European Commission

JRC TECHNICAL REPORTS

EU eMRTD Interoperability Test 2017

Final Report

Rana, A.
Arcediano-Garrido, E.

2018

Joint Research Centre

EUR 29216 EN

EU 2017 EMRTD INTEROPERABILITY TEST FINAL REPORT

Contact information
Name: Antonia Rana
Email: antonia.rana@ec.europa.eu

JRC Science Hub
https://ec.europa.eu/jrc

JRC111515

EUR 29216 EN

PDF ISBN 978-92-79-85687-7 ISSN 1831-9424 doi:10.2760/828262

Luxembourg: Publications Office of the European Union, 2018

How to cite this report: Rana, A., Arcediano-Garrido, E., *EU 2017 eMRTD Interoperability Test Final Report*, EUR 29216 EN, Publications Office of the European Union, Luxembourg, 2018, ISBN 978-92-79-85687-7, doi:10.2760/828262, JRC111515

Contents

Foreword

Interoperability test events for electronic travel documents have been held for a long time since ICAO started its work on the technical specifications for eMRTDs in Document 9303. This document incorporated the specifications for the employment of biometrics and contactless chip technology in travel documents, which thus became electronic machine readable travel documents, eMRTDs. The specifications included the details for the data structure storing the biometric and biographical data in the chip (Logical Data Structure, LDS) as well as the details for the use of the security measures based on symmetric and public key cryptography which could or had to be used to protect the authenticity, integrity and confidentiality of data both when stored in the chip and while transferred from the chip to the reading device in the process of reading the data contained in the chip at the border.

Interoperability test events were necessary to bring together producers of chips and chip personalisation software and producers of reading devices and inspection system software to ensure that their implementations were fully interoperable. This, in turn, would ensure a smooth border checking and better travel experience for travellers.

While most recent interoperability test events have shown a consistently improving success rate, indicating that both specifications and implementation have reached a good level of maturity, the need to hold such events still exists for two main reasons: on the one hand, specifications evolve as technology and the associated risks and countermeasures evolve, on the other hand new actors emerge on the market which can benefit from the learning process associated to an interoperability test event.

The organisation of the interoperability test event in Ispra aimed at addressing the need expressed at times by document and inspection systems producers, to assess the current status regarding implementation of the latest versions of the specifications, particularly PACE and PACE-CAM after the last official interoperability test event held in Madrid in 2014.

Acknowledgements

The authors wish to thank the team of experts from the technical subgroup of the Article 6 Committee, who helped in the execution and the preliminary technical evaluation of the results of the tests. They are also grateful to colleagues in DG HOME, most notably Ms Sylvia Kolligs-Tuffery, whose support was fundamental in the organisation of the event, and colleagues in the JRC, most notably Mr Andrea Ciardulli for his support in the preparation of the technical environment used for registration and results processing.

1 Introduction

Interoperability test events for electronic travel documents have been held since the specifications for the use of biometrics and contactless chip technology in travel documents were defined.

The use of chip technology also required the need to specify a data structure to store the data and security measures to protect their integrity, authenticity and privacy.

In order for electronic machine readable travel documents (eMRTDs) to be inspected correctly at the borders, it is necessary that both eMRTDs and inspection systems (which include the physical reading device as well as the border inspection software used to display the data to the inspecting entity) implement the technical specifications correctly. Technical specifications for the implementation of the eMRTDs and its inspecting devices are provided in [1] [2] [3] [4] [5] [6] [7] [8]. The correct implementation of the specifications can be assessed with conformity testing, i.e. by executing a set of tests aimed at assessing how an implementation of the specification responds to both correct and incorrect commands received from a software simulating the document verification system. Such tests are defined in a test specification. ICAO defines the following test specifications, which address different aspects of the eMRTD implementation:

- ICAO, TR – Durability of Machine Readable Passports, v3.2, August 2006 [32]
- ICAO, TR – RF Protocol and Application Test Standard for ePassport Part 2 – Tests for Air Interface, Initialisation, Anticollision and Transport Protocol, v1.02, February 2007 [33]
- ICAO, TR – RF Protocol and Application Test Standard for eMRTD Part 3 – Tests for Application Protocol and Logical Data Structure, v2.10, June 2016 [28]

For eMRTDs implementing extended access control (EAC), test specifications are defined in:

- BSI, TR-03105 Part 3.2: Test plan for eMRTDs with EACv1, v1.4.1, April 2014 [29]

Therefore testing for conformity is a big step towards ensuring interoperability. However, it is not sufficient, as experience has shown also in different application fields.

