENTICATE step 2.

7.3.17 ISO7816_C_17: Error on General Authenticate step 2 command – error on mapping data – All DH public key components

Test – ID	ISO7816_C_17
Purpose	Negative test : Error on General Authenticate step 2 command – error on mapping data – All DH public key components
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	- Configuration profile CFG.DFLT.PACE is loaded into the LT with following modifications. Use EF.CardAccess which contains exact one PACEInfo: protocol: id-PACE-DH-GM-3DES-CBC-CBC version: 2 parameterId: 2 - Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.

	When LT receives command GENERAL AUTHENTICATE (Step 2) with Mapping Data (DO81) from the test object, LT sends incorrect Mapping data (DO82) in the response APDU back to the test object. Mapping data contains the concatenation of the following objects in the given order: Tag 06: OID Tag 81: Prime Tag 82: Order Tag 83: Generator Tag 84: Public value It is accepted that the test object aborts protocol execution after receiving the incorrect mapping data. The return codes in the response APDUs of all commands apart from General Authenticate (Step 4) are positive (SW '90 00'). The return code in the response APDU to General Authenticate (Step 4) (if this message is sent) is an error code indicating that the authentication has failed.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST fail. The command APDUs for GENERAL AUTHENTICATE step 3 and 4 MAY missing if test object aborts PACE after GENERAL AUTHENTICATE step 2.

7.3.18 ISO7816_C_18: Error on General Authenticate step 3 command

Test – ID	ISO7816_C_18_template
Purpose	Negative test: Error on General Authenticate step 3 command
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. When LT receives command General Authenticate step 3, LT returns the SW as defined in Table 10 in response APDU back to the test object.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST be aborted because of the SW as defined in Table 10 in response APDU to General Authenticate (step 3) command.

Table 10 — Test case ISO7816_C_18

Test - ID	*Response SW to General Authenticate step 3*
ISO7816_C_18a	6A 80
ISO7816_C_18b	6F 00

7.3.19 ISO7816_C_19: Error on General Authenticate step 3 command – Bad Tag (use 94h instead of 84h)

Test – ID	ISO7816_C_19
Purpose	Negative test: Error on General Authenticate step 3 command – Bad Tag (use 94 instead of 84h)
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. When LT receives command General Authenticate step 3, LT returns incorrect Tag (94h instead of 84h) for the ephemeral public key in response APDU back to the test object.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST fail after receiving the response APDU to General Authenticate command step 3.

7.3.20 ISO7816_C_20: Abort PACE because of error in GA step 3

Test - ID	ISO7816_C_20
Purpose	Check that the test object aborts PACE when LT transmits an incorrect ephemeral public key in answer to command GENERAL AUTHENTICATE (step 3). The test is executed with the MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. When LT receives command GENERAL AUTHENTICATE (Step 3) with PCD Ephemeral Public Key (DO83) from the test object, LT sends incorrect (incremented by 1) PICC Ephemeral Public Key (DO84) in the response APDU back to the test object. It is accepted that the test object aborts protocol execution after detecting the

	incorrect $PK_{DH,IC}$ in response APDU. The return codes in the response APDUs of all commands apart from General Authenticate (Step 4) are positive (SW '90 00'). The return code in the response APDU to General Authenticate (Step 4) (if this message is sent) is an error code indicating that the authentication has failed.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST fail. The command APDU for GENERAL AUTHENTICATE step 4 MAY missing if test object aborts PACE after GENERAL AUTHENTICATE step 3.

7.3.21 ISO7816_C_21: Error on General Authenticate step 3 command – error on ephemeral public key – All ECDH Public key components

Test – ID	ISO7816_C_21
Purpose	Negative test : Error on General Authenticate step 3 command – error on ephemeral public key - All ECDH Public key components
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. When LT receives command GENERAL AUTHENTICATE (Step 3) with ephemeral public key (DO83) from the test object, LT sends incorrect (all key components instead of only point) ephemeral public key (DO84) in the response APDU back to the test object. Ephemeral public key contains the concatenation of the following objects in the given order: Tag 06: OID Tag 81: Prime Tag 82: Coefficient a Tag 83: Coefficient b Tag 84: Base point Tag 85: Order Tag 86: Public point Tag 87: Cofactor It is accepted that the test object aborts protocol execution after receiving the incorrect ephemeral public key. The return codes in the response APDUs of all commands apart from General Authenticate (Step 4) are positive (SW '90 00'). The return code in the response APDU to General Authenticate (Step 4) (if this message is sent) is an error code indicating that the authentication has failed.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess

	DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST fail. The command APDUs for GENERAL AUTHENTICATE step 4 MAY missing if test object aborts PACE after GENERAL AUTHENTICATE step 3.

7.3.22 ISO7816_C_22: Error on General Authenticate step 3 command – error on ephemeral public key – All DH public key components

Test – ID	ISO7816_C_22
Purpose	Negative test: Error on General Authenticate step 3 command – error on ephemeral public key - All DH public key components
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT with following modifications. Use EF.CardAccess which contains exact one PACEInfo: protocol: id-PACE-DH-GM-3DES-CBC-CBC version: 2 parameterId: 2 • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. When LT receives command GENERAL AUTHENTICATE (Step 3) with ephemeral public key (DO83) from the test object, LT sends incorrect (all key components instead of only public value) ephemeral public key (DO84) in the response APDU back to the test object. Ephemeral public key contains the concatenation of the following objects in the given order: Tag 06: OID Tag 81: Prime Tag 82: Order Tag 83: Generator Tag 84: Public value It is accepted that the test object aborts protocol execution after receiving the incorrect ephemeral public key. The return codes in the response APDUs of all commands apart from General Authenticate (Step 4) are positive (SW '90 00'). The return code in the response APDU to General Authenticate (Step 4) (if this message is sent) is an error code indicating that the authentication has failed.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST fail. The command APDUs for GENERAL AUTHENTICATE step 4 MAY missing if test object aborts PACE after GENERAL AUTHENTICATE step 3.

7.3.23 ISO7816_C_23: Abort PACE because of identical Ephemeral Public Keys

Test ID	ISO7816_C_23
Purpose	Check that the test object aborts PACE if the ephemeral public key $PK_{DH,IC}$ and the ephemeral public key $PK_{DH,PCD}$ transmitted in GENERAL AUTHENTICATE are equal. The test is executed with the MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. When LT receives command GENERAL AUTHENTICATE (Step 3) with PCD Ephemeral Public Key (DO83) from the test object, LT sends the same Ephemeral Public Key (as DO84) in the response APDU back to the test object. The test object MUST abort protocol execution after detecting that $PK_{DH,IC}$ and $PK_{DH,PCD}$ are equal.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST be aborted after receiving response APDU to GENERAL AUTHENTICATE step 3.

7.3.24 ISO7816_C_24: Error on General Authenticate step 4 command

Test – ID	ISO7816_C_24_template
Purpose	Negative test: Error on General Authenticate step 4 command
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. When LT receives command General Authenticate step 4, LT returns the SW as defined in Table 11 in response APDU back to the test object.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST be aborted because of the SW as defined in Table 11 in response APDU to General Authenticate (step 4) command.

Table 11 — Test case ISO7816_C_24

Test - ID	*Response SW to General Authenticate step 4*
ISO7816_C_24a	63 00
ISO7816_C_24b	6A 80
ISO7816_C_24c	6F 00

7.3.25 ISO7816_C_25: Error on General Authenticate step 4 command – Bad Tag (use 96 instead of 86h)

Test – ID	ISO7816_C_25
Purpose	Negative test: Error on General Authenticate step 4 command – Bad Tag (use 96h instead of 86h)
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. When LT receives command General Authenticate step 4, LT returns incorrect Tag (96h instead of 86h) for the authentication token in response APDU back to the test object.
Expected results	1. - 2. MSE:Set AT command MUST contain: DO80 with valid PACE protocol OID as provided in EF.CardAccess DO83 with value '01' for MRZ or '02' for CAN usage The inspection procedure MUST fail after receiving the response APDU to General Authenticate command step 4.

7.3.26 ISO7816_C_26: Abort PACE because of error in GA step 4

Test - ID	ISO7816_C_26
Purpose	Check that the test object aborts PACE protocol when LT returns an incorrect authentication token. The test is executed with the passwords MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. The LT introduces a failure in the response of the GENERAL AUTHENTICATE (step 4) command. The authentication token returned in the response APDU has an incorrect value

	(incremented by 1). The verification in the test object MUST fail.
Expected results	1. - 2. The inspection procedure MUST be aborted after receiving response APDU to GENERAL AUTHENTICATE command (step 4).

7.3.27 ISO7816_C_27: Abort PACE because of TLV error in EF.CardAccess

Test - ID	ISO7816_C_27
Purpose	Check that the test object aborts PACE protocol when LT transmits incorrect PACE parameters (inconsistent data in these parameters). The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. LT sends EF.CardAccess in response APDU to command READ BINARY with the following change: In SecurityInfo PACEInfo change length byte of tag "version" from '01' to '02'. 30 0F 06 0A 04 00 7F 00 07 02 02 04 02 02 02 02 01
Expected results	1. - 2. The test object must abort communication to LT after receiving the inconsistent data in response APDU to READ BINARY. UT receives information from test object about protocol abort.

7.3.28 ISO7816_C_28: Abort PACE because of incorrect parameterId in PACEInfo

Test - ID	ISO7816_C_28
Purpose	Check that the test object aborts PACE protocol when LT transmits incorrect parameterId in PACEInfo. The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT with the following modification: EF.CardAccess contains PACEInfo with parameterId 31 (RFU). • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. LT sends data from EF.CardAccess with standardized domain parameters in PACEInfo in response APDU to command READ BINARY. As parameterId in PACEInfo use a domain parameter identifier which is RFU (e.g. 31).
Expected results	1. -

	2. The command APDUs for MSE: Set AT, General Authenticate (Step 1, 2, 3, 4) SHALL be missing, since the test object must abort communication to LT after receiving the response APDU to READ BINARY. UT receives information from test object about protocol abort.

7.3.29 ISO7816_C_29: PACE-CAM with missing tag 8Ah but correct ECAD

Test - ID	ISO7816_C_29
Purpose	Check that the test object aborts PACE protocol when LT transmits incorrect GENERAL AUTHENTICATE with missing tag 8Ah but correct Encrypted Chip Authentication Data (ECAD). The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP, CAM
Preconditions	• Configuration profile CFG.DFLT.PACE.CAM is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. LT sends no tag 8Ah but correct ECAD in the step 4 of GENERAL AUTHENTICATE
Expected results	1. - 2. The test object must abort communication to LT after receiving the last GENERAL AUTHENTICATE command. UT receives information from test object about protocol abort.

7.3.30 ISO7816_C_30: PACE-CAM with incorrectly encoded ECAD (no octet string)

Test - ID	ISO7816_C_30
Purpose	Check that the test object aborts PACE protocol when LT transmits incorrect GENERAL AUTHENTICATE with incorrectly encoded ECAD (ECAD is not encoded as octet string). The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP, CAM
Preconditions	• Configuration profile CFG.DFLT.PACE.CAM is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. LT sends incorrectly encoded ECAD in the step 4 of GENERAL AUTHENTICATE
Expected results	1. - 2. The test object must abort communication to LT after receiving the last GENERAL AUTHENTICATE command. UT receives information from test object about protocol abort.

7.3.31 ISO7816_C_31: PACE-CAM with wrong ECAD

Test - ID	ISO7816_C_31
Purpose	Check that the test object aborts PACE protocol when LT transmits incorrect GENERAL AUTHENTICATE with wrong ECAD (increment ECAD by one). The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP, CAM
Preconditions	• Configuration profile CFG.DFLT.PACE.CAM is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. LT sends wrong tag ECAD in the step 4 of GENERAL AUTHENTICATE
Expected results	1. - 2. The test object must abort communication to LT after receiving the last GENERAL AUTHENTICATE command. UT receives information from test object about protocol abort.

7.3.32 ISO7816_C_32: PACE-CAM with wrong tag 8Ah (use 8Bh) but correct ECAD

Test - ID	ISO7816_C_32
Purpose	Check that the test object aborts PACE protocol when LT transmits incorrect GENERAL AUTHENTICATE with wrong tag 8Ah but correct ECAD. The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP, CAM
Preconditions	• Configuration profile CFG.DFLT.PACE.CAM is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. LT sends wrong tag 8Bh but correct ECAD in the step 4 of GENERAL AUTHENTICATE
Expected results	1. - 2. The test object must abort communication to LT after receiving the last GENERAL AUTHENTICATE command. UT receives information from test object about protocol abort.

7.3.33 ISO7816_C_33: PACE-CAM with correct tag 8Ah but missing ECAD

Test - ID	ISO7816_C_33
Purpose	Check that the test object aborts PACE protocol when LT transmits incorrect GENERAL AUTHENTICATE with correct tag 8Ah but missing ECAD.

	The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP, CAM
Preconditions	• Configuration profile CFG.DFLT.PACE.CAM is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. LT sends correct tag 8Ah but missing ECAD in the step 4 of GENERAL AUTHENTICATE
Expected results	1. - 2. The test object must abort communication to LT after receiving the last GENERAL AUTHENTICATE command. UT receives information from test object about protocol abort.

