International Civil Aviation Organization

TAG/MRTD/22-WP/9
16/04/14
English Only

WORKING PAPER

TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS (TAG/MRTD)

TWENTY-SECOND MEETING

Montréal, 21 to 23 May 2014

Agenda Item 2: Activities of the NTWG

TECHNICAL REPORT ON RF PROTOCOL TESTING PART 4

(Presented by the New Technologies Working Group)

1. INTRODUCTION

This document describes the work ongoing within ICAO and ISO SC17/WG3 on new test methodologies for inspection systems for electronic machine-readable travel documents (eMRTDs).

2. BACKGROUND

2.1 An essential element of ICAO compliant MRTDs is the addition of a contactless Proximity Integrated Circuit (PIC) that will securely hold biometric data of the MRTD bearer within the ICAO defined Logical Data Structure (LDS). Successful integration of the PIC into the MRTD and the integration of a Proximity Coupling Device (PCD) into an inspection system depends upon active

2.2 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 organisations involved minimise the probability that this error or fault is undetected before the design is approved and inspection systems are issued.

2.3 For a fully interoperable MRTD solution, it is not only the PCD hardware with the contactless interface which is important. It is also critical that the application of the inspection system complies with the relevant ISO and ICAO standards. Therefore, this document proposes a test plan to verify the application part of the inspection system.

3. CURRENT STATUS

3.1 The work has been finished. The tests comprise Basic Access Control (BAC), Password Authenticated Connection Establishment (PACE), Secure Messaging, Active Authentication (AA), and Handling of the LDS including Passive Authentication.

3.2 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.

3.3 Once endorsed by the TAG/MRTD this version will be put into the process of ISO balloting and is anticipated to become part of the ISO/IEC 18745 series of test standards for MRTDs in 2015 to reflect latest related standards.

4. ACTION BY THE TAG/MRTD

4.1 The TAG/MRTD is invited to approve and publish the TR.

4.2 Endorse the continued work at ISO/IEC JTC1/SC17/WG3 on the resulting international standard ISO/IEC 18745-4.

— END —

MACHINE READABLE TRAVEL DOCUMENTS

TECHNICAL REPORT

RF protocol and application test standard for eMRTD - part 4

Conformity test for inspection systems

Version – 1.01

File	: TR - RF and Protocol Testing Part 4 V1.01 20131125.docTR - RF and Protocol Testing Part 4 V1.01 20131125.docTR - RF and Protocol Testing Part 4 V1.00 20131119.docTR - RF and Protocol Testing Part 4 V1.00 20131105.doc
Author	: ISO/IEC JTC1 SC17 WG3/TF5

Release Control

Release	***Date***	***Description***
0.1	2012-02-23	First version based on TR-03105 parts 5.1/5.2
0.2	2012-05-07	Merged with the test cases from SOLIATIS "Inspection System conformity tests for SAC (PACE v2)" Version 0.3
0.3	2012-08-16	Some changes based on the comments of Keolabs (2012-08-13) and Morpho (2012-08-13)
0.4	2012-09-28	Changes based on comments from AFNOR and Japan were implemented
0.5	2012-10-24	Implemented comments which were clarified in the 45th Meeting of ISO/IEC JTC1/SC17 WG 3, held in New Orleans Rearranged test cases
0.6	2013-10-11	Implemented comments which were clarified in the meeting of ISO/IEC JTC1/SC17 WG 3, held in Singapore
1.0	2013-11-05	ICAO submission
1.01	2013-11-26	Update of expiry date in MRZ and DG1 data set

Table of Contents

Introduction

Scope and purpose

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 depends 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.

For a fully interoperable MRTD solution, it is not only the PCD hardware with the contactless interface which is important. It is also critical that the application of the inspection system complies with the ISO and ICAO standards (e.g. [10] and [4]).Therefore, this document proposes a test plan to verify the application part of the inspection system. The tests comprise

- Basic Access Conrol
- PACE
- Secure Messaging
- Active Authentication
- 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 [10] 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.

Terminology

The key words "MUST", “MUST NOT”, "SHALL", “SHALL NOT”, "REQUIRED", "SHOULD", “SHOULD NOT”, "RECOMMENDED", "MAY", and “OPTIONAL” in this document are to be interpreted as described in [11].

Definitions and 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
CAN	Card Access Number
C-APDU	Command APDU
DGPM	Data Group Presence Map
DH	Diffie-Hellman
DUT	Device under test
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
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
SSC	Send sequence counter
UT	Upper tester

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 [5]. These two interfaces are needed because the inspection system initiates and controls the communication sequence. The following figure 1 illustrates this concept.