Interoperability test events are useful to bring together producers of chips and chip personalisation software and producers of reading devices and inspection system software to ensure that their implementations were fully interoperable and thus ensure a smooth border checking and travel experience for travellers.

Interoperability test events help to assess the capability of communicating devices to correctly implement the specifications and to fulfil the required functional operations. In the context of electronic machine readable travel documents (eMRTDs) interoperability events constitute the possibility for eMRTD producers to have their documents tested for conformity from conformity test labs and for document verification system producers to test their implementation of the specifications against a range of different chip implementations.

An interoperability test event consists generally of two parts:

- Conformity test and
- Crossover test

In the conformity test, test laboratories implementing the test specifications [28] ([29] for EAC-related tests) run a pre-defined subset of the tests against the eMRTD to assess the correctness of the implementation of the technical specifications.

Since the execution of the full set of tests requires a considerable amount of time, usually interoperability test events focus on a particular aspect corresponding to a section in the specifications, thus selecting a subset of the tests which address that particular aspect.

In the crossover test, document verification systems (i.e. inspection systems) read eMRTDs verifying that all steps of an inspection or advanced inspection procedure can be run correctly and the information contained in the chip can be displayed and inspected correctly.

In the Interoperability test organised by the European Commission in the Joint Research Centre of Ispra, the following scenarios were investigated:

- Evaluation of conformity of submitted eMRTD to the ICAO specifications [6][7][8] following the test specification "ICAO Technical Report RF Protocol and Application Test Standard for e-Passport", Part 3 (version 2.10) [28] and
- Verification of the readability of submitted eMRTDs on different verifications systems (inspection systems) and assessment of the eMRTD behaviour in a regular inspection process.

The organisation of the interoperability test event in Ispra aimed at addressing the perceived need to assess the current status regarding implementation of the latest specifications after the last official interoperability event held in Madrid in 2014.

This document provides a report on the process followed in the preparation of the test event, on the characteristics of the eMRTDs submitted for the test and on the outcomes resulting in the two scenarios mentioned above.

It is organised in three main sections and two annexes.

In the first section we provide a description of the preparation of the event, including test scope definition, test environment setting and test results reporting mechanisms.

In the second section we provide the results of the tests including statistics about participants and documents and inspection systems taking part in the test. Test results are detailed for conformity tests and crossover tests.

In the two annexes we provide the smoke test results and the full test report form which was used to report the results of the crossover tests.

2 Test event preparation

The preparatory phase of the test event consisted in the set-up of the experts' team, in the definition of the scope of the test, in the invitation to participants and in the overall definition of the test plan.

The expert's team set-up for the event consisted of experts from the technical subgroup of the Article 6 committee and experts from the electronic documents laboratory in the JRC. It provided support during the preparatory phase, during the execution of the tests and in the preliminary evaluation of the test results, which were presented to test participants at the end of the interoperability test event.

2.1 Test scope definition

The scope of the test was defined in the call for participation which was shared with the ICAO New Technology Working Group (NTWG) and published on the JRC Science Hub website.

The main purpose of the test was aimed at addressing the latest specifications regarding access control, i.e. the Password Authenticated Connection Establishment (PACE) and its integration with Chip Authentication (PACE-CAM mapping).

The text of the call for participation is recalled in the box below.

The European Commission will organize conformity and interoperability tests for eMRTDs together with a conference on 25th and 26th September 2017. It will be held in the European Commission Joint Research Centre (JRC) premises in Ispra, Italy. The tests will focus on the latest access control specifications (e.g. the operation of the PACE protocol with Chip Authentication). This security mechanism, known as "Password Authenticated Connection Establishment with Chip Authentication Mapping" (PACE-CAM) is specified in Technical Report BSI TR-03110 "Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token" and it combines PACE and Chip Authentication (CA) into one protocol leading to faster ID document verification.