7.3.34 ISO7816_C_34: PACE-CAM with Passive Authentication

Test - ID	ISO7816_C_34
Purpose	Check that the test object performs Passive Authentication as soon as PACE-CAM was successfully performed. To indicate that the IS performs Passive Authentication, EF.SOD contains an invalid hash for EF.DG14. On this way the IS must detect a failure during Passive Authentication. The test is executed with the password MRZ or CAN.
Version	2.11
References	[ICAO Doc9303-11]
Profile	SIP, CAM
Preconditions	• Configuration profile CFG. PACE.7816C34 is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	1. - 2. The test object must perform Passive Authentication directly after performing PACE-CAM. UT receives information from test object about successful protocol PACE-CAM and failure during Passive Authentication.

ID		CFG.PACE.ISO7816.C34
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. EF.SOD must contain an invalid hash to assure that the IS fails during Passive Authentication. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.SOD***	Inavalid hash value for EF.DG14
		Access conditions: read and select with PACE

7.3.35 ISO7816_C_35: Return additional tag 8Ah during PACE-GM

Test - ID	ISO7816_C_35
Purpose	Check that the test object aborts PACE protocol when LT transmits additional tag 8Ah during GENERAL AUTHENTICATE. The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP, CAM
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. LT sends additional tag 8Ah in the step 4 of GENERAL AUTHENTICATE command
Expected results	1. - 2. The test object must abort communication to LT after receiving the last GENERAL AUTHENTICATE command. UT receives information from test object about protocol abort.

7.3.36 ISO7816_C_36: Use DG14 without SecurityInfo during PACE

Test - ID	ISO7816_C_36
Purpose	Check that the test object aborts PACE protocol when LT transmits a data group 14 for PACE without a SecurityInfo. The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP, CAM
Preconditions	• Configuration profile CFG.PACE.ISO7816_C36 is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	1. - 2. The test object must abort communication to LT PACE protocol. UT receives information from test object about protocol abort.

ID		CFG.PACE.ISO7816.C36
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	*EF.CardAccess*	Two PACEInfos: protocol: id-PACE-ECDH-GM-3DES-CBC-CBC protocol: id-PACE-ECDH-GM-AES-CBC-CMAC-128
		Access conditions: read and select always

	EF.DG14	Content of EF.CardAccess **but without SecurityInfo for PACE-GM**
		Access conditions: read and select with PACE
	EF.CardSecurity	SecurityInfo containing - ChipAuthenticationPublicKeyInfo as required for PACE-GM, - SecurityInfos contained in EF.CardAccess

7.3.37 ISO7816_C_37: Use EF.CardSecurity with wrong ChipAuthenticationPublicKey during PACE-CAM

Test - ID	ISO7816_C_37
Purpose	Check that the test object aborts PACE protocol when LT transmits an EF.CardSecurity for PACE-CAM with a wrong ChipAuthenticationPublicKey. The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP, CAM
Preconditions	• Configuration profile CFG.PACE.ISO7816_C37 is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	1. - 2. The test object must abort communication to LT PACE protocol. UT receives information from test object about protocol abort.

ID		CFG.PACE.ISO7816.C37
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.CardAccess***	Two PACEInfos: protocol: id-PACE-ECDH-GM-3DES-CBC-CBC protocol: id-PACE-ECDH-CAM-AES-CBC-CMAC-128
		Access conditions: read and select always
	EF.DG14	Content of EF.CardAccess
		Access conditions: read and select with PACE
	EF.CardSecurity	SecurityInfo containing - **Wrong ChipAuthenticationPublicKey** (e.g. increment by 1) as required for PACE-CAM, - SecurityInfos contained in EF.CardAccess

7.3.38 ISO7816_C_38: Use EF.CardSecurity without ChipAuthenticationPublicKeyInfo during PACE-CAM

Test - ID	ISO7816_C_38

Purpose	Check that the test object aborts PACE protocol when LT transmits an EF.CardSecurity for PACE-CAM with a missing ChipAuthenticationPublicKeyInfo. The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP, CAM
Preconditions	• Configuration profile CFG.PACE.ISO7816_C38 is loaded into the LT. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	1. - 2. The test object must abort communication to LT PACE protocol. UT receives information from test object about protocol abort.

ID		CFG.PACE.ISO7816.C38
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.CardAccess***	Two PACEInfos: protocol: id-PACE-ECDH-GM-3DES-CBC-CBC protocol: id-PACE-ECDH-CAM-AES-CBC-CMAC-128
		Access conditions: read and select always
	EF.DG14	Content of EF.CardAccess
		Access conditions: read and select with PACE
	EF.CardSecurity	SecurityInfo containing - **Missing ChipAuthenticationPublicKeyInfo**, - SecurityInfos contained in EF.CardAccess

7.3.39 ISO7816_C_39: Check supported standardized Domain Parameters with Chip Authentication Mapping

Test - ID	ISO7816_C_39_template
Purpose	Check correct execution of PACE protocol in the test object. The test has to be executed for each PACE Domain Parameters in Table 12. This test case is only rated as a PASS if all passes are completed successfully. The test is executed with the password MRZ or CAN.
Version	1.0
References	[ICAO Doc9303-11]
Profile	SIP, CAM
Preconditions	• Configuration profile CFG.DFLT.PACE.CAM is loaded into the LT. • In addition to the PACEInfo for PACE with generic mapping as required by CFG.DFLT.PACE.CAM, use exact one PACEInfo with

	standardized domain parameter (see Table 12) for PACE-CAM in EF.CardAccess. Don't use a PACEDomainParameterInfo within EF.CardAccess. • Make MRZ or CAN available in UT.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	1. - 2. MSE:Set AT command contains DO83 with value '01' or '02'. DO80 contains valid PACE protocol OID as provided in EF.CardAccess. The inspection procedure SHALL be successful.

Table 12 — Test case ISO7816_C_39

Test - ID	***Domain Parameter***	***parameterId***	***Mapping***
ISO7816_C_39d	NIST P-192 (secp192r1)	8	CAM
ISO7816_C_39e	NIST P-224 (secp224r1)	10	CAM
ISO7816_C_39f	NIST P-256 (secp256r1)	12	CAM
ISO7816_C_39g	NIST P-384 (secp384r1)	15	CAM
ISO7816_C_39h	NIST P-521 (secp521r1)	18	CAM
ISO7816_C_39i	BrainpoolP192r1	9	CAM
ISO7816_C_39j	BrainpoolP224r1	11	CAM
ISO7816_C_39k	BrainpoolP256r1	13	CAM
ISO7816_C_39l	BrainpoolP320r1	14	CAM
ISO7816_C_39m	BrainpoolP384r1	16	CAM
ISO7816_C_39n	BrainpoolP512r1	17	CAM

7.4 Unit ISO7816_D: Test of Secure Messaging

The test cases ISO716_D_02 to ISO7816_D_06 in this test unit can be performed with BAC or PACE profile.

7.4.1 ISO7816_D_01: SM failure returned by MRTD

Test - ID	ISO7816_D_01_template
Purpose	This test verifies that the inspection system recognizes an SM error generated by the MRTD. Perform standard inspection procedure and read BAC/PACE protected data groups from the lower tester.
Version	0.4
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile as defined in Table 13 is loaded into the LT.

	- Modification: The LT SHALL derive wrong session keys. The key derivation function uses c = 04 for the derivation of session key KS_{ENC} and c = 05 for the derivation of session key KS_{MAC}. - IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. The LT uses wrong session keys for the first incoming secured C-APDU. The LT SHALL return SW '6988' (Incorrect SM-DO) because the MAC verification fails.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

Table 13 — Test case ISO7816_D_01

Test - ID	***Configuration profile***
ISO7816_D_01a	CFG.DFLT.BAC
ISO7816_D_01b	CFG.DFLT.PACE

7.4.2 ISO7816_D_02: SM failure – MAC missing

Test - ID	ISO7816_D_02
Purpose	This test verifies that the inspection system recognizes an incorrect R-APDU in secure messaging. Perform standard inspection procedure and read BAC/PACE protected data groups from the lower tester.
Version	0.4
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	- Configuration profile CFG.DFLT.BAC or CFG.DFLT.PACE is loaded into the LT. - Modification: The LT SHALL NOT return the MAC data object (tag 8E) in the secured R-APDU. - IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. Wait until BAC/PACE is performed. In the first R-APDU the LT introduces a failure in the computation of the secure messaging R-APDU. The MAC data object (tag 8E) is not added to the secured response.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

7.4.3 ISO7816_D_03: SM failure – cryptogram missing

Test - ID	ISO7816_D_03
Purpose	This test verifies that the inspection system recognizes an incorrect R-APDU in secure messaging. Perform standard inspection procedure and read BAC/PACE protected data groups from the lower tester.
Version	0.4

Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC or CFG.DFLT.PACE is loaded into the LT. • Modification: The LT SHALL NOT return the cryptogram data object (tag 87) in the first secured R-APDU. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. The LT introduces a failure in the computation of the secure messaging. The cryptogram data object (tag 87) is not added to the secured response.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

7.4.4 ISO7816_D_04: SM failure – secured status bytes missing

Test - ID	ISO7816_D_04
Purpose	This test verifies that the inspection system recognizes an incorrect R-APDU in first secure messaging command. Perform standard inspection procedure and read BAC/PACE protected data groups from the lower tester.
Version	0.4
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC or CFG.DFLT.PACE is loaded into the LT. • Modification: The LT SHALL NOT return the status bytes (tag 99) in the secured R-APDU. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. The LT introduces a failure in the computation of the secure messaging. The SW data object (tag 99) is not added to the secured response.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

7.4.5 ISO7816_D_05: SM failure – incorrect MAC

Test - ID	ISO7816_D_05
Purpose	This test verifies that the inspection system recognizes an SM failure in the R-APDU. Perform standard inspection procedure and read BAC/PACE protected data groups from the lower tester.
Version	0.4
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC or CFG.DFLT.PACE is loaded

	into the LT. - Modification: The LT SHALL NOT increase the SSC for the computation of a MAC, which forces a secure messaging failure in the first R-APDU because the MAC data object is incorrect. The SSC is not increased when the first command while reading the EF.DG1 is executed. - IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. The LT introduces a failure in the computation of the secure messaging. The MAC of all secured responses are incorrect.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

7.4.6 ISO7816_D_06: SM failure – incorrect cryptogram

Test - ID	ISO7816_D_06
Purpose	This test verifies that the inspection system recognizes an SM failure in the first R-APDU. Perform standard inspection procedure and read BAC/PACE protected data groups from the lower tester.
Version	0.4
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	- Configuration profile CFG.DFLT.BAC or CFG.DFLT.PACE is loaded into the LT. - Modification: The LT SHALL pad the plaintext to be returned using 00 and not 80, which forces a secure messaging failure because the cryptogram data object is incorrect. - IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. The LT introduces a failure in the computation of the secure messaging. The cryptogram of all secured responses is wrong due to an incorrect padding of the plaintext.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed

7.5 Unit ISO7816_E: Test of Active Authentication

7.5.1 ISO7816_E_01: Performing Active Authentication with RSA-SHA1

Test - ID	ISO7816_E_01_template
Purpose	This test case verifies that the inspection system performs Active Authentication with RSA algorithm in signature function and based on signature production function B.6.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	AA
Preconditions	- Configuration profile CFG.PACE.ISO7816.E01 is loaded into the LT.

	- IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

Table 14 — Test case ISO7816_E_01

Test-ID	***Signature algorithm***	***Key length***
ISO7816_E_01a	RSA with SHA1	1024 bit
ISO7816_E_01b	RSA with SHA1	2048 bit

ID		CFG.PACE.ISO7816.E01
Purpose		This configuration is based on CFG.DFLT.PACEAA. The following files are modified as specified below. The hash values of the LDS security object MUST be updated to obtain a valid and authentic configuration.
	EF.DG15	Signature algorithm: see Table 14 (the signature production function B.6 is used)
		Access conditions: read and select with PACE

7.5.2 ISO7816_E_02: Performing Active Authentication with ECDSA

Test - ID	ISO7816_E_02_template
Purpose	This test case verifies that the inspection system performs Active Authentication with different ECDSA algorithms in signature function and based on signature production function B.6.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	AA
Preconditions	- Configuration profile CFG.PACE.ISO7816.E02 is loaded into the LT. - IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

Table 15 — Test case ISO7816_E_02

Test-ID	***Signature algorithm***	***Key length***
ISO7816_E_02a	ECDSA with SHA1	160 bit
ISO7816_E_02b	ECDSA with SHA224	224 bit
ISO7816_E_02c	ECDSA with SHA256	256 bit
ISO7816_E_02d	ECDSA with SHA384	384 bit

Test-ID	*Signature algorithm*	*Key length*
ISO7816_E_02e	ECDSA with SHA512	512 bit

ID		CFG.PACE.ISO7816.E02
Purpose		This configuration is based on CFG.DFLT.PACEAA. The following files are modified as specified below. The hash values of the LDS security object MUST be updated to obtain a valid and authentic configuration.
	EF.DG14	Security Info must contain a valid ActiveAuthenticationInfo : Algorithm Identifier must be 2.23.136.1.1.5 Signature algorithm: see Table 15 Version must be 1
		Access conditions: read and select with PACE
	EF.DG15	Signature algorithm: see Table 15 (the signature production function B.6 is used)
		Access conditions: read and select with PACE