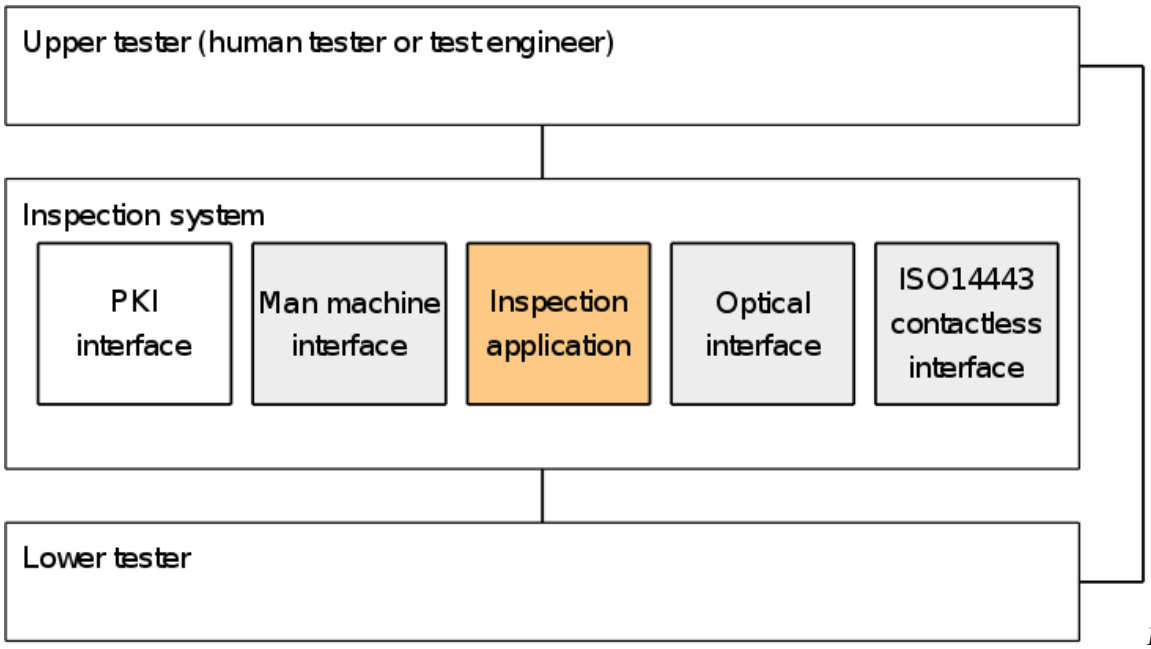

Figure 11111111: Upper and lower tester of the test environment

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.

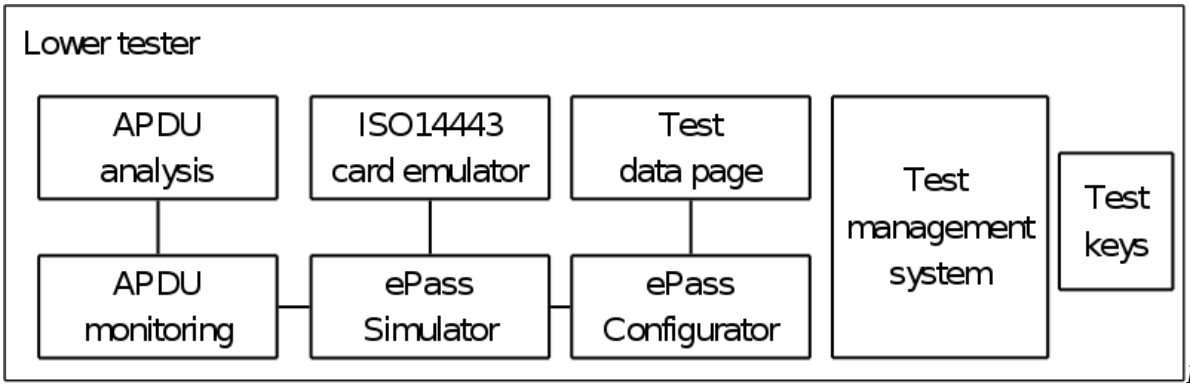

Figure 22222222: Functional components of the lower tester

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 [4]. 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 [5]. 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 [9] file system (number and size of files) to store the data groups
- Large transparent file as specified in [9] with size larger than 32k.
- The ISO/IEC 7816-4 application commands defined by [4] and [3].
- 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.

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.

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

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.

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.
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.
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 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 [8][1].

Table 1: Profiles to be tested for specified inspection system

The applicant SHALL fill in the following implementation conformance statement.

Information for test setup	***Profile-ID***	***Applicant declaration***
IS supports standard inspection procedure (mandatory).	SIP	
IS supports SIP with CAN	CAN	
IS supports active authentication	AA	
IS performs checks on DG1 contents.	DG1	

[1] Note: As specified in [4], always the lastet version of [8] is to use.

IS performs checks on DG2 contents.	DG2
IS verifies ISO/IEC 19794-6 [8] information in DG2.	ISO19794-5

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

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, this conformity test uses only "<".

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 0): JPEG2000 of Erika Mustermann Access conditions: read and select always
Data page MRZ		P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<4

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 0): JPEG2000 of Erika Mustermann Access conditions: read and select with BAC
Data page MRZ		`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<` `C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<4`

Configuration of default PACE protected MRTD

ID		CFG.DFLT.PACE
Purpose		This configuration defines a default PACE protected MRTD.
MF		
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 0): 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

Configuration of default PACE and AA MRTD

ID		CFG.DFLT.PACEAA
Purpose		This configuration defines a default PACE protected MRTD with Active Authentication.
MF		
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 0): 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

Definition of biometric data

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

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

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.

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.

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.

Layer 6 tests (Application protocol tests)

Unit ISO7816_A: Test of Application Selection

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	0.5
Reference	[4]
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.

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	0.5
Reference	[4]
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.

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	0.5
Reference	[4], [3]
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.

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 a invalid ICAO AID.
Version	0.5
Reference	[4]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC is loaded into the LT with the following modification: The installed ICAO application has an invaild 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 invaild 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.

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 a invalid ICAO AID.
Version	0.5
Reference	[4]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT with the following modification: The installed ICAO application has an invaild 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 invaild 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.

Unit ISO7816_B: Test of Basic Access Control

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	0.5
Reference	[4]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC is loaded into the LT. • Modification: the MUTUAL AUTHENTICATE command SHALL use a manipulated KMAC – last byte of the KMAC 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.

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	0.5
Reference	[4]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC is loaded into the LT. • Modification: the MUTUAL AUTHENTICATE command SHALL use

	a manipulated KENC – last byte of the KENC 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 session keys computed by the IS are not correct and the failure occurs in the next command because the the chip is not able to verify the MAC. The failure occurs in the next command (read EF:COM).
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

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	0.5
Reference	[4]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC is loaded into the LT. • The BAC keys KENC and KMAC 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.