The conference will take place on the second day (26/09/2017) and will include speakers from the EU Commission, ICAO (requested) and Member States (requested). At its end, the high-level aggregate results of the tests will be presented.

The main beneficiaries of these tests are EU Member States. Depending on the number of EU Member States that will participate in the event, and provided that it is possible from an organisational perspective, a limited number of non-EU ICAO Member States and private sector travel document manufacturers will be allowed to participate in the test (on a first come first serve basis).

The test will focus on the implementation of PACE as specified in the Technical Report "Radio Frequency Protocol and Application Test Standard for eMRTD Part 3 Tests for Application Protocol and Logical Data Structure, Version: 2.10, July 2016.

The European Commission, with the assistance of EU Member States experts, will lead and supervise the technical aspects of the tests. The independent services of various private sector document verification system providers and conformity test laboratories will be secured. Individual test results will be kept confidential.

The following scenarios will be investigated:

— Evaluation of document conformity according to the test specification "ICAO Technical Report Radio Frequency Protocol and Application Test Standard for eMRTD Part 3 Tests for Application Protocol and Logical Data Structure, Version: 2.10, July 2016.; and

— Assessment of the readability of eMRTDs on different verifications systems and/or versions and evaluation of document behaviour in a regular document verification process.

The following types of documents will be accepted:

— Government eMRTD samples (already issued or to be issued in the near future),

— EU residence permits.

The event is open to:

— Governments

— Document verification system providers and

— Conformity testing laboratories and providers

Pre-Registration:

The deadline for registrations is Friday 7 July 2017.

The number of participants is limited. To pre-register your participation, please send the following information to eu-interoperability-test-2017@ec.europa.eu

— Your name

— Your organisation name

— Number of participants to the conference

— Number of participants to the interoperability testing

— Device under test (i.e. eMRTD, eRP)

— Number of samples per device

Pre-registered participants will receive further information in order to complete registration in July.

The conference programme will be published closer to the event.

2.2 Test environment set-up

Data gathered at pre-registration was used to estimate the number of participants and therefore prepare adequate space for testing, although around 20% of the final number of participants were admitted after pre-registration was closed.

Pre-registered participants were then asked to register the documents and or the document verification systems they intended to submit for the test.

Documents registration consisted in filling in forms providing the following information:

- ICAO 9303 Implementation Conformance Statement (ICS), which is defined in [28] and includes information about:
    - *Access control applied (plain, BAC, EAC, PACE, Password Type: MRZ, CAN)*
    - *LDS version*
    - *READ BINARY with Odd instruction byte supported*
    - *eMRTD contains elementary file with LDS Data Group 3*
    - *eMRTD contains elementary file with LDS Data Group 4*
    - *eMRTD contains elementary file with LDS Data Group 5*
    - *eMRTD contains elementary file with LDS Data Group 6*
    - *eMRTD contains elementary file with LDS Data Group 7*

  - *eMRTD contains elementary file with LDS Data Group 8*
  - *eMRTD contains elementary file with LDS Data Group 9*
  - *eMRTD contains elementary file with LDS Data Group 10*
  - *eMRTD contains elementary file with LDS Data Group 11*
  - *eMRTD contains elementary file with LDS Data Group 12*
  - *eMRTD contains elementary file with LDS Data Group 13*
  - *eMRTD contains elementary file with LDS Data Group 16*
  - *Authentication supported (passive authentication, active authentication)*
  - *MRZ provided with the samples*
  - *Country signing certificate used to verify EF.SOD and EF.CardSecurity (if applicable)*
  - *Expected value for document type (2 characters)*
  - *Invalid key reference for PACE (as used in test case ISO7816_P_09)*
  - *Invalid password identifier for PACE (as used in test case ISO7816_P_08)*
  - *Valid PACE OID not supported by the eMRTD (used in test case ISO7816_P_68. If such an OID can't be provided, ISO7816_P_68 is not applicable)*
  - *Command to send to the eMRTD to verify the chip's ability to still require Secured APDU after performing valid or incomplete PACE protocol.*
  - *Configuration list described in the EF.CardAccess*
    - *Algorithm*
    - *Domain parameters*
- EAC Implementation Conformance Statement, as defined in [29] and containing information about:
  - *Chip authentication support*
  - *Chip Authentication with MSE:Set AT & General Authenticate for 3DES algorithm support*
  - *Diffie-Hellman support*
  - *Elliptic Curve Diffie-Hellman support*
  - *Explicit key selection support*
  - *Terminal Authentication support*
  - *Supported cryptographic algorithm*
    - *Signature algorithm OID*
    - *Key Size (in bits)*
    - *Curve Name (for ECDSA)*
- ISO/IEC 18745-2 [34] Applicant declaration (compilation of this form was optional), containing information about:
  - *Physical size of product*
  - *Location of antenna within eMRTD*
  - *Claimed PICC class*
  - *Shielding of the eMRTD*