7.5.3 ISO7816_E_03: Performing Active Authentication with RSA-SHA224

Test - ID	ISO7816_E_03
Purpose	This test case verifies that the inspection system performs Active Authentication with RSA-SHA224 algorithm in signature function and based on signature production function B.6.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	AA
Preconditions	• Configuration profile CFG.PACE.ISO7816.E03 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.PACE.ISO7816.E03
Purpose		This configuration is based on CFG.DFLT.PACEAA. The following files are modified as specified below. The hash values of the LDS security object MUST be updated to obtain a valid and authentic configuration.
	EF.DG15	Signature algorithm: RSA SHA224 (the signature production function B.6 is used)
		Access conditions: read and select with PACE

7.5.4 ISO7816_E_04: Performing Active Authentication with RSA-SHA256

Test - ID	ISO7816_E_04

Purpose	This test case verifies that the inspection system performs Active Authentication with RSA-SHA256 algorithm in signature function and based on signature production function B.6.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	AA
Preconditions	• Configuration profile CFG.PACE.ISO7816.E04 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.PACE.ISO7816.E04
Purpose		This configuration is based on CFG.DFLT.PACEAA. The following files are modified as specified below. The hash values of the LDS security object MUST be updated to obtain a valid and authentic configuration.
	EF.DG15	Signature algorithm: RSA SHA256 (the signature production function B.6 is used)
		Access conditions: read and select with PACE

7.5.5 ISO7816_E_05: Performing Active Authentication with RSA-SHA384

Test - ID	ISO7816_E_05
Purpose	This test case verifies that the inspection system performs Active Authentication with RSA-SHA384 algorithm in signature function and based on signature production function B.6.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	AA
Preconditions	• Configuration profile CFG.PACE.ISO7816.E05 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.PACE.ISO7816.E05
Purpose		This configuration is based on CFG.DFLT.PACEAA. The following files are modified as specified below. The hash values of the LDS security object MUST be updated to obtain a valid and authentic configuration.
	EF.DG15	Signature algorithm: RSA SHA384 (the signature production function B.6 is used)
		Access conditions: read and select with PACE

7.5.6 ISO7816_E_06: Performing Active Authentication with RSA-SHA512

Test - ID	ISO7816_E_06
Purpose	This test case verifies that the inspection system performs Active Authentication with RSA-SHA512 algorithm in signature function and based on signature production function B.6.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	AA
Preconditions	• Configuration profile CFG.PACE.ISO7816.E06 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.PACE.ISO7816.E06
Purpose		This configuration is based on CFG.DFLT.PACEAA. The following files are modified as specified below. The hash values of the LDS security object MUST be updated to obtain a valid and authentic configuration.
	EF.DG15	Signature algorithm: RSA SHA512 (the signature production function B.6 is used)
		Access conditions: read and select with PACE

7.5.7 ISO7816_E_07: Performing Active Authentication with wrong trailer

Test - ID	ISO7816_E_07
Purpose	This test case verifies that the inspection system performs Active Authentication with wrong trailer during calculation and based on signature production function B.6.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	AA
Preconditions	• Configuration profile CFG.DFLT.PACEAA is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. The simulation delivers a wrong trailer during AA ('33', valid trailers can be found in ISO9796-2)
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

7.5.8 ISO7816_E_08: Performing Active Authentication with invalid signature OID

Test - ID	ISO7816_E_08
Purpose	This test case verifies that the inspection system performs Active

	Authentication with invalid algorithm OID in signature function and based on signature production function B.6.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	AA
Preconditions	• Configuration profile CFG.PACE.ISO7816.E08 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.ISO7816.E08
Purpose		This configuration is based on CFG.DFLT.PACEAA. The following files are modified as specified below. The hash values of the LDS security object MUST be updated to obtain a valid and authentic configuration.
	EF.DG15	Invalid Signature algorithm OID: 1.2.840.113549.1.1.6 (Valid OIDs can be found in [ISO/IEC 9796-2]) (the signature production function B.6 is used)
		Access conditions: read and select with PACE

7.5.9 ISO7816_E_09: Performing Active Authentication with RSA SHA1 and B6 method

Test - ID	ISO7816_E_09_template
Purpose	This test case verifies that the inspection system performs the Active Authentication with RSA algorithm in the signature function. The signature shall be generated by using [ISO/IEC 9796-2] clause B.6 “Alternative signature production function”.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	AA
Preconditions	Configuration profile CFG.PACE.ISO7816.E09 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. The RSA operation during AA must result in a value bigger than n/2 with n being the modulus to ensure that method B6 is really used in this test case.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful

Table 16 — Test case ISO7816_E_09

Test-ID	***Signature algorithm***	***Key Length***

ISO7816_E_09a	RSA with SHA1	1024
ISO7816_E_09b	RSA with SHA1	2048

ID		CFG.PACE.ISO7816.E09
Purpose		This configuration is based on CFG.DFLT.PACEAA. The following files are modified as specified below. The hash values of the LDS security object MUST be updated to obtain a valid and authentic configuration. The signature shall be generated using the B6 method.
	EF.DG15	Signature algorithm: see Table 16 (the signature production function B.6 is used)
		Access conditions: read and select with PACE

7.5.10 ISO7816_E_10: Performing Active Authentication with invalid DG15 Public key

Test - ID	ISO7816_E_10_template
Purpose	This test case verifies that the inspection system really checks the signature of the AA function and gives appropriate status using signature production function B.6 in case of RSA.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	AA
Preconditions	Configuration profile CFG.PACE.ISO7816.E10 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

Table 17 — Test case ISO7816_E_10

Test-ID	***Signature algorithm***	***Key Length***
ISO7816_E_10a	RSA with SHA	1024
ISO7816_E_10b	ECDSA with SHA1	160

ID		CFG.PACE.ISO7816.E10
Purpose		This configuration is based on CFG.DFLT.PACEAA. The following files are modified as specified below. The hash values of the LDS security object MUST be updated to obtain a valid and authentic configuration.
	EF.DG15	Invalid public Key with signature algorithm see Table 17 (the signature production function B.6 is used)

		Access conditions: read and select with PACE

7.5.11 ISO7816_E_11: Performing Active Authentication with RSA SHA1 and B4 method

Test - ID	ISO7816_E_11_template
Purpose	This test case verifies that the inspection system performs the Active Authentication with RSA algorithm in the signature function. The signature shall be generated by using [ISO/IEC 9796-2] clause B.4 “Signature production function”.
Version	2.11
Reference	[ICAO Doc9303-11]
Profile	AA_B4
Preconditions	Configuration profile CFG.PACE.ISO7816.E11 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. The RSA operation prior to the ISO/IEC 9796-2 B.4 minimum calculation (i.e. J^s mod n in the ISO/IEC 9796-2 notation) during AA must result in a value bigger than n/2 with n being the modulus. This ensures that n-(J^s mod n) is used as the signature, i.e. that the method B.4 is really used in this test case
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful

Table 18 — Test case ISO7816_E_09

Test-ID	***Signature algorithm***	***Key Length***
ISO7816_E_09a	RSA with SHA1	1024
ISO7816_E_09b	RSA with SHA1	2048

ID		CFG.PACE.ISO7816.E11
Purpose		This configuration is based on CFG.DFLT.PACEAA. The following files are modified as specified below. The hash values of the LDS security object MUST be updated to obtain a valid and authentic configuration. The signature shall be generated using the B4 method.
	EF.DG15	Signature algorithm: see Table 19 (the signature production function B.4 is used)
		Access conditions: read and select with PACE

7.6 Unit ISO7816_F: Test of Reading Binary Files

7.6.1 ISO7816_F_01: File selection failure

Test - ID	ISO7816_F_01

Purpose	This test verifies that the inspection system recognizes a file selection failure due to a data group declared in EF.COM but does not exist in the file system. Perform standard inspection procedure and read BAC protected data groups DG1 and DG2, which does not exist, from the lower tester.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.BAC.ISO7816.F01 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. The LT returns checking error SW '6A 82' if EF.DG2 is selected by FID or SFI.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.ISO7816.F01
Purpose		This configuration defines a BAC protected MRTD.
Content	***EF.COM***	LDS Version 1.7, Unicode version 4.0.0, Data groups present: 61, 75
		Access conditions: read and select with BAC
	EF.SOD	LDS security object containing hash values of DG1 and DG2 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with BAC
	EF.DG1	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4
		Access conditions: read and select with BAC
	EF.DG2	No DG2 installed!
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4

7.6.2 ISO7816_F_02: Reading large files

Test - ID	ISO7816_F_02
Purpose	This test verifies that the inspection system is capable of reading large binary files. Perform standard inspection procedure and read BAC protected data groups from the lower tester. DG2 contains a face image of size larger than 32k.
Version	1.0
Reference	[ICAO Doc9303-11]

Profile	SIP
Preconditions	• Configuration profile CFG.BAC.ISO7816.F02 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.BAC.ISO7816.F02
Purpose		This configuration defines a BAC protected MRTD.
Content	***EF.COM***	LDS Version 1.7, Unicode version 4.0.0, Data groups present: 61, 75
		Access conditions: read and select with BAC
	EF.SOD	LDS security object containing hash values of DG1 and DG2 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with BAC

	EF.DG1	`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<`
		`C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4`

		Access conditions: read and select with BAC
	EF.DG2	Facial Image 3 (see chapter 0), JPEG2000 with image size larger than 32 KByte
		Access conditions: read and select with BAC

	Data page MRZ	`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<`
		`C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4`

7.6.3 ISO7816_F_03: Reading beyond EOF

Deleted in version 2.11

7.6.4 ISO7816_F_04: Reading end of file with status word 6B00

Test - ID	ISO7816_F_04
Purpose	This test verifies that the inspection system recognizes the end of a binary file. Perform standard inspection procedure and read BAC protected data groups from the lower tester. DG2 contains parts of a face image stored in a binary file that is too small for the whole image data. The LT answers with checking error SW '6B 00' and the IS must handle this error correct.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.BAC.ISO7816.F03 is loaded into the LT.

	• IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. If the inspection system reads beyond EOF, LT shall return checking error SW '6B 00'
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

7.6.5 ISO7816_F_05: Reading end of file with status word 6282

Test - ID	ISO7816_F_05
Purpose	This test verifies that the inspection system recognizes the end of a binary file. Perform standard inspection procedure and read BAC protected data groups from the lower tester. DG2 contains parts of a face image stored in a binary file that is too small for the whole image data. The LT answers with warning processing SW '62 82' and the IS must handle this warning correct.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.BAC.ISO7816.F03 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. If the inspection system reads beyond EOF, LT shall return warning processing SW '62 82'
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

7.6.6 ISO7816_F_06: Reading end of file with status word 6Cxx

Test - ID	ISO7816_F_06
Purpose	This test verifies that the inspection system recognizes the end of a binary file. Perform standard inspection procedure and read BAC protected data groups from the lower tester. DG2 contains parts of a face image stored in a binary file that is too small for the whole image data. The LT answers with checking error SW '6Cxx' and the IS must handle this error correct.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.BAC.ISO7816.F03 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. If the inspection system reads beyond EOF, LT shall return checking error SW '6C xx' (xx is free to choose)
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

7.6.7 ISO7816_F_07: Reading file with OddIns

Test - ID	ISO7816_F_07
Purpose	This test verifies that the inspection system is capable of using odd instruction bytes (odd ins). Perform standard inspection procedure and read BAC protected data groups from the lower tester.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start standard inspection procedure if not automatically started. 3. If IS reads a BAC protected data group the LT SHALL response with R-APDU including odd instruction bytes. R-APDU must include tag 53 and BER encoded length.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

7.6.8 ISO7816_F_08: Reading DG2 with image size 0

Test - ID	ISO7816_F_08
Purpose	This test verifies that the inspection system is capable of reading data groups with empty files. Perform standard inspection procedure and read BAC protected data groups from the lower tester. DG2 contains a face image of size 0.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.BAC.ISO7816.F08 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.BAC.ISO7816.F08
Purpose		This configuration defines a BAC protected MRTD. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST are updated to obtain a valid and authentic configuration.
Content	***EF.COM***	LDS Version 1.7, Unicode version 4.0.0, Data groups present: 61, 75
		Access conditions: read and select with BAC
	EF.DG2	Facial Image: JPEG2000 with image size equals 0 Byte DG2 does contain the Biometric full face record format as described in [ISO/IEC 19794-5] (CBEFF Header, Facial Record Header and Facial Record Data) but without Image data (size of the image is zero).

		Access conditions: read and select with BAC

7.7 Unit ISO7816_G: Tests of Chip Authentication

7.7.1 ISO7816_G_01: Chip Authentication with DH

Test - ID	ISO7816_G_01
Purpose	This test case verifies that the inspection system performs chip authentication successfully with Diffie-Hellman algorithm and no key reference in DG14.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.EAC.ISO7816.G01 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.EAC.ISO7816.G01
Purpose		This configuration is based on CFG.DFLT.EAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.DG14***	Key agreement algorithm: **id-CA-DH-3DES-CBC-CBC** Key reference: none, implicitly known
		Access conditions: read and select with BAC or PACE

7.7.2 ISO7816_G_02: Chip Authentication with ECDH

Test - ID	ISO7816_G_02
Purpose	This test case verifies that the inspection system performs chip authentication successfully with Elliptic Curve Diffie-Hellman algorithm and no key reference in DG14.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.DFLT.EAC is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

7.7.3 ISO7816_G_03: DG14 with one key reference

Test - ID	ISO7816_G_03
Purpose	This test case verifies that the inspection system performs chip authentication successfully if there is one key reference in data group 14.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.EAC.ISO7816.G03 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.EAC.ISO7816.G03
Purpose		This configuration is based on CFG.DFLT.EAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.DG14***	Key agreement algorithm: id-CA-ECDH-3DES-CBC-CBC Key reference: **01**
		Access conditions: read and select with BAC or PACE

7.7.4 ISO7816_G_04: DG14 with two key references

Test - ID	ISO7816_G_04
Purpose	This test case verifies that the inspection system performs chip authentication successfully if there are two key references in data group 14. Every key referenced in DG14 MUST be accepted.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.EAC.ISO7816.G04 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID	CFG.EAC.ISO7816.G04
Purpose	This configuration is based on CFG.DFLT.EAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.