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 [3] chapter 2.2).

According to [TR-SAC] [3] Version 1.01 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 per-

formed, the LT SHALL deny the selection of the ePassport-Application in all test cases by returning SW '69 82' until PACE performed successful.

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).

ISO7816_C_01: Correct execution of PACE protocol

Test - ID	ISO7816_C_01
Purpose	Check correct execution of PACE protocol in the terminal. The test is executed with CAN and/or MRZ.
Version	0.5
References	[3] 2.3, 3.2.1, 3.3
Profile	See table 3
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.
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.

Test - ID	***Profiles***	***Password***	*<DO83>*
ISO7816_C_01a	SIP	Use PACE with MRZ	`'01'`
ISO7816_C_01b	SIP, CAN	Use PACE with CAN	`'02'`

Table 3: Test case ISO7816_C_01

ISO7816_C_02: Check supported standardized Domain Parameters with Generic Mapping

Test - ID	ISO7816_C_02
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	0.5
References	[3] 2.3, 3.2
Profile	SIP

Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Use exact one PACEInfo with standardized domain parameter (see table 4) 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.

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

Table 4: Test case ISO7816_C_02

ISO7816_C_03: Check supported standardized Domain Parameters with Integrated Mapping

Test - ID	ISO7816_C_03
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	0.5
References	[3] 2.3, 3.2,
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT. • Use exact one PACEInfo with standardized domain parameter (see table 5) 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.

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

Table 5: Test case ISO7816_C03

ISO7816_C_04: Check supported algorithms

Test - ID	ISO7816_C_04
Purpose	Check correct execution of PACE protocol in the test object. The test has to be executed for each PACE algorithm specified in [3]. 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	0.5
References	[3] 2.3, 3.2,
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 the OID from table 6 as protocol in PACEInfo. The DomainParameters SHOULD be the same for all test runs. • 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.

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
ISO7816_C_04m	id-PACE-ECDH-IM-3DES-CBC-CBC
ISO7816_C_04n	id-PACE-ECDH-IM-AES-CBC-CMAC-128

Test - ID	*Algorithm OID*
ISO7816_C_04o	id-PACE-ECDH-IM-AES-CBC-CMAC-192
ISO7816_C_04p	id-PACE-ECDH-IM-AES-CBC-CMAC-256

Table 6: Test case ISO7816_C_04

ISO7816_C_05:Supplemental Access Control with additional entries in SecurityInfos

Test – ID	ISO7816_C_05
Purpose	Positive test with Supplemental Access Control with additional entries in SecurityInfos which should be ignored by the IS.
Version	0.5
References	[3]
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.

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	0.5
References	[3] 2.3, 3.2
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 [3]. 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.

ISO7816_C_07: EF.CardAccess contains two PACEInfo and PACEDomainParameter

Test - ID	ISO7816_C_07
Purpose	Positive test with EF.CardAccess containing two PACEInfo and one PACEDomainParameter. Check that IS can handle two different PACE parameters and perform one possible option.
Version	0.5
References	[3]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LT with following modifications: • Use two different PACEInfo objects and one PACEDomainParameter object in EF.CardAccess with different algorithms in PACEInfo. Use one standardized domain parameter identifier (parameterId: between 0 and 18)in the first PACEInfo. In the second PACEInfo the parameterID SHALL indicate proprietary domain parameters (parameterID above 31). The PACEDomainParameter object MUST contain valid parameters. The algorithms and domain parameters MUST be vaild parameters as described in [3]. • 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.

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

Test - ID	ISO7816_C_08
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	0.2

References	[3] 3.2.1
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.

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

Table 7: Test case ISO7816_C_08

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	0.5
References	[3]
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.

ISO7816_C_10: Error on General Authenticate step 1 command

Test – ID	ISO7816_C_10
Purpose	Negative test: Error on General Authenticate step 1command
Version	0.5
References	[3]
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.`

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

Table 8: Test case ISO7816_C_10

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	0.5
References	[3]
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.`

ISO7816_C_12: Error on General Authenticate step 2 command

Test – ID	ISO7816_C_12
Purpose	Negative test: Error on General Authenticate step 2command
Version	0.5
References	[3]
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 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.`

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

Table 9: Test case ISO7816_C_12

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	0.5
References	[3]
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.`

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 AUTHENTICATION (step 2) when using general mapping The test is executed with the MRZ or CAN.
Version	0.5
References	[3] 2.3, 3.2.2
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 AUTHENTICATION (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 AUTHENTICATION step 3 and 4 MAY missing if test object aborts PACE after GENERAL AUTHENTICATION step 2.

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 AUTHENTICATION (step 2) when using integrated mapping. The test is executed with the MRZ or CAN.
Version	0.5
References	[3] 2.3, 3.2.2, 3.3
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 AUTHENTICATION (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 AUTHENTICATION step 3 and 4 MAY missing if test object aborts PACE after GENERAL AUTHENTICATION step 2.

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	0.5
References	[3]
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 AUTHENTICATION (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 :`
	`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 AUTHENTICATION step 3

	and 4 MAY missing if test object aborts PACE after GENERAL AUTHENTICATION step 2.

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	0.5
References	[3]
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: 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 AUTHENTICATION (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 : 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 AUTHENTICATION step 3 and 4 MAY missing if test object aborts PACE after GENERAL AUTHENTICATION step 2.

ISO7816_C_18: Error on General Authenticate step 3 command

Test – ID	ISO7816_C_18
Purpose	Negative test: Error on General Authenticate step 3 command
Version	0.5
References	[3]
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 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.`

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

Table 10: Test case ISO7816_C_18

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	0.5
References	[3]
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.