  - *eMRTD resonance minimum frequency (MHz)*
  - *eMRTD resonance maximum frequency (MHz)*
  - *Protocol Type (A or B)*
  - *UID (Type A) Random*
  - *PUPI (Type B) Random*
  - *eMRTD reader to eMRTD supported bit rates*
  - *eMRTD to eMRTD reader supported bit rates*
  - *Support of exchange of additional parameters*
  - *Maximum Frame size supported (bytes)*
  - *Frames with error correction supported*
  - *NAD support*
  - *CID support*
  - *Extended length APDU supported*

In addition to the above information, document providers were asked to provide:

- *CSCA certificates*
- *MRZ (and CAN if available)*
- *CVCA, DV, IS certificates and IS private key*

Documents verification systems registration consisted in filling in information sheets providing the following information:

- *Software name*
- *Software version*
- *e-Passport test software*
- *OCR reader type*
- *Information read and displayed (Data groups)*
- *Security mechanisms implemented and details related to*
  - *Signature algorithms*
  - *Hash algorithms*
  - *Mapping*
  - *Key agreement*
- *eMRTD reader to eMRTD supported bit rates*
- *eMRTD to eMRTD reader supported bit rates*
- *PICC classes support*

2.3 Invitation of stakeholders

In addition to the document providers and document verification system providers, who were invited through the ICAO NTWG and the technical subgroup of the Article 6 committee, three test laboratories were invited by the expert's team based on their participation to previous interoperability test events.

2.4 Technical preparation

As already indicated in the previous sections, an interoperability test event consists of two components: conformity testing and crossover testing. Conformity testing verifies that implementations are conforming to the specifications. In context of eMRTDs, conformity testing consists in running a set of tests defined in the test specifications using software which emulates a reader. Such tests include sending incorrect or malformed commands or APDUs (Application Protocol Data Units) to the document and verifying that the document reacts as expected and as defined in the relevant specifications. Crossover testing, on the other hand, verifies that document verification systems (inspection systems) can read (i.e. run the inspection procedure) on all documents submitted to the test.

The execution of both types of tests provides a good level of assurance that the documents are compliant to the specifications and that document verification systems and documents are interoperable.

It should be noted, however, that when a limited subset of the test specifications is used in a test event, the only conclusion that can be drawn is that documents are conformant to the subset of the technical specifications corresponding to the test subset which has been executed.

2.4.1 Conformity testing

For this interoperability test event, the focus was on PACE and PACE-CAM implementations and the following subset of the test specifications was selected:

- **ISO7816_O**: Security conditions for PACE protected eMRTDs – **58 test cases**
- **ISO7816_P**: Password Authenticated Connection Establishment (PACEv2) – **76 test cases**
- **ISO7816_Q**: Command READ and SELECT for le EF.CardAccess – **4 test cases**
- **ISO7816_S**: Command READ and SELECT for EF.CardSecurity – **4 test cases**
- **LDS_E**: Matching between EF.DG14 and EF.CardAccess – **4 test cases**
- **LDS_I**: Structure of EF.CardAccess – **4 test cases**
- **LDS_K**: Structure of EF.CardSecurity – **4 test cases**
- **LDS_D_06**: Test case to perform Passive Authentication – **1 test case**

Altogether, the number of tests included in these test units is 155, which means that each test laboratory had to run 155 tests against each of the documents submitted to the test event.

Test laboratories were asked to report the results of the execution of the test cases in a CSV file for each document tested.