Content	***EF.DG14***	Key agreement algorithm: id-CA-ECDH-3DES-CBC-CBC Key reference: **01, 02**
		Access conditions: read and select with BAC or PACE

7.7.5 ISO7816_G_05: DG14 with three key references

Test - ID	ISO7816_G_05
Purpose	This test case verifies that the inspection system performs chip authentication successfully if there are three key references in data group 14. Every key referenced in DG14 MUST be accepted.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.EAC.ISO7816.G05 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.EAC.ISO7816.G05
Purpose		This configuration is based on CFG.DFLT.EAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.DG14***	Key agreement algorithm: id-CA-ECDH-3DES-CBC-CBC Key reference: **01, 02, 03**
		Access conditions: read and select with BAC or PACE

7.7.6 ISO7816_G_06: DG14 with invalid key reference

Test - ID	ISO7816_G_06
Purpose	This test case verifies that the chip authentication fails if there is an invalid key reference in data group 14.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.EAC.ISO7816.G06 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.EAC.ISO7816.G06
Purpose		This configuration is based on CFG.DFLT.EAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.DG14***	Key agreement algorithm: id-CA-ECDH-3DES-CBC-CBC Two key reference: 'FF' and 'FE' in DG14 but '01' in chip
		Access conditions: read and select with BAC or PACE

7.7.7 ISO7816_G_07: DG14 with corrupted DH public key

Test - ID	ISO7816_G_07
Purpose	This test case verifies that the chip authentication fails if there is a corrupted DH public key in data group 14.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.EAC.ISO7816.G07 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.EAC.ISO7816.G07
Purpose		This configuration is based on CFG.DFLT.EAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.DG14***	Key agreement algorithm: id-CA-DH-3DES-CBC-CBC Key reference: none, implicitly known Public key integer SHALL be added by 1.
		Access conditions: read and select with BAC or PACE

7.7.8 ISO7816_G_08: DG14 with corrupted ECDH public key

Test - ID	ISO7816_G_08
Purpose	This test case verifies that chip authentication fails if there is a corrupted ECDH key in data group 14.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.EAC.ISO7816.G08 is loaded into the LT. • IS is „ready“.

Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.EAC.ISO7816.G08
Purpose		This configuration is based on CFG.DFLT.EAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.DG14***	Key agreement algorithm: id-CA-ECDH-3DES-CBC-CBC Key reference: none Public key point SHALL NOT be on the Elliptic Curve.
		Access conditions: read and select with BAC or PACE

7.7.9 ISO7816_G_09: Use old session keys after Chip Authentication

Test - ID	ISO7816_G_09
Purpose	This test case verifies that the inspection system uses new session keys after chip authentication.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.DFLT.EAC is loaded into the eMRTD simulator. Modification: The simulator SHALL reuse old session keys after a successful chip authentication. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

7.7.10 ISO7816_G_10: Verify lifetime of ephemeral keys

Test - ID	ISO7816_G_10
Purpose	This test case verifies that the inspection system uses ephemeral keys with short lifetime.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.DFLT.EAC is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. Store first ephemeral key. 4. Place test data page onto the test object.

	5. Start advanced inspection procedure if not automatically started. 6. Store second ephemeral key. 7. Ephemeral key of step 3 and ephemeral key of step 6 MUST be different to assure that ephemeral keys lifetime is short.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

7.7.11 ISO7816_G_11: DG14 with invalid DH public key specification

Test - ID	ISO7816_G_11
Purpose	This test case verifies that chip authentication fails if there is an invalid DH key specification in data group 14.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.EAC.ISO7816.G11 loaded into the eMRTD simulator. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. Chip delivers invalid DH key specification.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.EAC.ISO7816.G11
Purpose		This configuration is based on CFG.DFLT.EAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.DG14***	Key agreement algorithm: id-CA-DH-3DES-CBC-CBC Key reference: none Invalid OID in SubjectPublicKeyInfo (2A 86 48 86 F7 0D 01 03 02)
		Access conditions: read and select with BAC or PACE

7.7.12 ISO7816_G_12: DG14 with invalid ECDH public key specification

Test - ID	ISO7816_G_12
Purpose	This test case verifies that chip authentication fails if there is an invalid ECDH key specification in data group 14.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.EAC.ISO7816.G12 loaded into the eMRTD simulator. • IS is „ready“.

Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. Chip delivers invalid ECDH key specification.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.EAC.ISO7816.G12
Purpose		This configuration is based on CFG.DFLT.EAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.DG14***	Key agreement algorithm: id-CA-ECDH-3DES-CBC-CBC Key reference: none Invalid OID in SubjectPublicKeyInfo (2A 86 48 CE 3D 02 02)
		Access conditions: read and select with BAC or PACE

7.7.13 ISO7816_G_13: ChipAuthenticationPublicKeyInfo: key reference does not match key reference in ChipAuthenticationInfo

Test - ID	ISO7816_G_13
Purpose	This test case verifies that the inspection system performs correctly if EF.DG14 is wrong (incorrect key reference, that does not match key reference in ChipAuthenticationInfo)
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.EAC.ISO7816.G13 loaded into the eMRTD simulator. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.EAC.ISO7816.G13
Purpose		This configuration is based on CFG.DFLT.EAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.DG14***	Key agreement algorithm: id-CA-ECDH-3DES-CBC-CBC Use EF.DG14 with incorrect key reference, which does not match key reference in ChipAuthenticationInfo.
		Access conditions: read and select with BAC or PACE

7.7.14 ISO7816_G_14: Chip Authentication with Extended Length

Test - ID	ISO7816_G_14
Purpose	This test case verifies that the inspection system performs correctly if EF.DG14 enforces Extended length because of certificates larger than 256 Bytes.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.EAC.ISO7816.G14 loaded into the eMRTD simulator. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.EAC.ISO7816.G14
Purpose		This configuration is based on CFG.DFLT.EAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.DG14***	Use EF.DG14 with DH and keys size 2048 as algorithm. Key agreement algorithm: id-CA-DH-3DES-CBC-CBC
		Access conditions: read and select with BAC or PACE

7.7.15 ISO7816_G_15: Use various status words for invalid key reference

Test - ID	ISO7816_G_15_template
Purpose	This test case verifies that the inspection system performs correctly if valid EF.DG14 is used and the simulator sends various valid status words for this behaviour.
Version	1.0
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.DFLT.EAC loaded into the eMRTD simulator. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. Repeat test case for every valid status word as specified in Table 20.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

Table 20 — Test case ISO7816_G_15

Test - ID	*Response SW to Chip Authentication*
ISO7816_G_15a	63 00
ISO7816_G_15b	67 00
ISO7816_G_15c	68 00
ISO7816_G_15d	69 00
ISO7816_G_15e	6A 00
ISO7816_G_15f	6B 00
ISO7816_G_15g	6C 00
ISO7816_G_15h	6E 00
ISO7816_G_15i	6F 00

7.7.16 ISO7816_G_16: Chip supported CA algorithms

Test - ID	ISO7816_G_16_template
Purpose	Check correct execution of the chip authentication protocol in the test object. The test has to be executed for each CA algorithm specified in [ICAO Doc9303-11]. This test case is only rated as a PASS if all passes are completed successfully.
Version	2.11
Reference	[ICAO Doc9303-11]
Profile	CA
Preconditions	• Configuration profile CFG.EAC.ISO7816.G16 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.EAC.ISO7816.G16
Purpose		This configuration is based on CFG.DFLT.EAC. The following files are modified for the different test cases as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Test-ID		
ISO7816_G_16a	***EF.DG14***	Key agreement algorithm: id-CA-ECDH-3DES-CBC-CBC Key reference: none, implicitly known
		Access conditions: read and select with BAC
ISO7816_G_16b	***EF.DG14***	Key agreement algorithm: id-CA-ECDH-AES-CBC-CMAC-128 Key reference: none, implicitly known
		Access conditions: read and select with BAC
ISO7816_G_16c	***EF.DG14***	Key agreement algorithm: id-CA-ECDH-AES-CBC-CMAC-192 Key reference: none, implicitly known
		Access conditions: read and select with BAC

ISO7816_G_ 16d	***EF.DG14***	Key agreement algorithm: id-CA-ECDH-AES-CBC-CMAC-256 Key reference: none, implicitly known
		Access conditions: read and select with BAC
ISO7816_G_ 16e	***EF.DG14***	Key agreement algorithm: id-CA-DH-3DES-CBC-CBC Key reference: none, implicitly known
		Access conditions: read and select with BAC
ISO7816_G_ 16f	***EF.DG14***	Key agreement algorithm: id-CA-DH-AES-CBC-CMAC-128 Key reference: none, implicitly known
		Access conditions: read and select with BAC
ISO7816_G_ 16g	***EF.DG14***	Key agreement algorithm: id-CA-DH-AES-CBC-CMAC-192 Key reference: none, implicitly known
		Access conditions: read and select with BAC
ISO7816_G_ 16h	***EF.DG14***	Key agreement algorithm: id-CA-DH-AES-CBC-CMAC-256 Key reference: none, implicitly known
		Access conditions: read and select with BAC

8 Layer 7 tests (Logical data structures)

8.1 Unit LDS_A: Tests with EF.COM

8.1.1 LDS_A_01: DG tag 60 wrong (use tag 61 instead)

Test - ID	LDS_A_01
Purpose	This test case verifies that the inspection system performs correctly if EF.COM is wrong (wrong tag 60).
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.A01 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.A01
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.COM***	LDS Version 1.7, Unicode version 4.0.0, Data groups present: 61, 6E, 75 Tag 60 is replaced by wrong tag 61 **61** 15 5F 01 04 30 31 30 37 5F 36 06 30 34 30 30 30 30 5C 03 61 75 6E
		Access conditions: read and select with PACE

8.1.2 LDS_A_02: DG tag 60 length byte too small

Test - ID	LDS_A_02
Purpose	This test case verifies that the inspection system performs correctly if EF.COM is wrong (length byte of tag 60 is too small).
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.A02 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.A02
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.COM***	LDS Version 1.7, Unicode version 4.0.0, Data groups present: 61, 6E, 75 Tag 60 length byte is decreased to 14. 60 **14** 5F 01 04 30 31 30 37 5F 36 06 30 34 30 30 30 30 5C 03 61 75 6E
		Access conditions: read and select with PACE

8.1.3 LDS_A_03: DG tag 60 length byte too big

Test - ID	LDS_A_03
Purpose	This test case verifies that the inspection system performs correctly if EF.COM is wrong (length byte of tag 60 is too big).
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.A03 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID	CFG.PACE.LDS.A03
Purpose	This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.

Content	***EF.COM***	LDS Version 1.7, Unicode version 4.0.0, Data groups present: 61, 6E, 75 Tag 60 length byte is increased to 16. 60 **16** 5F 01 04 30 31 30 37 5F 36 06 30 34 30 30 30 30 5C 03 61 75 6E
		Access conditions: read and select with PACE

8.1.4 LDS_A_04: Incorrect LDS version (use V3.0 instead)

Test - ID	LDS_A_04
Purpose	This test case verifies that the inspection system performs correctly if EF.COM is wrong (incorrect LDS version).
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.A04 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.A04
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.COM***	LDS Version 3.0, Unicode version 4.0.0, Data groups present: 61, 6E, 75 LDS version is set to V3.0. 60 15 5F 01 04 **30 33 30 30** 5F 36 06 30 34 30 30 30 30 5C 03 61 75 6E
		Access conditions: read and select with PACE

8.1.5 LDS_A_05: Missing LDS version

Test - ID	LDS_A_05
Purpose	This test case verifies that the inspection system performs correctly if EF.COM is wrong (missing LDS version).
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.A05 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.A05
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.COM***	LDS Version 1.7, Unicode version 4.0.0, Data groups present: 61, 6E, 75 LDS version is deleted. 60 **0E** 5F 36 06 30 34 30 30 30 30 5C 03 61 75 6E
		Access conditions: read and select with PACE

8.1.6 LDS_A_06: Incorrect Unicode version (use V05.00.00 instead)

Test - ID	LDS_A_06
Purpose	This test case verifies that the inspection system performs correctly if EF.COM is wrong incorrect Unicode version).
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.A06 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.A06
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.COM***	LDS Version 1.7, Unicode version 5.0.0, Data groups present: 61, 6E, 75 Unicode version is set to 5.0.0. 60 15 5F 01 04 30 31 30 37 5F 36 06 **30 35 30 30 30 30** 5C 03 61 75 6E
		Access conditions: read and select with PACE

8.1.7 LDS_A_07: Missing Unicode version

Test - ID	LDS_A_07
Purpose	This test case verifies that the inspection system performs correctly if EF.COM is wrong (missing Unicode version).
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.A07 is loaded into the LT.

	- IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.A07
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.COM***	LDS Version 1.7, Unicode version 4.0.0, Data groups present: 61, 6E, 75 Unicode version is deleted. 60 **0C** 5F 01 04 30 31 30 37 5C 03 61 75 6E
		Access conditions: read and select with PACE

8.1.8 LDS_A_08: Incorrect DGPM (missing DG1 tag)

Test - ID	LDS_A_08
Purpose	This test case verifies that the inspection system performs correctly if EF.COM is wrong (incorrect DGPM).
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	- Configuration profile CFG.PACE.LDS.A08 is loaded into the LT. - IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.A08
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.COM***	LDS Version 1.7, Unicode version 4.0.0, Data groups present: , 6E, 75 Tag 61 is deleted from the DGPM. 60 **14** 5F 01 04 30 31 30 37 5F 36 06 30 34 30 30 30 30 **5C 02** 75 6E
		Access conditions: read and select with PACE

8.1.9 LDS_A_09: Missing DGPM

Test - ID	LDS_A_09
Purpose	This test case verifies that the inspection system performs correctly if

	EF.COM is wrong (incorrect DGPM).
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.A09 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.A09
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.COM***	LDS Version 1.7, Unicode version 4.0.0 DGPM is deleted from EF.COM. 60 **10** 5F 01 04 30 31 30 37 5F 36 06 30 34 30 30 30 30
		Access conditions: read and select with PACE

8.1.10 LDS_A_10: EF.COM with LDS version 1.8

Test - ID	LDS_A_10
Purpose	This test case verifies that the inspection system performs correctly if EF.COM is contains LDS version 1.8.
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.A10 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.PACE.LDS.A10
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.COM***	**LDS Version 1.8**, Unicode version 4.0.0, Data groups present: 61, 6E, 75 60 15 5F 01 04 30 31 30 **38** 5F 36 06 30 34 30 30 30 30 5C 03 61 75 6E
		Access conditions: read and select with PACE

8.2 Unit LDS_B: Tests with EF.DG1

8.2.1 LDS_B_01: MRZ with optional data

Test - ID	LDS_B_01
Purpose	This test case verifies that the inspection system performs correctly if the MRZ stored in EF.DG1 contains optional data.
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B01 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.BAC.LDS.B01
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	*EF.DG1*	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314**ZE184226B<<<<<16**
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314**ZE184226B<<<<<16**

8.2.2 LDS_B_02: Name in MRZ indicates abbreviation of the secondary identifier

Test - ID	LDS_B_02
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 contains an abbreviation of secondary identifier.
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B02 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.BAC.LDS.B02
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.DG1***	P<D<<MUSTERMANN<<ERIKA<**MARTA<PAM<CLARA<SYNTH** C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<**MARTA<PAM<CLARA<SYNTH** C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4

8.2.3 LDS_B_03: Name in MRZ without secondary identifier

Test - ID	LDS_B_03
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 contains no secondary identifier.
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B03 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.BAC.LDS.B03
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.DG1***	P<D<<MUSTERMANN<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4

8.2.4 LDS_B_04: No optional data, checksum is '0' instead of '<'

Test - ID	LDS_B_04
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (checksum is '0' instead of '<')
Version	1.0

Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B04 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.BAC.LDS.B04
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.

Content	***EF.DG1***	`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<`
		`C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<`**`0`**`4`

		Access conditions: read and select with BAC

	Data page MRZ	`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<`
		`C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<`**`0`**`4`

8.2.5 LDS_B_05: DG tag 61 wrong (use tag 62 instead)

Test - ID	LDS_B_05
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (incorrect tag 61, use tag 62 instead)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B05 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B05
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.DG1***	Use EF.DG1 with incorrect tag 61, use tag 62 instead: **`62`**`5B5F1F58503C443C3C...`
		Access conditions: read and select with BAC

8.2.6 LDS_B_06: DG tag 61 length byte too small

Test - ID	LDS_B_06
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (length byte of tag 61 is too small)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B06 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B06
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.DG1***	Use EF.DG1 with length byte of tag 61 is too small: `61`**`5A`**`5F1F58503C443C3C...`
		Access conditions: read and select with BAC

8.2.7 LDS_B_07: DG tag 61 length byte too big

Test - ID	LDS_B_07
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (length byte of tag 61 is too big)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B07 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B07
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use EF.DG1 with length byte of tag 61 is too big:

		61**7F**5F1F58503C443C3C...
		Access conditions: read and select with BAC

8.2.8 LDS_B_08: Incorrect MRZ, document type unknown

Test - ID	LDS_B_08
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (unknown document type in MRZ)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B08 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B08
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use EF.DG1 with unknown document type (BB): **BB**D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4
		Access conditions: read and select with BAC
	Data page MRZ	**BB**D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4

8.2.9 LDS_B_09: Incorrect MRZ, issuing state syntax error

Test - ID	LDS_B_09
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (issuing state syntax error in MRZ)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B09 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B09
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use EF.DG1 with issuing state syntax error: P<**D21**MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4
		Access conditions: read and select with BAC
	Data page MRZ	P<**D21**MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4

8.2.10 LDS_B_10: Incorrect MRZ, name is void

Test - ID	LDS_B_10
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (name is void in MRZ)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B10 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B10
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use EF.DG1 with void name in MRZ: P<**D**<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4
		Access conditions: read and select with BAC
	Data page MRZ	P<**D**<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4

8.2.11 LDS_B_11: Incorrect MRZ, name different from data page

Test - ID	LDS_B_11

Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (name in DG1 and on data page are different).
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B11 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B11
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.

	EF.DG1	Use EF.DG1 with different name than on data page:
		`P<D<<ERIKSSON<<ANNA<<<<<<<<<<<<<<<<<<<<<<<<<`
		`C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4`

		Access conditions: read and select with BAC

	Data page MRZ	`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<`
		`C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4`

8.2.12 LDS_B_12: Incorrect MRZ, document number different from data page

Test - ID	LDS_B_12
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (document number in DG1 and on data page are different)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B12 is loaded into the LT. The BAC keys SHALL be derived from the MRZ of the data page. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID	CFG.BAC.LDS.B12
Purpose	This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and

		authentic configuration.

	EF.DG1	Use EF.DG1 with different document number than on data page:
		`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<`
		`F421231D``<`**`1`**`D<<9608122F2310314<<<<<<<<<<<<<<<`**`0`**

		Access conditions: read and select with BAC

	Data page MRZ	`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<`
		`C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4`

8.2.13 LDS_B_13: Incorrect MRZ, wrong document number checksum

Test - ID	LDS_B_13
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (incorrect checksum of document number)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B13 is loaded into the LT. The BAC keys SHALL be derived from the MRZ of the data page. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL respond: “Inspection procedure failed” or MRTD is rejected because checksum of document number is not correct.

ID		CFG.BAC.LDS.B13
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.

	EF.DG1	Use EF.DG1 with incorrect document number checksum:
		`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<`
		`C11T002JM`**`5`**`D<<9608122F2310314<<<<<<<<<<<<<<<`**`1`**

		Access conditions: read and select with BAC

	Data page MRZ	`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<`
		`C11T002JM`**`5`**`D<<9608122F2310314<<<<<<<<<<<<<<<`**`1`**

8.2.14 LDS_B_14: Incorrect MRZ, nationality syntax error

Test - ID	LDS_B_14
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (nationality syntax error)
Version	1.0

Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B14 is loaded into the LT. The BAC keys SHALL be derived from the MRZ of the data page. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B14
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use DG2 with nationality syntax error: P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4**D21**9608122F2310314<<<<<<<<<<<<<<<4
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4**D21**9608122F2310314<<<<<<<<<<<<<<<4

8.2.15 LDS_B_15: Incorrect MRZ, date of birth syntax error

Test - ID	LDS_B_15
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (syntax error in date of birth)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B15 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B15
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use DG1 with with syntax error in date of birthday (3112AB): P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<

		C11T002JM4D<<**3112AB0**F2310314<<<<<<<<<<<<<<<**6**
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<**3112AB0**F2310314<<<<<<<<<<<<<<<**6**

8.2.16 LDS_B_16: Incorrect MRZ, date of birth error

Test - ID	LDS_B_16
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (error in date of birth)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B16 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B16
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use DG1 with error in date of birth (671331): P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<**6713315**F2310314<<<<<<<<<<<<<<<**6**
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<**6713315**F2310314<<<<<<<<<<<<<<<**6**

8.2.17 LDS_B_17: Incorrect MRZ, incorrect date of birth checksum

Test - ID	LDS_B_17
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (incorrect checksum of date of birth)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B17 is loaded into the LT. • IS is „ready".

Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B17
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use DG1 with incorrect checksum of date of birth: P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<960812**3**F2310314<<<<<<<<<<<<<<<**7**
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<960812**3**F2310314<<<<<<<<<<<<<<<**7**

8.2.18 LDS_B_18: Incorrect MRZ, incorrect sex

Test - ID	LDS_B_18
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (incorrect sex)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B18 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B18
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use EF.DG1 with incorrect sex (D): P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122**D**2310314<<<<<<<<<<<<<<<4
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122**D**2310314<<<<<<<<<<<<<<<4

8.2.19 LDS_B_19: Incorrect MRZ, date of expiry syntax error

Test - ID	LDS_B_19
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (syntax error in date of expiry)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B19 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B19
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use EF.DG1 with syntax error in date of expiry (3112AB): P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F**3112AB0**<<<<<<<<<<<<<<<8
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F**3112AB0**<<<<<<<<<<<<<<<8

8.2.20 LDS_B_20: Incorrect MRZ, date of expiry error

Test - ID	LDS_B_20
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (error in date of expiry)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B20 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID	CFG.BAC.LDS.B20
Purpose	This configuration is based on CFG.DFLT.BAC. The following files are

		modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use EF.DG1 with error in date of expiry (671331): P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F6713315<<<<<<<<<<<<<<<0
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F**6713315**<<<<<<<<<<<<<<<**0**

8.2.21 LDS_B_21: Incorrect MRZ, incorrect date of expiry checksum

Test - ID	LDS_B_21
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (incorrect checksum of date of expiry)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B21 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B21
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use EF.DG1 with incorrect checksum of date of expiry: P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F231031**8**<<<<<<<<<<<<<<<**8**
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F231031**8**<<<<<<<<<<<<<<<**8**

8.2.22 LDS_B_22: Incorrect MRZ, incorrect optional data checksum

Test - ID	LDS_B_22
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (incorrect checksum of optional data)
Version	1.0

Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	- Configuration profile CFG.BAC.LDS.B22 is loaded into the LT. - IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B22
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use EF.DG1 with incorrect checksum of optional data: P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314**ZE184226B**<<<<<**27**
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314**ZE184226B**<<<<<**27**

8.2.23 LDS_B_23: Incorrect MRZ, incorrect checksum

Test - ID	LDS_B_23
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (incorrect checksum of complete MRZ)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	- Configuration profile CFG.BAC.LDS.B23 is loaded into the LT. - IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B23
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use EF.DG1 with incorrect checksum of complete MRZ: P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<**3**

		Access conditions: read and select with BAC
	Data page MRZ	`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<` `C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<`**3**

8.2.24 LDS_B_24: Missing MRZ data object

Test - ID	LDS_B_24
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (missing MRZ data element)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B24 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.BAC.LDS.B24
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Missing data element in DG1: 6100
		Access conditions: read and select with BAC

8.2.25 LDS_B_25: Incomplete birth date (missing day)

Test - ID	LDS_B_25
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 stores an incomplete birth date (missing day)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B25 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.BAC.LDS.B25
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use EF.DG1 with incomplete birth date: P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608<<7F2310314<<<<<<<<<<<<<<<4
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608**<<7**F2310314<<<<<<<<<<<<<<<4

8.2.26 LDS_B_26: Incomplete birth date (missing month)

Test - ID	LDS_B_26
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 stores an incomplete birth date (missing month)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B26 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.BAC.LDS.B26
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use EF.DG1 with incomplete birth date: P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<96**<<**12**6**F2310314<<<<<<<<<<<<<<<**2**
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<96**<<**12**6**F2310314<<<<<<<<<<<<<<<**2**

8.2.27 LDS_B_27: Incomplete birth date (missing year)

Test - ID	LDS_B_27
Purpose	This test case verifies that the inspection system performs correctly if

	EF.DG1 stores an incomplete birth date (missing year)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B27 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.BAC.LDS.B27
Purpose		This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG1	Use EF.DG1 with incomplete birth date: P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<**<<**0812**1**F2310314<<<<<<<<<<<<<<<**8**
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<**<<**0812**1**F2310314<<<<<<<<<<<<<<<**8**

8.2.28 LDS_B_28: Incomplete birth date (missing complete dob)

Test - ID	LDS_B_28
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 stores an incomplete birth date (missing complete dob)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B28 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID	CFG.BAC.LDS.B28
Purpose	This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.