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 AUTHENTICATION (step 3). The test is executed with the MRZ or CAN.
Version	0.4
References	[3] 2.3, 3.2.2
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 AUTHENTICATION (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_{PICC} 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 AUTHENTICATION step 4 MAY missing if test object aborts PACE after GENERAL AUTHENTICATION step 3.

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	0.5
References	[3]
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 AUTHENTICATION (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: 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 AUTHENTICATION step 4 MAY missing if test object aborts PACE after GENERAL AUTHENTICATION step 3.

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	0.5
References	[3]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.PACE is loaded into the LTwith following modifications. Use EF.CardAccess which contains exact one PACEInfo: protocol: id-PACE-DH-GM-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 AUTHENTICATION (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 : 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 AUTHENTICATION step 4 MAY missing if test object aborts PACE after GENERAL AUTHENTICATION step 3.

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_{PICC} and the ephemeral public key PK_{PCD} transmitted in GENERAL AUTHENTICATION are equal. The test is executed with the MRZ or CAN.
Version	0.4
References	[3] 2.3, 3.2.2
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 AUTHENTICATION (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_{PICC} and PK_{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 AUTHENTICATION step 3.

ISO7816_C_24: Error on General Authenticate step 4 command

Test – ID	ISO7816_C_24
Purpose	Negative test: Error on General Authenticate step 4 command
Version	0.5
References	[3]
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 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.

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

Table 11: Test case ISO7816_C_24

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	0.5
References	[3]
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.

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	0.4
References	[3] 2.3, 3.2.2
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 AUTHENTICATION command (step 4).

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	0.4
References	[3] 3.1.2
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 an information from test object about protocol abort.

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	0.5
References	[3] 3.1.2
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 an information from test object about protocol abort.

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.

ISO7816_D_01: SM failure returned by MRTD

Test - ID	ISO7816_D_01
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	[4]
Profile	SIP
Preconditions	• Configuration profile as defined in table 12 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 SKENC and c = 05 for the derivation of session key SKMAC. • 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.

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

Table 12: Test case ISO7816_D_01

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	[4]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC or CFG.DFLT.PACE is loaded into the LT. • Modification: The LT SHALL NOT 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.

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	[4]
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.

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	[4]
Profile	SIP
Preconditions	• Configuration profile CFG.DFLT.BAC or CFG.DFLT.PACE is loaded into the LT. • Modification: The LT SHALL NOT 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.

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	[4]
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.

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	[4]
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 are wrong due to an incorrect padding of the plaintext.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

Unit ISO7816_E: Test of Active Authentication

ISO7816_E_01: Performing Active Authentication with RSA-SHA1

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 13
	Access conditions: read and select with PACE

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

Table 13: Test case ISO7816_E_01

Test - ID	ISO7816_E_01
Purpose	This test case verifies that the inspection system performs Active Authentication with RSA algorithm in signature function.
Version	0.5
Reference	[4]
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.

ISO7816_E_02: Performing Active Authentication with ECDSA

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.DG15	Signature algorithm: see table 14
	Access conditions: read and select with PACE

Test-ID	***Signature algorithm***	***Key length***
ISO7816_E_02a	ECDSA with SHA1	160 bit

Test-ID	*Signature algorithm*	*Key length*
ISO7816_E_02b	ECDSA with SHA224	224 bit
ISO7816_E_02c	ECDSA with SHA256	256 bit
ISO7816_E_02d	ECDSA with SHA384	384 bit
ISO7816_E_02e	ECDSA with SHA512	512 bit

Table 14: Test case ISO7816_E_02

Test - ID	ISO7816_E_02
Purpose	This test case verifies that the inspection system performs Active Authentication with different ECDSA algorithms in signature function.
Version	0.5
Reference	[4]
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.

ISO7816_E_03: Performing Active Authentication with RSA-SHA224

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
	Access conditions: read and select with PACE

Test - ID	ISO7816_E_03
Purpose	This test case verifies that the inspection system performs Active Authentication with RSA-SHA224 algorithm in signature function.
Version	0.5
Reference	[4]
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.

ISO7816_E_04: Performing Active Authentication with RSA-SHA256

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
	Access conditions: read and select with PACE

Test - ID	ISO7816_E_04
Purpose	This test case verifies that the inspection system performs Active Authentication with RSA-SHA26 algorithm in signature function.
Version	0.5
Reference	[4]
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.

ISO7816_E_05: Performing Active Authentication with RSA-SHA384

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
	Access conditions: read and select with PACE

Test - ID	ISO7816_E_05
Purpose	This test case verifies that the inspection system performs Active Authentication with RSA-SHA384 algorithm in signature function.
Version	0.5
Reference	[4]
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.

ISO7816_E_06: Performing Active Authentication with RSA-SHA512

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 Access conditions: read and select with PACE

Test - ID	ISO7816_E_06
Purpose	This test case verifies that the inspection system performs Active Authentication with RSA-SHA512 algorithm in signature function.
Version	0.5
Reference	[4]
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.

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.
Version	0.5
Reference	[4]
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.

ISO7816_E_08: Performing Active Authentication with invalid signature OID

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 [7]) Access conditions: read and select with PACE

Test - ID	ISO7816_E_08
Purpose	This test case verifies that the inspection system performs Active Authentication with invalid algorithm OID in signature function.
Version	0.5
Reference	[4]
Profile	AA
Preconditions	• Configuration profile CFG.PACE.ISO7816.E08is 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.