The structure of the content of the CSV file was the following:

- Laboratory ID

- Document ID
- Test case ID (as in the standard test specification)
- Test result (P(ass)/F(ail)/N(ot applicable))

Test laboratories were asked to name the files according to the following convention:

<LAB_id><Doc_id>.csv

A document containing the description of the tests and the procedure to be followed at on-site document registration and hand-over was sent to all document providers before the event.

A similar document, describing the test procedure was sent to document verification systems providers and to test laboratories.

2.4.2 Crossover test

The purpose of the crossover test in an interoperability test event is to verify that every document can be read/inspected with every document verification system participating to the test event.

A document verification system should read an eMRTD following the standard or advanced inspection procedure depending on the security mechanisms implemented in the eMRTD.

In the case of crossover testing, there is no standard mechanism to report the results as it cannot be expected that document verification systems produce a log of the operations executed in a standardised format.

For this reason, in order to collect the results of the crossover test in way which would make results from different participants comparable, a template was prepared which document verification systems providers were asked to fill-in during or after the reading process of each document.

The template was structured in nine sections as follows:

- **Handling of cryptographic material**: with questions about the import of CSCA, CRL, CVCA, DV, IS certificates and IS private key
- **Authentication of data**: with questions about the execution of Passive Authentication
- **Access to the contactless IC**: with questions on BAC and PACE
- **Authentication to the contactless IC**: with questions on Active Authentication, Chip Authentication and PACE-CAM
- **Authentication of the terminal**: with questions on Terminal Authentication
- **Optical check**: with questions on the comparison between data on the data page and data contained in the LDS
- **Biometric pictures**: with questions about the display of the biometric images
- **Data groups**: with questions on the presence and readability of the different data groups
- **Elementary files**: with questions on presence and decoding of EF.ATRinfo and EF.COM

For each question a radio button provided the possibility to give a simple **Yes/No/Not executed (or Not Available)** answer to each question, a second field provided the possibility to explain the reason in case of negative answer. A drop-down menu suggesting possible values for fail reasons was provided but testers could also introduce their own free text.

The pre-encoded reasons were provided in order to ensure uniformity of reports when the same reason for failure occurred in different tests, thus allowing us to extract more meaningful statistics and useful information about the most common or frequent reasons for failures.

As an example, possible reasons which could be used to report issues in reading a document were:

- BAC executed (a possible reason for PACE not executed)
- EF.CardAccess.notFound
- InspectionSystem.extendedLength.notSupported
- InspectionSystem.password.notAvailable
- PACE-CAM.notSupported
- Protocol.notSupported
- ASN.1 error coding
- Errors in select EF.CardAccess or EF.CardSecurity

3 TEST EXECUTION

The test room was prepared having one table with two chairs for each document verification system provider and for each test lab.

Slightly more than one full day was available for official tests and about half a day was available for free-style testing, i.e. tests agreed on a bilateral basis between document producers and document verification systems producers, the results of which were not collected and are therefore not available in this report.

Testing started at 12:00 on Monday 25th September and continued until Thursday 26th September around 14:00 with all test stations having completed all the tests on all the documents. Preliminary results were evaluated and presented at the conference organised back-to-back with the test event on Wednesday 27th.

3.1 Registration Process

Before the event, each participant was sent a registration confirmation letter containing a participant id number (PID) which they were invited to present at on-site registration.

At registration, each document producer presented their PID and the five samples for the documents which they had registered by compiling the forms received by email. Each document was labelled with the document id and a stamped receipt, with the list of all the document ids corresponding to the documents submitted for the test was given back to document producers. Document producers were invited to present the receipt at the document recollection point at end of the event in order to collect back their samples. The five samples were then put into an envelope which was passed on to the expert's team for the smoke testing.

Each document verification system producer presented their PID and was given information about their test station id and was guided to the test room where their test station had been labelled.

After registration of all the documents (including some late registrations), the USB sticks which had been prepared in advance containing all the certificates, IS private keys and MRZ/CAN were distributed to test stations.

Implementation Conformity Statements were distributed to the conformity test laboratories.

3.2 Participants

Thirty-six different organisations participated to the test, from EU and non EU countries. Some participants from industry were participating both as document producers and as document verification system providers.