	EF.DG1	Use EF.DG1 with incomplete birth date: P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<**<<<<<<0**F2310314<<<<<<<<<<<<<<<**6**
		Access conditions: read and select with BAC
	Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<**<<<<<<0**F2310314<<<<<<<<<<<<<<<**6**

8.2.29 LDS_B_29: Format mismatch between EF.DG1 (TD1) and MRZ (TD2)

Test - ID	ISO7816_B_29
Purpose	This test verifies that the test object can detect a mismatch between MRZ and EF.DG1 where MRZ uses TD2 format and EF.DG1 uses TD1 format. Perform standard inspection procedure and read data groups from the lower tester.
Version	2.11
Reference	[ICAO Doc9303-11]
Profile	DG1
Preconditions	• Configuration profile CFG. BAC.LDS.B29 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID	CFG.BAC.LDS.B29
Purpose	This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The MRZ includes two lines (TD2) and EF.DG1 three lines (TD1).
Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<<4
EF.DG1	EF.DG1 must be encoded as TD1 formatted MRZ.

8.2.30 LDS_B_30: Format mismatch between EF.DG1 (TD2) and MRZ (TD1)

Test - ID	ISO7816_B_30
Purpose	This test verifies that the test object can detect a mismatch between MRZ and EF.DG1 where MRZ uses TD1 format and EF.DG1 uses TD2 format. Perform standard inspection procedure and read data groups from the lower tester.
Version	2.11
Reference	[ICAO Doc9303-11]
Profile	DG1
Preconditions	• Configuration profile CFG. BAC.LDS.B30 is loaded into the LT. • IS is „ready".

Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID	CFG.BAC.LDS.B30
Purpose	This configuration is based on CFG.DFLT.BAC. The following files are modified as specified below. The MRZ includes three lines (TD1) and EF.DG1 two lines (TD2).
Data page MRZ	P<D<<C11T002JM4<<<<<<<<<<<<<<< 9608122F2310314D<<<<<<<<<<<<<4 MUSTERMANN<<ERIKA<<<<<<<<<<<<<
EF.DG1	EF.DG1 must be encoded as TD2 formatted MRZ.

8.3 Unit LDS_C: Tests with EF.DG2

8.3.1 LDS_C_01: JPEG2000 image, full frontal

Test - ID	LDS_C_01
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 contains an image in JPEG2000 format
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG2
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

8.3.2 LDS_C_02: JPEG image, full frontal

Test - ID	LDS_C_02
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 contains an image in JPEG format
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG2
Preconditions	• Configuration profile CFG.PACE.LDS.C02 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.PACE.LDS.C02
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Facial image 1: **JPEG** of Erika Mustermann
		Access conditions: read and select with PACE

8.3.3 LDS_C_03: JPEG2000 image, full frontal with additional facial feature points

Test - ID	LDS_C_03
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 contains an image in JPEG2000 format with additional facial feature points

Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG2
Preconditions	• Configuration profile CFG.PACE.LDS.C03 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.PACE.LDS.C03
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Facial image 5: JPEG2000 of Erika Mustermann with additional facial feature points
		Access conditions: read and select with PACE

8.3.4 LDS_C_04: DG tag 75 wrong (tag 76 instead)

Test - ID	LDS_C_04
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (wrong tag 75, tag 76 instead)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG2
Preconditions	• Configuration profile CFG.PACE.LDS.C04 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C04
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with wrong tag 75 and tag 76 instead: `76823AE77F61823AE20201017F60823ADAA10...` JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.5 LDS_C_05: DG tag 75 length byte too small

Test - ID	LDS_C_05
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (length byte of tag 75 is too small)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG2
Preconditions	• Configuration profile CFG.PACE.LDS.C05 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C05
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with length byte of tag 75 is too small: 75**823AE6**7F61823AE20201017F60823ADAA10... JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.6 LDS_C_06: DG tag 75 length byte too big

Test - ID	LDS_C_06
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (length byte of tag 75 is too big)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG2
Preconditions	• Application profile CFG.PACE.LDS.C06 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID	CFG.PACE.LDS.C06
Purpose	This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.

	EF.DG2	Use EF.DG2 with length byte of tag 75 is too big: `75`**`823AE8`**`7F61823AE20201017F60823ADAA10...` JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.7 LDS_C_07: BIGT, missing tag for number of instances

Test - ID	LDS_C_07
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (missing number of BIT instances)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG2
Preconditions	• Configuration profile CFG.PACE.LDS.C07 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C07
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with missing tag for number of BIT instances. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.8 LDS_C_08: BHT, not allowed format owner

Test - ID	LDS_C_08
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (BHT, not allowed format owner)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG2
Preconditions	• Configuration profile CFG.PACE.LDS.C08 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C08
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with not allowed format owner in BHT. Use '0F0F' as not allowed format owner. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.9 LDS_C_09: BHT, missing format owner

Test - ID	LDS_C_09
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (BHT, missing format owner)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG2
Preconditions	• Configuration profile CFG.PACE.LDS.C09 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C09
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with missing format owner in BHT. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.10 LDS_C_10: BHT, not allowed format type

Test - ID	LDS_C_10
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (BHT, not allowed format type)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG2
Preconditions	• Configuration profile CFG.PACE.LDS.C10 is loaded into the LT. • IS is „ready“.

Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C10
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with not allowed format type in BHT (0009). JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.11 LDS_C_11: BHT, missing format type

Test - ID	LDS_C_11
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (BHT, missing format type)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG2
Preconditions	- Configuration profile CFG.PACE.LDS.C11 is loaded into the LT. - IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C11
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with missing format type in BHT. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.12 LDS_C_12: BHT, deprecated biometric type

Test - ID	LDS_C_12
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (BHT, incorrect biometric type)
Version	1.0

Reference	[ICAO Doc9303-10]
Profile	DG2
Preconditions	• Configuration profile CFG.PACE.LDS.C12 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C12
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect biometric type in BHT ('FF'). JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.13 LDS_C_13: BHT, incorrect biometric type

Test - ID	LDS_C_13
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (BHT, incorrect biometric type)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG2
Preconditions	• Configuration profile CFG.PACE.LDS.C13 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C13
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect biometric type in BHT ('01'). JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.14 LDS_C_14: FRH, incorrect format identifier

Test - ID	LDS_C_14
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FRH, incorrect format identifier)
Version	1.0
Reference	[ICAO Doc9303-10], [ISO/IEC 19794-5]
Profile	ISO19794-5
Preconditions	• Configuration profile CFG.PACE.LDS.C14 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C14
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect format identifier in FRH (46424300). JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.15 LDS_C_15: FRH, incorrect version number

Test - ID	LDS_C_15
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FRH, incorrect version number)
Version	1.0
Reference	[ICAO Doc9303-10], [ISO/IEC 19794-5]
Profile	ISO19794-5
Preconditions	• Configuration profile CFG.PACE.LDS.C15 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C15
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect version number in FRH ('30323000').

		JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.16 LDS_C_16: FIB, incorrect Facial Record Data Length due to additional feature points

Test - ID	LDS_C_16
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect Facial Record Data Length due to additional feature points)
Version	1.0
Reference	[ICAO Doc9303-10], [ISO/IEC 19794-5]
Profile	ISO19794-5
Preconditions	• Configuration profile CFG.PACE.LDS.C16 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C16
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect Facial Record Data Length due to additional feature points. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.17 LDS_C_17: FIB, incorrect gender

Test - ID	LDS_C_17
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect gender)
Version	1.0
Reference	[ICAO Doc9303-10], [ISO/IEC 19794-5]
Profile	ISO19794-5
Preconditions	• Configuration profile CFG.PACE.LDS.C17 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C17
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect gender in FIB. Set value to 03. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.18 LDS_C_18: FIB, incorrect eye colour

Test - ID	LDS_C_18
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect eye colour)
Version	1.0
Reference	[ICAO Doc9303-10], [ISO/IEC 19794-5]
Profile	ISO19794-5
Preconditions	• Configuration profile CFG.PACE.LDS.C18 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C18
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect eye colour in FIB. Set value to 08. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.19 LDS_C_19: FIB, incorrect hair colour

Test - ID	LDS_C_19
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect hair colour)
Version	1.0
Reference	[ICAO Doc9303-10], [ISO/IEC 19794-5]
Profile	ISO19794-5
Preconditions	• Configuration profile CFG.PACE.LDS.C19 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object.

	2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C19
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect hair colour in FIB. Set value to 08. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.20 LDS_C_20: FIB, incorrect Pose Angle – Yaw

Test - ID	LDS_C_20
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect pose angle - yaw)
Version	1.0
Reference	[ICAO Doc9303-10], [ISO/IEC 19794-5]
Profile	ISO19794-5
Preconditions	• Configuration profile CFG.PACE.LDS.C20 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C20
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect pose angel (yaw) in FIB. Set value to 182. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.21 LDS_C_21: FIB, incorrect Pose Angle – Pitch

Test - ID	LDS_C_21
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect pose angle - pitch)
Version	1.0
Reference	[ICAO Doc9303-10], [ISO/IEC 19794-5]

Profile	ISO19794-5
Preconditions	• Configuration profile CFG.PACE.LDS.C21 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C21
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect pose angel (pitch) in FIB. Set value to 182. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.22LDS_C_22: FIB, incorrect Pose Angle – Roll

Test - ID	LDS_C_22
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect pose angle - roll)
Version	1.0
Reference	[ICAO Doc9303-10], [ISO/IEC 19794-5]
Profile	ISO19794-5
Preconditions	• Configuration profile CFG.PACE.LDS.C22 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C22
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect pose angel (roll) in FIB. Set value to 182. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.23 LDS_C_23: FIB, incorrect Pose Angle Uncertainty - Yaw

Test - ID	LDS_C_23

Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect pose angle uncertainty - yaw)
Version	1.0
Reference	[ICAO Doc9303-10], [ISO/IEC 19794-5]
Profile	ISO19794-5
Preconditions	- Configuration profile CFG.PACE.LDS.C23 is loaded into the LT. - IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C23
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect pose angel uncertainty (yaw) in FIB. Set value to 182. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.24 LDS_C_24: FIB, incorrect Pose Angle Uncertainty – Pitch

Test - ID	LDS_C_24
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect pose angle uncertainty - pitch)
Version	1.0
Reference	[ICAO Doc9303-10], [ISO/IEC 19794-5]
Profile	ISO19794-5
Preconditions	- Configuration profile CFG.PACE.LDS.C24 is loaded into the LT. - IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C24
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect pose angel uncertainty (pitch) in FIB. Set value to 182. JPEG2000 of Erika Mustermann

		Access conditions: read and select with PACE

8.3.25 LDS_C_25: FIB, incorrect Pose Angle Uncertainty – Roll

Test - ID	LDS_C_25
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect pose angle uncertainty - roll)
Version	1.0
Reference	[ICAO Doc9303-10], [ISO/IEC 19794-5]
Profile	ISO19794-5
Preconditions	• Configuration profile CFG.PACE.LDS.C25 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C25
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect pose angel uncertainty (roll) in FIB. Set value to 182. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.26 LDS_C_26: IIB, incorrect face image type

Test - ID	LDS_C_26
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (IIB, incorrect face image type)
Version	1.0
Reference	[ICAO Doc9303-10], [ISO/IEC 19794-5]
Profile	ISO19794-5
Preconditions	• Configuration profile CFG.PACE.LDS.C26 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID	CFG.PACE.LDS.C26

Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect face image type in IIB. Set value to 03. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.27 LDS_C_27: IIB, incorrect image data type

Test - ID	LDS_C_27
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect image data type)
Version	1.0
Reference	[ICAO Doc9303-10], [ISO/IEC 19794-5]
Profile	ISO19794-5
Preconditions	• Configuration profile CFG.PACE.LDS.C27 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C27
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with incorrect image data type in IIB. Set value to 02. JPEG2000 of Erika Mustermann
		Access conditions: read and select with PACE

8.3.28 LDS_C_28: Missing facial image (tag 5F2E)

Test - ID	LDS_C_28
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (Missing facial image (tag 5F2E))
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	DG2
Preconditions	• Configuration profile CFG.PACE.LDS.C28 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.

Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.C28
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG2	Use EF.DG2 with missing facial image. Tag 5F2E must be deleted from DG2.
		Access conditions: read and select with PACE

8.4 Unit LDS_D: Tests with EF.SOD

8.4.1 LDS_D_01: Test signature support

Test - ID	LDS_D_01_template
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD contains RSA signature algorithm
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D01 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.PACE.LDS.D01
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: see Table 21 Digest algorithm: see Table 21 Signature algorithm: see Table 21 Signature generation: see Table 21 CSCA and DS certificates are based on algorithm as described in Table 21 in the complete chain
		Access conditions: read and select with PACE

Table 21 — Test case LDS_D_01[2]

Test - ID	***LDS security object digest algorithm***	***Digest algorithm***	***Signature algorithm***	***Country Signer***	***Document Signer***
LDS_D_01a	SHA-1	SHA-1	RSASSA-PSS	RSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_01b	SHA-256	SHA-256	RSASSA-PSS	RSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_01c	SHA-1	SHA-1	RSASSA-PKCS1_v15	RSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_01d	SHA-224	SHA-224	RSASSA-PKCS1_v15	RSA 3072 bit	RSA 2048 bit stored inside SOD

[2] The CSCA keys and DS keys may use the different algorithms in future amendment to Doc 9303-12.