ISO7816_E_09: Performing Active Authentication with RSA SHA1 and A6 method

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 A6 method.
	EF.DG15	Signature algorithm: see table 15
		Access conditions: read and select with PACE

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

Table 15: Test case ISO7816_E_09

Test - ID	ISO7816_E_09
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 A.6 Alternative signature production function
Version	0.6
Reference	[4]
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.
Expected results	IS SHALL indicate to the UT that the inspection procedure was successful

ISO7816_E_10: Performing Active Authentication with invalid DG15 Public key

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 16
		Access conditions: read and select with PACE

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

Table 16: Test case ISO7816_E_10

Test - ID	ISO7816_E_10
Purpose	This test case verifies that the inspection system really checks the signature of

	the AA function and give appropriate status
Version	0.6
Reference	[4]
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.

Unit ISO7816_F: Test of Reading Binary Files

ISO7816_F_01: File selection failure

ID		CFG.BAC.ISO7816.F01
Purpose		This configuration defines a BAC protected passport.
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`

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	0.5

Reference	[4]
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.

ISO7816_F_02: Reading large files

ID		CFG.BAC.ISO7816.F02
Purpose		This configuration defines a BAC protected passport.
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`

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	0.5
Reference	[4]
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.

ISO7816_F_03: Reading beyond EOF

ID		CFG.BAC.ISO7816.F03
Purpose		This configuration defines a BAC protected passport.
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 4: JPEG2000 of Erika Mustermann with image truncated after 200 bytes. The file size SHALL be reduced to the same size. Access conditions: read and select with BAC
	Data page MRZ	`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<<<` `C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<4`

Test - ID	ISO7816_F_03
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.
Version	0.5

Reference	[4]
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 a checking error (like 6B00, 6282 or 6Cxx).
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

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	0.5
Reference	[4]
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.

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	0.5
Reference	[4]
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.

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	0.5
Reference	[4]
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.

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	0.5
Reference	[4]
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.

ISO7816_F_08: Reading DG2 with image size 0

ID		CFG.BAC.ISO7816.F08
Purpose		This configuration defines a BAC protected passport. 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, 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 [8] (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

Test - ID	ISO7816_F_08
Purpose	This test verifies that the inspection system is capable of reading datagroups 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	0.5
Reference	[4]
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.

Layer 7 tests (Logical data structures)

Unit LDS_A: Tests with EF.COM

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

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, 63, 6E, 75, 76 Tag 60 is replaced by tag 61 **61**175F0104303130375F36063034303030305C05617563766E Access conditions: read and select with PACE

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	0.5
Reference	[4]
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.

LDS_A_02: DG tag 60 length byte too small

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, 63, 6E, 75, 76 Tag 60 length byte is decreased by 1. 60**16**5F0104303130375F36063034303030305C05617563766E Access conditions: read and select with PACE

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	0.5
Reference	[4]
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.

LDS_A_03: DG tag 60 length byte too big

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, 63, 6E, 75, 76 Tag 60 length byte is increased to 7F. 60**7F**5F0104303130375F36063034303030305C05617563766E

Access conditions: read and select with PACE

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	0.5
Reference	[4]
Profile	SIP
Preconditions	• Configuration profile CFG.PACE.LDS.A03 is loaded into the LT. • IS is „ready“.
Test scenario	Place test data page onto the test object. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

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

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, 63, 6E, 75, 76

LDS version is set to V3.0.
60175F0104**30333030**5F36063034303030305C05617563766E

Access conditions: read and select with PACE

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	0.5
Reference	[4]
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.

LDS_A_05: Missing LDS version

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, 63, 6E, 75, 76 LDS version is deleted. 60**10**5F36063034303030305C05617563766E Access conditions: read and select with PACE

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	0.5
Reference	[4]
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.

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

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, 63, 6E, 75, 76 Unicode version is set to 3.0.0. 60175F0104303130375F3606**303530303030**5C05617563766E Access conditions: read and select with PACE

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	0.5
Reference	[4]
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.

LDS_A_07: Missing Unicode version

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, 63, 6E, 75, 76 Unicode version is deleted. 60**0E**5F0104303130375C05617563766E Access conditions: read and select with PACE

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	0.5
Reference	[4]
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.

LDS_A_08: Incorrect DGPM (missing DG1 tag)

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: 61, 63, 6E, 75, 76 Tag 61 is deleted from the DGPM. 60**16**5F0104303130375F360630343030303030**5C04**7563766E

Access conditions: read and select with PACE

Test - ID	LDS_A_08
Purpose	This test case verifies that the inspection system performs correctly if EF.COM is wrong (incorrect DGPM).
Version	0.5
Reference	[4]
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.

LDS_A_09: Missing DGPM

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, Data groups present: 61, 63, 6E, 75, 76 DGPM is deleted from EF.COM. 60**10**5F0104303130375F3606303430303030 Access conditions: read and select with PACE

Test - ID	LDS_A_09
Purpose	This test case verifies that the inspection system performs correctly if EF.COM is wrong (incorrect DGPM).
Version	0.5
Reference	[4]
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.

Unit LDS_B: Tests with EF.DG1

LDS_B_01: MRZ with optional data

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**

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	0.5
Reference	[4]
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.

LDS_B_02: Name in MRZ indicates abbreviation of the secondary identifier

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

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	0.5
Reference	[4]
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.

LDS_B_03: Name in MRZ without secondary identifier

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

Test - ID	LDS_B_03
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 contains no secondary identifier.
Version	0.5
Reference	[4]
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.

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

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

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	0.5
Reference	[4]
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.

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

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

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	0.5
Reference	[4]
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.

LDS_B_06: DG tag 61 length byte too small

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

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	0.5
Reference	[4]
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.

LDS_B_07: DG tag 61 length byte too big

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

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	0.5
Reference	[4]
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.

LDS_B_08: Incorrect MRZ, document type unknown

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

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	0.5
Reference	[4]
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.