More in detail, the following figures summarise the participation to the event:

- 23 Document Providers
- 28 Samples' Sets from Countries (each set consisting of 5 documents with exactly the same configuration)
- 14 Samples' Sets from Industry (each set, but one, consisting of 5 documents with exactly the same configuration, one set consisting of three samples with the same configuration)
- 42 different document samples submitted in total
- 12 Document verification system (inspection system) providers
- 16 Inspection Systems stations (some providers participated to the test with two different inspection systems)
- 3 Mobile systems

- 3 Test Laboratories for Conformity Testing

3.3 Pre-processing

In some cases, pre-processing the information and data received with the email registration of the documents was necessary in order to prepare them for the smoke test environment and in order to ensure that all data was in the same formats for the test stations.

3.3.1 Cryptographic material

Several participants sent the certificates in PEM format. The PEM text format was converted to the DER binary format using openssl.

In one case, we received only the test CVCA certificate and the corresponding private key with no DV and IS certificate. For this case, an in-house tool was used to generate the certificate chain and the Inspection System (IS) private key.

Some participants sent the certificates or the private keys with the wrong file extension (e.g. a CVC extension for a X.509 certificate). In that case, the extension was changed to the correct one.

One participant sent a certificate in a PEM format which was only accepted by Microsoft tools, in this case, the certificate was edited manually.

One participant sent an expired CSCA certificate; in this case, a new CSCA certificate with a correct validity field was requested.

3.4 Documents and document verification systems data

The following sections provide some figures about generic characteristics of the documents and document verification systems participating to the tests.

3.4.1 Documents

The figures presented in this section summarise the information contained in the declarations provided by the applicants (document providers). In some cases, as can be seen by comparing these data with the results of the smoke tests presented in Annex B, they do not reflect the actual characteristics of the documents, suggesting that enough time should be planned before tests start in order to cross-check the information received in the ICS and the documents submitted to the tests.

3.4.1.1 LDS version

48% of the document providers did not indicate which version of LDS was implemented.

45% declared that version 1.7 was used.

7% declared that version 1.8 was used.

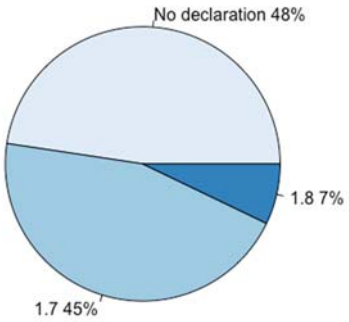

Figure 1: LDS version

3.4.1.2 PACE Mapping

PACE may use Integrated Mapping (IM), Generic Mapping (GM) or Chip-Authentication Mapping (CAM) to map the nonce.

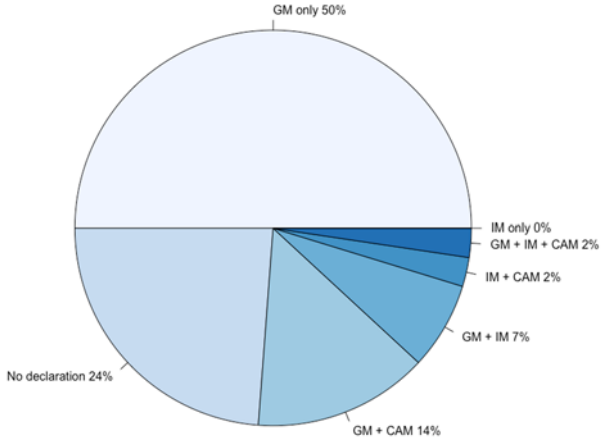

Figure 2: PACE mappings support declarations

The second section of the document registration form asked for the list of PACE algorithms supported by the chip. Figure 3 shows that more than half of the samples declared support for one PACE algorithm only, while one document supported 10 different PACE algorithms. Some ICS did not provide any information related to supported PACE algorithms.

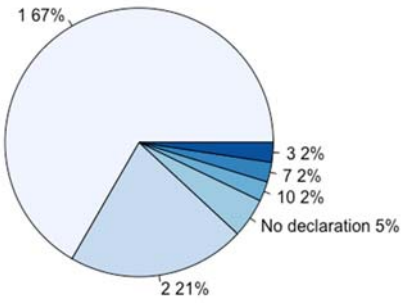

Figure 3: Number of PACE algorithms supported

Regarding the key agreement algorithm used in PACE, Figure 4 shows that most of the document declared to use elliptic curve key agreement.