Test - ID	*LDS security object digest algorithm*	*Digest algorithm*	*Signature algorithm*	*Country Signer*	*Document Signer*
LDS_D_01e	SHA-256	SHA-256	RSASSA-PKCS1_v15	RSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_01f	SHA-384	SHA-384	RSASSA-PKCS1_v15	RSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_01g	SHA-512	SHA-512	RSASSA-PKCS1_v15	RSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_01h	SHA-256	SHA-256	RSASSA-PKCS1_v15	RSA 3072 bit	RSA 2048 bit **NOT** stored inside SOD
LDS_D_01i	SHA-256	SHA-256	RSASSA-PSS	RSA 3072 bit	RSA 2048 bit **NOT** stored inside SOD
LDS_D_01j	SHA-1	SHA-1	DSA with SHA-1	DSA 3072 bit	DSA 2048 bit stored inside SOD
LDS_D_01k	SHA-1	SHA-1	ECDSA with SHA1	ECDSA 256 bit	ECDSA 224 bit stored inside SOD
LDS_D_01l	SHA-224	SHA-224	ECDSA with SHA224	ECDSA 256 bit	ECDSA 224 bit stored inside SOD
LDS_D_01m	SHA-256	SHA-256	ECDSA with SHA256	ECDSA 256 bit	ECDSA 256 bit stored inside SOD
LDS_D_01n	SHA-384	SHA-384	ECDSA with SHA384	ECDSA 384 bit	ECDSA 384 bit stored inside SOD
LDS_D_01o	SHA-512	SHA-512	ECDSA with SHA512	ECDSA 512 bit	ECDSA 512 bit stored inside SOD
LDS_D_01p	SHA-224	SHA-224	ECDSA with SHA224	ECDSA 256 bit	ECDSA224 bit **NOT** stored inside SOD
LDS_D_01q	SHA-224	SHA-224	DSA with SHA-224	DSA 3072 bit	DSA 2048 bit stored inside SOD
LDS_D_01r	SHA-256	SHA-256	DSA with SHA-256	DSA 3072 bit	DSA 2048 bit stored inside SOD
LDS_D_01u	SHA-256	SHA-256	DSA with SHA-256	RSA 3072 bit	DSA 2048 bit stored inside SOD
LDS_D_01v	SHA-256	SHA-256	ECDSA with SHA-256	RSA 2056 bit	ECDSA 256 bit stored inside SOD
LDS_D_01w	SHA-256	SHA-256	RSASSA-PKCS1_v15	DSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_01x	SHA-224	SHA-224	ECDSA with SHA-224	DSA 2056 bit	ECDSA 224 bit stored inside SOD
LDS_D_01y	SHA-384	SHA-384	RSASA-PSS	ECDSA 512 bit	RSA 3072 bit stored inside SOD
LDS_D_01z	SHA-256	SHA-256	DSA with SHA-256	ECDSA 384 bit	DSA 2048 bit stored inside SOD

8.4.2 LDS_D_02: DG tag 77 wrong (tag 78 instead)

Test - ID	LDS_D_02
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (DG tag 77 wrong, use tag 78 instead)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D02 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D02
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with DG tag 77 wrong, use tag 78 instead: **78**xxxxxx308204C206092A864886F70D010702A08204B330... LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.3 LDS_D_03: DG tag 77 length byte too small

Test - ID	LDS_D_03
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (length byte of DG tag 77 is too small)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D03 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.

Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D03
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with length byte of DG tag 77 is too small: 77**xxxxxx**308204C206092A864886F70D010702A08204B330... LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.4 LDS_D_04: DG tag 77 length byte too big

Test - ID	LDS_D_04
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (length byte of DG tag 77 is too big)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D04 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D04
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with length byte of DG tag 77 is too big: 77**xxxxxx**308204C206092A864886F70D010702A08204B330... LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA

		2048 bit
		Access conditions: read and select with PACE

8.4.5 LDS_D_05: SignedData version incorrect

Test - ID	LDS_D_05
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignedData version incorrect)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D05 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D05
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with incorrect SignedData version. Use '0F' as invalid version. LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.6 LDS_D_06: SignedData version missing

Test - ID	LDS_D_06
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignedData version missing)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D06 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.

Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D06
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with missing SignedData version. LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.7 LDS_D_07: SignedData illegal digestAlgorithm (MD5)

Test - ID	LDS_D_07
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignedData with illegal digest algorithm)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D07 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D07
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with illegal digestAlgorithm in SignedData (MD5) LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: **MD5** Digest algorithm: **MD5** Signature algorithm: RSASSA-PSS with **MD5** DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit

		Access conditions: read and select with PACE

8.4.8 LDS_D_08: SignedData missing digestAlgorithm list

Test - ID	LDS_D_08
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignedData missing digestAlgorithm list)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D08 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D08
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with missing digestAlgorithm list in SignedData LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.9 LDS_D_09: SignedData incorrect content type OID for id-icao-ldsSecurityObject

Test - ID	LDS_D_09
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignedData incorrect content type OID for id-icao-ldsSecurityObject)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D09 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.

Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D09
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with incorrect content type OID for id-icao-ldsSecurityObject in SignedData. Use content type OID with last byte changed is to 'FF'. LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.10 LDS_D_10: SignedData missing content type OID for id-icao-ldsSecurityObject

Test - ID	LDS_D_10
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignedData missing content type OID for id-icao-ldsSecurityObject
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D10 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D10
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with missing content type OID for id-icao-ldsSecurityObject in SignedData LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA

		2048 bit
		Access conditions: read and select with PACE

8.4.11 LDS_D_11: SignerInfo, incorrect signer info version value

Test - ID	LDS_D_11
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignerInfo, incorrect signer info version value)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D11 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D11
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with incorrect signer info version value in SignerInfo. Use '0F' as incorrect version. LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.12 LDS_D_12: SignerInfo, missing signer info version

Test - ID	LDS_D_12
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignerInfo, missing signer info version)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D12 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object.

	2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D12
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with missing signer info value in SignerInfo. LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.13 LDS_D_13: SignerInfo, Version 1 and incorrect issuerAndSerialNumber

Test - ID	LDS_D_13
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignerInfo, Version 1 with incorrect issuerAndSerialNumber)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D13 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D13
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with Version 1 with incorrect issuerAndSerialNumber in SignerInfo LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD

		Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.14 LDS_D_14: SignerInfo, Version 3 and incorrect subjectKeyIdentifier

Test - ID	LDS_D_14
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignerInfo, Version 3 with incorrect subjectKeyIdentifier)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D14 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D14
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with Version 3 with incorrect subjectKeyIdentifier in SignerInfo LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.15 LDS_D_15: SignerInfo, illegal digestAlgorithm

Test - ID	LDS_D_15
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignerInfo, not allowed digestAlgorithm)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D15 is loaded into the LT. • IS is „ready“.

Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D15
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with not allowed digestAlgorithm in SignerInfo (e.g. RIPEMD, MD5) LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.16 LDS_D_16: SignerInfo, missing digestAlgorithm

Test - ID	LDS_D_16
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignerInfo, missing digestAlgorithm)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D16 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D16
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with missing digestAlgorithm in SignerInfo LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD

		Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.17 LDS_D_17: SignerInfo, incorrect messageDigest attribute value

Test - ID	LDS_D_17
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignerInfo, incorrect messageDigest attribute value)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D17 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D17
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with incorrect messageDigest attribute value in SignerInfo. Change the last byte of the attribute value to 'FF' (e.g. 301506092A864886F70D0109FF). LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.18 LDS_D_18: SignerInfo, missing messageDigest attribute

Test - ID	LDS_D_18
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignerInfo, missing messageDigest attribute)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D18 is loaded into the LT. • IS is „ready".

Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D18
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with missing messageDigest attribute in SignerInfo LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.19 LDS_D_19: SignerInfo, incorrect Signature

Test - ID	LDS_D_19_template
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignerInfo contains incorrect Signature). Check that IS verifies all signature schemes.
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D19 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D19
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with incorrect Signature in SignerInfo. Use signature with last byte added by 1. LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: see Table 22 Digest algorithm: see Table 22 Signature algorithm: see Table 22

		CSCA and DS certificates are based on algorithm as described in Table 22 in the complete chain.
		Access conditions: read and select with PACE

Table 22 — Test case LDS_D_19[3]

Test - ID	*LDS security object digest algorithm*	*Digest algorithm*	*Signature algorithm*	*Country Signer*	*Document Signer*
LDS_D_19a	SHA-1	SHA-1	RSASSA-PSS	RSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_19b	SHA-256	SHA-256	RSASSA-PSS	RSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_19c	SHA-1	SHA-1	RSASSA-PKCS1_v15	RSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_19d	SHA-224	SHA-224	RSASSA-PKCS1_v15	RSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_19e	SHA-256	SHA-256	RSASSA-PKCS1_v15	RSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_19f	SHA-384	SHA-384	RSASSA-PKCS1_v15	RSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_19g	SHA-512	SHA-512	RSASSA-PKCS1_v15	RSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_19h	SHA-256	SHA-256	RSASSA-PKCS1_v15	RSA 3072 bit	RSA 2048 bit **NOT** stored inside SOD
LDS_D_19i	SHA-256	SHA-256	RSASSA-PSS	RSA 3072 bit	RSA 2048 bit **NOT** stored inside SOD
LDS_D_19j	SHA-1	SHA-1	DSA with SHA-1	DSA 3072 bit	DSA 2048 bit stored inside SOD
LDS_D_19k	SHA-1	SHA-1	ECDSA with SHA-1	ECDSA 256 bit	ECDSA 224 bit stored inside SOD
LDS_D_19l	SHA-224	SHA-224	ECDSA with SHA-224	ECDSA 256 bit	ECDSA 224 bit stored inside SOD
LDS_D_19m	SHA-256	SHA-256	ECDSA with SHA-256	ECDSA 256 bit	ECDSA 256 bit stored inside SOD
LDS_D_19n	SHA-384	SHA-384	ECDSA with SHA-384	ECDSA 384 bit	ECDSA 384 bit stored inside SOD
LDS_D_19o	SHA-512	SHA-512	ECDSA with SHA-512	ECDSA 512 bit	ECDSA 512 bit stored inside SOD
LDS_D_19p	SHA-224	SHA-224	ECDSA with	ECDSA 256 bit	ECDSA 224 bit

[3] The CSCA keys and DS keys may use the different algorithms in future amendment to Doc 9303-12.

Test - ID	*LDS security object digest algorithm*	*Digest algorithm*	*Signature algorithm*	*Country Signer*	*Document Signer*
			SHA-224		**NOT** stored inside SOD
LDS_D_19q	SHA-224	SHA-224	DSA with SHA-224	DSA 3072 bit	DSA 2048 bit stored inside SOD
LDS_D_19r	SHA-256	SHA-256	DSA with SHA-256	DSA 3072 bit	DSA 2048 bit stored inside SOD
LDS_D_19u	SHA-256	SHA-256	DSA with SHA-256	RSA 3072 bit	DSA 2048 bit stored inside SOD
LDS_D_19v	SHA-256	SHA-256	ECDSA with SHA-256	RSA 2056 bit	ECDSA 256 bit stored inside SOD
LDS_D_19w	SHA-256	SHA-256	RSASSA-PKCS1_v15	DSA 3072 bit	RSA 2048 bit stored inside SOD
LDS_D_19x	SHA-224	SHA-224	ECDSA with SHA-224	DSA 2056 bit	ECDSA 224 bit stored inside SOD
LDS_D_19y	SHA-384	SHA-384	RSASA-PSS	ECDSA 512 bit	RSA 3072 bit stored inside SOD
LDS_D_19z	SHA-256	SHA-256	DSA with SHA-256	ECDSA 384 bit	DSA 2048 bit stored inside SOD

8.4.20 LDS_D_20: SignerInfo, missing Signature

Test - ID	LDS_D_20
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (SignerInfo: missing signature)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D20 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D20
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with missing Signature in SignerInfo LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256

		DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.21 LDS_D_21: LDS Security Object, incorrect security object version

Test - ID	LDS_D_21
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (LDS Security Object, incorrect security object)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D21 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D21
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with incorrect security object in LDS Security Object. LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.22 LDS_D_22: LDS Security Object, missing security object version

Test - ID	LDS_D_22
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (LDS Security Object, missing security object version)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D22 is loaded into the LT. • IS is „ready“.

Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D22
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with missing security object in LDS Security Object LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.23 LDS_D_23: LDS Security Object, illegal digestAlgorithm

Test - ID	LDS_D_23
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (LDS Security Object, not allowed digestAlgorithm)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D23 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D23
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with not allowed digestAlgorithm in LDS Security Object (MD5) LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: **MD5** Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD

		Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.24 LDS_D_24: LDS Security Object, missing digestAlgorithm

Test - ID	LDS_D_24
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (LDS Security Object, missing digestAlgorithm)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D24 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D24
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with missing digestAlgorithm in LDS Security Object LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.25 LDS_D_25: LDS Security Object, incorrect DataGroup Hash value for DG2

Test - ID	LDS_D_25
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (LDS Security Object, incorrect DataGroup Hash value for DG2)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D25 is loaded into the LT. • IS is „ready".

Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D25
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with incorrect DataGroup Hash value for DG2 in LDS Security Object LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.26 LDS_D_26: LDS Security Object, missing DataGroup Hash value for DG1

Test - ID	LDS_D_26
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (LDS Security Object, missing DataGroup Hash value for DG1)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D26 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D26
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with missing DataGroup Hash value for DG1 in LDS Security Object LDS security object containing hash values of DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256

		Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.27 LDS_D_27: DS certificate, incorrect certificate version

Test - ID	LDS_D_27
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (DS certificate, incorrect certificate version)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D27 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D27
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with incorrect certificate version in DS certificate. The certificate version is '0201FF' LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.28 LDS_D_28: DS certificate, missing certificate version

Test - ID	LDS_D_28
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (DS certificate, missing certificate version)
Version	1.0
Reference	[ICAO Doc9303-10]

Profile	SIP
Preconditions	- Configuration profile CFG.PACE.LDS.D28 is loaded into the LT. - IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D28
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with missing certificate version in DS certificate LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with BAC

8.4.29 LDS_D_29: DS certificate, incorrect issuer element (naming convention does not follow ICAO)

Test - ID	LDS_D_29
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (DS certificate, incorrect issuer element (naming convention does not follow ICAO))
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	- Configuration profile CFG.PACE.LDS.D29 is loaded into the LT. - IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D29
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with incorrect issuer element (naming convention does not

		follow ICAO) in DS certificate AND in SOD (SignerInfo: signerIdentifier (sid)): Use invalid country code with three letters 'DDD'. Correct codes can be found in [ISO/IEC 3166]. LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.30 LDS_D_30: DS certificate, incorrect signatureValue

Test - ID	LDS_D_30
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (DS certificate, incorrect signatureValue (last bit flipped))
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D30 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D30
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with incorrect signatureValue (last bit flipped) in DS certificate LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.31 LDS_D_31: DS certificate, missing signatureValue

Test - ID	LDS_D_31
Purpose	This test case verifies that the inspection system performs correctly if

	EF.SOD is wrong (DS certificate, missing signatureValue)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D31 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D31
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with missing signatureValue in DS certificate LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.32 LDS_D_32: Passive Authentication with revocation list

Test - ID	LDS_D_32
Purpose	This test verifies that the inspection system recognizes a revoked certificate during passive authentication. Perform standard inspection procedure and read BAC protected data groups from the lower tester.
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC is loaded into the LT. • Load a revocation list (CRL) into the IS that revoke the certificate of the LT (see section 7.2 of [ICAO Doc9303-12]). • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started. 3. The LT uses a revoked certificate that the IS MUST deny.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

8.4.33 LDS_D_33: LDS Security Object, incorrect DataGroup Hash value for DG14

Test - ID	LDS_D_33
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (LDS Security Object, incorrect DataGroup Hash value for DG14)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D33 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D33
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with incorrect DataGroup Hash value for DG14 in LDS Security Object LDS security object containing hash values of DG1, DG2 and DG14 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE

8.4.34 LDS_D_34: LDS Security Object, missing DataGroup Hash value for DG14

Test - ID	LDS_D_34
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD is wrong (LDS Security Object, missing DataGroup Hash value for DG14)
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D34 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D34
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.SOD	Use EF.SOD with missing DataGroup Hash value for DG14 in LDS Security Object LDS security object containing hash values of DG1 and DG2 LDS security object digest algorithm: SHA 256 Digest algorithm: SHA 256 Signature algorithm: RSASSA-PSS with SHA256 DS certificate contained in SOD Signature generation: Country Signer RSA 3072 bit, Document Signer RSA 2048 bit
		Access conditions: read and select with PACE / BAC

8.4.35 LDS_D_35: EF.SOD with LDS Version 1.8

Test - ID	LDS_D_35
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD contains an additional security object with LDS in version 1.8.
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D35 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful.

ID		CFG.PACE.LDS.D35
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	*EF.SOD*	Additional LDSVersionInfo: ldsVersion 1.8 LDSSecurityObjectVersion 1
		Access conditions: read and select with PACE / BAC

8.4.36 LDS_D_36: Security Object with LDS Version 1.8 but wrong LDSSecurityObjectVersion

Test - ID	LDS_D_36
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD contains an additional security object with LDS in version 1.8 but wrong version number V=0.

Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D36 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D36
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.SOD***	Additional LDSVersionInfo: ldsVersion 1.8 LDSSecurityObjectVersion 0
		Access conditions: read and select with PACE / BAC

8.4.37 LDS_D_37: Security Object with LDS Version 1.7 but LDSSecurityObjectVersion 1

Test - ID	LDS_D_37
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD contains an additional security object with LDS in version 1.7 but version number V=1.
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D37 is loaded into the LT. • IS is „ready".
Test scenario	3. Place test data page onto the test object. 4. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D37
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
Content	***EF.SOD***	Additional LDSVersionInfo: ldsVersion 1.7 LDSSecurityObjectVersion 1
		Access conditions: read and select with PACE / BAC

8.4.38 LDS_D_38: EF.SOD with future LDS Version 1.9

Deleted in version 2.11

8.4.39 LDS_D_39: Check signature validation of EF.CardSecurity

Test - ID	LDS_D_39
Purpose	This test case verifies that the inspection system checks the signature in EF.CardSecurity and detects an invalid signature.
Version	2.11
Reference	[ICAO Doc9303-10]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.D39 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.D39
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The signature of EF.CardSecurity must be invalid.
Content	***EF.CardSecurity***	Invalid signature
		Access conditions: read and select with PACE / BAC

8.5 Unit LDS_E: Tests with EF.DG15

8.5.1 LDS_E_01: DG tag 6F wrong (use tag 70 instead)

Test - ID	LDS_E_01
Purpose	This test case verifies that the inspection system performs Active Authentication with wrong tag in data group.
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	AA
Preconditions	• Configuration profile CFG.PACE.LDS.E01 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.E01
Purpose		This configuration is based on CFG.DFLT.PACEAA. The following files are modified as specified below. The hash values of the LDS security object MUST be updated to obtain a valid and authentic configuration.
	EF.DG15	Use EF.DG15 with wrong tag: **70**81A130819E300D0609... Signature algorithm: RSA with SHA1
		Access conditions: read and select with PACE

8.5.2 LDS_E_02: DG tag length too small

Test - ID	LDS_E_02
Purpose	This test case verifies that the inspection system performs correctly if EF.DG15 is wrong (length byte of tag 6F is too small).
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	AA
Preconditions	• Configuration profile CFG.PACE.LDS.E02 is loaded into the LT. • IS is „ready“.
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID	CFG.PACE.LDS.E02
Purpose	This configuration is based on CFG.DFLT.PACEAA. The following files are modified as specified below. The hash values of the LDS security object MUST be updated to obtain a valid and authentic configuration.

	EF.DG15	Use EF.DG15 with tag length too small: 6F**81A0**30819E300D0609... Signature algorithm: RSA with SHA1
		Access conditions: read and select with PACE

8.5.3 LDS_E_03: DG tag length too big

Test - ID	LDS_E_03
Purpose	This test case verifies that the inspection system performs correctly if EF.DG15 is wrong (length byte of tag 6F is too big).
Version	1.0
Reference	[ICAO Doc9303-10]
Profile	AA
Preconditions	• Configuration profile CFG.PACE.LDS.E03 is loaded into the LT. • IS is „ready".
Test scenario	1. Place test data page onto the test object. 2. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.E03
Purpose		This configuration is based on CFG.DFLT.PACEAA. The following files are modified as specified below. The hash values of the LDS security object MUST be updated to obtain a valid and authentic configuration.
	EF.DG15	Use EF.DG15 with tag length too big: 6F**81A2**30819E300D0609... Signature algorithm: RSA with SHA1
		Access conditions: read and select with PACE

8.6 Unit LDS_F: Tests with EF.DG14

8.6.1 LDS_F_01: DG tag 6E wrong (tag 6F instead)

Test - ID	LDS_F_01
Purpose	This test case verifies that the inspection system performs correctly if EF.DG14 is wrong (tag 6E wrong, use tag 6F instead)
Version	1.0
Reference	[ICAO Doc9303-10], [ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.F01 is loaded into the LT. • IS is „ready".
Test scenario	1) Place test data page onto the test object. 2) Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.F01
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG14	Use EF.DG14 with wrong tag 6E, use tag 6F instead: **6F**<length[4]>3182014630820122060904007F000702... Key agreement algorithm: id-CA-ECDH-3DES-CBC-CBC Key reference: none
		Access conditions: read and select with BAC / PACE

8.6.2 LDS_F_02: DG tag 6E length byte too small

Test - ID	LDS_F_02
Purpose	This test case verifies that the inspection system performs correctly if EF.DG14 is wrong (length byte of tag 6E is too small)
Version	1.0
Reference	[ICAO Doc9303-10], [ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.F02 is loaded into the LT. • IS is „ready“.
Test scenario	1) Place test data page onto the test object. 2) Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.F02
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG14	Use EF.DG14 with length byte of tag 6E is too small: 6E**<length -1>**3182014630820122060904007F000702... Key agreement algorithm: id-CA-ECDH-3DES-CBC-CBC Key reference: none
		Access conditions: read and select with BAC / PACE

8.6.3 LDS_F_03: DG tag 6E length byte too big

Test - ID	LDS_F_03
Purpose	This test case verifies that the inspection system performs correctly if EF.DG14 is wrong (length byte of tag 6E is too big)
Version	1.0

[4] <length> is the length of EF.DG14 to be encoded.

Reference	[ICAO Doc9303-10], [ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.F03 is loaded into the LT. • IS is „ready“.
Test scenario	1) Place test data page onto the test object. 2) Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.F03
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG14	Use EF.DG14 with length byte of tag 6E is too big: 6E**<length +1>**3182014630820122060904007F000702... Key agreement algorithm: id-CA-ECDH-3DES-CBC-CBC Key reference: none
		Access conditions: read and select with BAC / PACE

8.6.4 LDS_F_04: Check consistency (EF.CardAccess and EF.DG14), no PACEInfo in CardAccess but DG14

Test - ID	LDS_F_04
Purpose	This test case verifies that the inspection system checks consistency between EF.CardAcces and EF.DG14 EF.CardAccess doesn't contain any PACEInfo but EF.DG14 does contain a valid PACEInfo.
Version	1.0
Reference	[ICAO Doc9303-10], [ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.EAC.LDS.F04 is loaded into the LT. • IS is „ready“.
Test scenario	1) Place test data page onto the test object. 2) Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.F04
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.CardAccess	Contains no PACEInfo nor PACEDomainParameterInfo
		Access conditions: read and select always

	EF.DG14	Contains one PACEInfo: protocol: id-PACE-ECDH-GM-3DES-CBC-CBC version: 2 parameterId: 13
		Access conditions: read and select with BAC / PACE

8.6.5 LDS_F_05: Check consistency (EF.CardAccess and EF.DG14), no PACEInfo in CardAccess, DG14 is absent

Test - ID	LDS_F_05
Purpose	This test case verifies that the inspection system checks consistency between EF.CardAcces and EF.DG14 EF.CardAccess doesn't contain any PACEInfo and EF.DG14 is absent
Version	1.0
Reference	[ICAO Doc9303-10], [ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.EAC.LDS.F05 is loaded into the LT. • IS is „ready".
Test scenario	1) Place test data page onto the test object. 2) Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.F05
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.CardAccess	Contains no PACEInfo nor PACEDomainParameterInfo
		Access conditions: read and select always
	EF.DG14	EF.DG14 is absent

8.6.6 LDS_F_06: Check consistency (EF.CardAccess and EF.DG14), PACEInfo in CardAccess and DG14 different

Test - ID	LDS_F_06
Purpose	This test case verifies that the inspection system checks consistency between EF.CardAcces and EF.DG14 The parameters of PACEInfo in EF.CardAccess are different from the parameters of PACEInfo in DG14.
Version	1.0
Reference	[ICAO Doc9303-10], [ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.EAC.LDS.F06 is loaded into the LT. • IS is „ready".

Test scenario	1) Place test data page onto the test object. 2) Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.F06
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.DG14	Contains one PACEInfo: protocol: id-PACE-DH-GM-3DES-CBC-CBC version: 2 parameterId: 2
		Access conditions: read and select with BAC / PACE

8.6.7 LDS_F_07: Check consistency (EF.CardAccess and EF.DG14), CardAccess is absent but DG14 contains valid PACEInfo

Test - ID	LDS_F_07
Purpose	This test case verifies that the inspection system checks consistency between EF.CardAcces and EF.DG14 EF.CardAccess is absent but EF.DG14 contains a valid PACEInfo element
Version	1.0
Reference	[ICAO Doc9303-10], [ICAO Doc9303-11]
Profile	SIP
Preconditions	• Configuration profile CFG.EAC.LDS.F07 is loaded into the LT. • IS is „ready“.
Test scenario	1) Place test data page onto the test object. 2) Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

ID		CFG.PACE.LDS.F07
Purpose		This configuration is based on CFG.DFLT.PACE. The following files are modified as specified below. The hash values of the LDS security object and the signature of the SOD MUST be updated to obtain a valid and authentic configuration.
	EF.CardAccess	EF.CardAccess is absent
	EF.DG14	Contains one PACEInfo: protocol: id-PACE-ECDH-GM-3DES-CBC-CBC version: 2 parameterId: 13
		Access conditions: read and select with BAC / PACE

Bibliography

[1] AFNOR, *Automatic Interface Specification*

[2] BSI TR-03105 Part 5.1, *Test plan for ICAO compliant Inspection Systems with EAC*