LDS_B_09: Incorrect MRZ, issuing state syntax error

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<D21MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<`
		`C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<4`
		
		Access conditions: read and select with BAC

	Data page MRZ	`P<D21MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<` `C11T002JM4D<<9608122F2310314<<<<<<<<<<<<<<4`

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	0.5
Reference	[4]
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.

LDS_B_10: Incorrect MRZ, name is void

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`

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	0.5
Reference	[4]
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.

LDS_B_11: Incorrect MRZ, name different from data page

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`

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	0.5
Reference	[4]
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.

LDS_B_12: Incorrect MRZ, document number different from data page

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`

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	0.5
Reference	[4]
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.

LDS_B_13: Incorrect MRZ, wrong document number checksum

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**

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	0.5
Reference	[4]
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 of document number is not correct.

LDS_B_14: Incorrect MRZ, nationality syntax error

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 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

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	0.5
Reference	[4]
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.

LDS_B_15: Incorrect MRZ, date of birth syntax error

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`**

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	0.5
Reference	[4]
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.

LDS_B_16: Incorrect MRZ, date of birth error

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<<6713315F2310314<<<<<<<<<<<<<<6
```

Access conditions: read and select with BAC

Data page MRZ

```
P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<
C11T002JM4D<<6713315F2310314<<<<<<<<<<<<<<6
```

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	0.5
Reference	[4]
Profile	DG1
Preconditions	• Configuration profile CFG.BAC.LDS.B16 is loaded into the LT. • IS is „ready“.
Test scenario	Place test data page onto the test object. Start inspection procedure if not automatically started.
Expected results	IS SHALL indicate to the UT that the inspection procedure failed.

LDS_B_17: Incorrect MRZ, incorrect date of birth checksum

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<<9608123F2310314<<<<<<<<<<<<<<7
```

Access conditions: read and select with BAC

Data page MRZ `P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<`
`C11T002JM4D<<9608123F2310314<<<<<<<<<<<<<<7`

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	0.5
Reference	[4]
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.

LDS_B_18: Incorrect MRZ, incorrect sex

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<<9608122D2310314<<<<<<<<<<<<<<4`

Access conditions: read and select with BAC

Data page MRZ `P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<`
`C11T002JM4D<<9608122D2310314<<<<<<<<<<<<<<4`

Test - ID	LDS_B_18
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 is wrong (incorrect sex)
Version	0.5
Reference	[4]

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.

LDS_B_19: Incorrect MRZ, date of expiry syntax error

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`

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	0.5
Reference	[4]
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.

LDS_B_20: Incorrect MRZ, date of expiry error

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<<9608122F6713315<<<<<<<<<<<<<<0`

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	0.5
Reference	[4]
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.

LDS_B_21: Incorrect MRZ, incorrect date of expiry checksum

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<<9608122F2310318<<<<<<<<<<<<<<8`

Access conditions: read and select with BAC

Data page MRZ `P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<`
`C11T002JM4D<<9608122F2310318<<<<<<<<<<<<<<8`

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	0.5
Reference	[4]
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.

LDS_B_22: Incorrect MRZ, incorrect optional data checksum

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`**

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	0.5
Reference	[4]
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.

LDS_B_23: Incorrect MRZ, incorrect checksum

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`

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	0.5
Reference	[4]
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.

LDS_B_24: Missing MRZ data object

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

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	0.5
Reference	[4]
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.

LDS_B_25: Incomplete birth date (missing day)

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<<7F2310314<<<<<<<<<<<<<<4`

Test - ID	LDS_B_25
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 stores a incomplete birth date (missing day)
Version	0.5
Reference	[4]
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.

LDS_B_26: Incomplete birth date (missing month)

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<<126F2310314<<<<<<<<<<<<<<2`
		
		Access conditions: read and select with BAC

	Data page MRZ	`P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<` `C11T002JM4D<<96<<126F2310314<<<<<<<<<<<<<<2`

Test - ID	LDS_B_26
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 stores a incomplete birth date (missing month)
Version	0.5
Reference	[4]
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.

LDS_B_27: Incomplete birth date (missing year)

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<<**<<**08121F2310314<<<<<<<<<<<<<<**8**

Access conditions: read and select with BAC

Data page MRZ	P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<< C11T002JM4D<<**<<**08121F2310314<<<<<<<<<<<<<<**8**

Test - ID	LDS_B_27
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 stores a incomplete birth date (missing year)
Version	0.5
Reference	[4]
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.

LDS_B_28: Incomplete birth date (missing complete dob)

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**

Test - ID	LDS_B_28
Purpose	This test case verifies that the inspection system performs correctly if EF.DG1 stores a incomplete birth date (missing complete dob)
Version	0.5

Reference	[4]
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.

Unit LDS_C: Tests with EF.DG2

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	0.5
Reference	[4]
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.

LDS_C_02: JPEG image, full frontal

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

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	0.5
Reference	[4]
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.

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

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

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	0.5
Reference	[4]
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.

LDS_C_04: DG tag 75 wrong (tag 76 instead)

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: **76**823AE77F61823AE20201017F60823ADAA10... JPEG2000 of Erika Mustermann Access conditions: read and select with PACE

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	0.5

Reference	[4]
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.

LDS_C_05: DG tag 75 length byte too small

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

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	0.5
Reference	[4]
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.

LDS_C_06: DG tag 75 length byte too big

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

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	0.5
Reference	[4]
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.

LDS_C_07: BIGT, missing tag for number of instances

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

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	0.5
Reference	[4]
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.

LDS_C_08: BHT, not allowed format owner

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

Test - ID	LDS_C_09
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (BHT, not allowed format owner)
Version	0.5
Reference	[4]
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.

LDS_C_09: BHT, missing format owner

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

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	0.5
Reference	[4]
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.

LDS_C_10: BHT, not allowed format type

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

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	0.5
Reference	[4]
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.

LDS_C_11: BHT, missing format type

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

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	0.5
Reference	[4]
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.

LDS_C_12: BHT, deprecated biometric type

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

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	0.5
Reference	[4]
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.

LDS_C_13: BHT, incorrect biometric type

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

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	0.5
Reference	[4]
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.

LDS_C_14: FRH, incorrect format identifier

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 BAC

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	0.5
Reference	[4], [8]
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.

LDS_C_15: FRH, incorrect version number

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

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	0.5
Reference	[4], [8]
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.

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

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

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	0.5
Reference	[4], [8]
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.

LDS_C_17: FIB, incorrect gender

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 gender in FIB. Set value to 03.** JPEG2000 of Erika Mustermann Access conditions: read and select with PACE

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	0.5
Reference	[4], [8]
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.

LDS_C_18: FIB, incorrect eye colour

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

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	0.5
Reference	[4], [8]
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.

LDS_C_19: FIB, incorrect hair colour

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

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	0.5
Reference	[4], [8]
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.

LDS_C_20: FIB, incorrect Pose Angle - Yaw

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

Test - ID	LDS_C_20
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect pose angel - yaw)
Version	0.5
Reference	[4], [8]
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.

LDS_C_21: FIB, incorrect Pose Angle - Pitch

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

Test - ID	LDS_C_21
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect pose angel - pitch)
Version	0.5
Reference	[4], [8]
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.

LDS_C_22: FIB, incorrect Pose Angle - Roll

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

Test - ID	LDS_C_22
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect pose angel - roll)
Version	0.5
Reference	[4], [8]
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.

LDS_C_23: FIB, incorrect Pose Angle Uncertainty - Yaw

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

Test - ID	LDS_C_23
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect pose angel uncertainty - yaw)
Version	0.5
Reference	[4], [8]
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.

LDS_C_24: FIB, incorrect Pose Angle Uncertainty - Pitch

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

Test - ID	LDS_C_24
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect pose angel uncertainty - pitch)
Version	0.5
Reference	[4], [8]
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.

LDS_C_25: FIB, incorrect Pose Angle Uncertainty - Roll

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

Test - ID	LDS_C_25
Purpose	This test case verifies that the inspection system performs correctly if EF.DG2 is wrong (FIB, incorrect pose angel uncertainty - roll)
Version	0.5
Reference	[4], [8]
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.

LDS_C_26: IIB, incorrect face image type

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

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	0.5
Reference	[4], [8]
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.

LDS_C_27: IIB, incorrect image data type

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

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	0.5
Reference	[4], [8]

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.

LDS_C_28: Missing facial image (tag 5F2E)

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

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	0.5
Reference	[4]
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.

Unit LDS_D: Tests with EF.SOD

LDS_D_01: Test signatur support

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
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	256 bit	224 bit stored inside SOD
LDS_D_01l	SHA-224	SHA-224	ECDSA with SHA224	256 bit	224 bit stored inside SOD
LDS_D_01m	SHA-256	SHA-256	ECDSA with SHA256	256 bit	256 bit stored inside SOD
LDS_D_01n	SHA-384	SHA-384	ECDSA with SHA384	384 bit	384 bit stored inside SOD
LDS_D_01o	SHA-512	SHA-512	ECDSA with SHA512	512 bit	512 bit stored inside SOD
LDS_D_01p	SHA-224	SHA-224	ECDSA with	256 bit	224 bit

Test - ID	*LDS security object digest algorithm*	*Digest algorithm*	*Signature algorithm*	*Country Signer*	*Document Signer*
			SHA224		**NOT** stored inside SOD

Table 17: Test cases LDS_D_01

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 17 Digest algorithm: see table 17 Signature algorithm: see table 17 Signature generation: see table 17 CSCA and DS certificates are based on algorithm as described in table 17 in the complete chain Access conditions: read and select with PACE

Test - ID	LDS_D_01
Purpose	This test case verifies that the inspection system performs correctly if EF.SOD contains RSA signature algorithm
Version	0.5
Reference	[4]
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.

LDS_D_02: DG tag 77 wrong (tag 78 instead)

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

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	0.5
Reference	[4]
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.

LDS_H_03: DG tag 77 length byte too small

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

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	0.5
Reference	[4]
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.

LDS_D_04: DG tag 77 length byte too big

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

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	0.5
Reference	[4]
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.

LDS_D_05: SignedData version incorrect

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

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	0.5
Reference	[4]
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.

LDS_D_06: SignedData version missing

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

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	0.5
Reference	[4]
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.

LDS_D_07: SignedData illegal digestAlgorithm (MD5)

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

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	0.5
Reference	[4]
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.

LDS_D_08: SignedData missing digestAlgorithm list

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

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	0.5
Reference	[4]
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.

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

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

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	0.5
Reference	[4]
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.

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

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

Test - ID	LDS_D_25
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	0.5
Reference	[4]
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.

LDS_D_11: SignerInfo, incorrect signer info version value

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

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	0.5
Reference	[4]
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.

LDS_D_12: SignerInfo, missing signer info version

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

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	0.5
Reference	[4]
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.

LDS_D_13: SignerInfo, Version 1 and incorrect issuerAndSerialNumber

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

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	0.5
Reference	[4]
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.

LDS_D_14: SignerInfo, Version 3 and incorrect subjectKeyIdentifier

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

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	0.5
Reference	[4]
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.

LDS_D_15: SignerInfo, illegal digestAlgorithm

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

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	0.5

Reference	[4]
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.

LDS_D_16: SignerInfo, missing digestAlgorithm

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

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	0.5
Reference	[4]
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.

LDS_D_17: SignerInfo, incorrect messageDigest attribute value

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.** 301506092A864886F70D0109**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

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	0.5
Reference	[4]
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.

LDS_D_18: SignerInfo, missing messageDigest attribute

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

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	0.5
Reference	[4]
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.

LDS_D_19: SignerInfo, incorrect Signature

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

Test - ID	*LDS security object digest algorithm*	*Digest algorithm*	*Signature algorithm*	*Country Signer*	*Document Signer*
					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	256 bit	224 bit stored inside SOD
LDS_D_19l	SHA-224	SHA-224	ECDSA with SHA-224	256 bit	224 bit stored inside SOD
LDS_D_19m	SHA-256	SHA-256	ECDSA with SHA-256	256 bit	256 bit stored inside SOD
LDS_D_19n	SHA-384	SHA-384	ECDSA with SHA-384	384 bit	384 bit stored inside SOD
LDS_D_19o	SHA-512	SHA-512	ECDSA with SHA-512	512 bit	512 bit stored inside SOD
LDS_D_19p	SHA-224	SHA-224	ECDSA with SHA-224	256 bit	224 bit **NOT** stored inside SOD

Table 18: Test case LDS_D_19

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 18 Digest algorithm: see table 18 Signature algorithm: see table 18 CSCA and DS certificates are based on algorithm as described in table 18 in the complete chain. Access conditions: read and select with PACE

Test - ID	LDS_D_19
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	0.5
Reference	[4]
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.

LDS_D_20: SignerInfo, missing Signature

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

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	0.5
Reference	[4]
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.

LDS_D_21: LDS Security Object, incorrect security object version

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

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	0.5
Reference	[4]
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.

LDS_D_22: LDS Security Object, missing security object version

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

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	0.5
Reference	[4]
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.

LDS_D_23: LDS Security Object, illegal digestAlgorithm

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

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	0.5
Reference	[4]

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.

LDS_D_24: LDS Security Object, missing digestAlgorithm

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

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	0.5
Reference	[4]
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.

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

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

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	0.5
Reference	[4]
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.

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

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 BAC

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	0.5
Reference	[4]
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.

LDS_D_27: DS certificate, incorrect certificate version

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

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	0.5
Reference	[4]
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.

LDS_D_28: DS certificate, missing certificate version

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

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	0.5
Reference	[4]
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.

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

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 [6].** 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

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	0.5
Reference	[4]
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.

LDS_D_30: DS certificate, incorrect signatureValue

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

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	0.5
Reference	[4]
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.

LDS_D_31: DS certificate, missing signatureValue

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

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	0.5
Reference	[4]
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.

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	0.5
Reference	[4]
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 appendix 2 of [4] Volume 2). • 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.

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

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

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	0.5
Reference	[4]
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.

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

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

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	0.5
Reference	[4]
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.

Unit LDS_E: Tests with EF.DG15

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

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 BAC

Test - ID	LDS_E_01
Purpose	This test case verifies that the inspection system performs Active Authentication with wrong tag in data group.
Version	0.5
Reference	[4]
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.

LDS_E_02: DG tag length too small

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 BAC

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	0.5
Reference	[4]
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.

LDS_E_03: DG tag length too big

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 BAC

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	0.5
Reference	[4]
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.

Unit LDS_F: Tests with EF.DG14

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

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**82014A3182014630820122060904007F000702... Key agreement algorithm: CA-ECDH-3DES-CBC-CBC Key reference: none Access conditions: read and select with BAC / PACE

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	0.5
Reference	[3], [4]
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.

LDS_F_02: DG tag 6E length byte too small

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**820149**3182014630820122060904007F000702... Key agreement algorithm: CA-ECDH-3DES-CBC-CBC Key reference: none Access conditions: read and select with BAC / PACE

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	0.5
Reference	[3], [4]
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.

LDS_F_03: DG tag 6E length byte too big

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**82014B**3182014630820122060904007F000702... Key agreement algorithm: CA-ECDH-3DES-CBC-CBC Key reference: none Access conditions: read and select with BAC / PACE

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	0.5
Reference	[3], [4]
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.

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

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

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	0.5
Reference	[3] 2.2, 3.1.5, [4]
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.

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

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

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	0.5
Reference	[3] 2.2, 3.1.5, [4]
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.

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

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: 9 Access conditions: read and select with BAC / PACE

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	0.5
Reference	[3] 2.2, 3.1.5, [4]
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.

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

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

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	0.5
Reference	[3] 2.2, 3.1.5, [4]
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.

References

[1] AFNOR, Automatic Interface Specification
[2] Bundesamt für Sicherheit in der Informationstechnik (BSI), TR-03105 Part 5.1, Test plan for ICAO compliant Inspection Systems with EAC
[3] ICAO, Technical Report - Supplemental Access Control for Machine Readable Travel Documents
[4] International Civil Aviation Organization, Doc 9303, Machine Readable Travel Documents
[5] ISO/IEC, ISO/IEC 10373-6 Identification cards - Test methods - Part 6: Proximity cards
[6] ISO/IEC, ISO/IEC 9796 Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms
[7] ISO/IEC, ISO/IEC 3166 Codes for the representation of names of countries and their subdivisions
[8] ISO/IEC, ISO/IEC 19794-5 Information technology — Biometric data interchange formats — Part 5: Facialimage data
[9] ISO/IEC, ISO/IEC 7816-4 Identification cards — Integrated circuitcards — Part 4: Organization, security and commands for interchange
[10] ISO/IEC, ISO/IEC 7816 Identification cards — Integrated circuitcards
[11] Network Working Group, Key words for use in RFCs to indicate requirement levels, BCP 14, RFC 2119