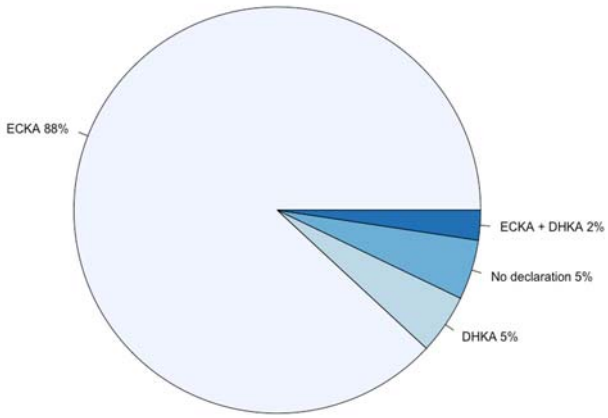

Figure 4: Key exchange algorithms for PACE

Almost all the samples declared their support for extended key length, while only slightly more than 20% declared no support for extended key length or provided no declaration in relation to support for extended key length.

Figure 5: Support for extended key length

A large percentage of the samples did not provide any information on the chip type, while for those which did provide the chip type information the most recurrent value was type A.

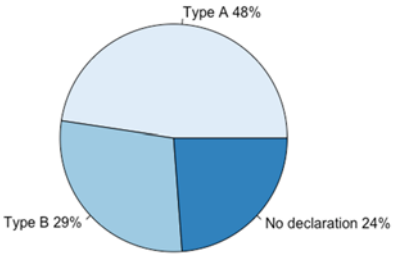

Figure 6: Chip type

3.4.2 Document verification systems

Sixteen different document verification systems participated to the test, most of them using a PCSC reader and three mobile devices.

When registering for the test, document verification system providers were asked to provide some basic information on the device under test. Here is a summary of the overall characteristics declared for the document verification systems.

Feature		Counts
Test software		10/16

OCR reader type	Full page reader	10/16
	Manual MRZ entry	6/10
DG read and displayed	DG1	15/16
	DG2	16/16
	DG3	16/16
	DG4	8/16
	DG5	6/16
	DG6	6/16
	DG7	8/16
	DG8	4/16
	DG9	4/16
	DG10	4/16
	DG11	8/16
	DG12	8/16
	DG13	9/16
	DG14	14/16
	DG15	13/16
	DG16	6/16
Passive authentication supported signature algorithms	DSA	11/16
	ECDSA	15/16
	RSASSA-PKCS1_v15	13/16
	RSASSA-PSS	13/16
Passive authentication supported hash algorithms	SHA-1	15/16
	SHA-224	13/16
	SHA-256	15/16
	SHA-384	14/16
	SHA-512	14/16
CDS validation		15/16
CDS revocation		10/16
BAC support		15/16
PACE key agreement algorithms	DH	15/16
	ECDH	16/16
PACE Mapping	Generic mapping	16/16
	Integrated mapping	14/16
	Chip authentication mapping	13/16
Support for CAN		15/16
Active authentication supported signature algorithms	ECDSA	12/16
	RSA ISO/IEC 9796-2 DS scheme 1	14/16
Active authentication supported hash algorithms	SHA-1	14/16
	SHA-224	12/16
	SHA-256	14/16
	SHA-384	13/16
	SHA-512	13/16
Chip authentication supported signature algorithms	DH	12/16
	ECDH	15/16
Terminal authentication supported signature algorithm	ECDSA	15/16
	RSASSA-PKCS1_v15	12/16
	RSASSA-PSS	12/16
Terminal authentication supported hash algorithms	SHA-1	15/16
	SHA-224	15/16
	SHA-256	15/16
	SHA-384	12/16
	SHA-512	12/16

Table 1. Document verification system characteristics.

In Annex B, we will show that in some cases there were some discrepancies between the declarations provided in the ICS and the data resulting from the smoke test execution. In the case of document verification systems, we have no possibility to provide a similar assessment of the data from the declarations provided by document verification systems producers.

3.5 Smoke Test Execution

In computer testing, smoke testing (also called confidence testing) is a preliminary test to reveal simple failures and, if this case happens, to reject the tested version of the device. In this case, smoke testing consisted in:

- The visual inspection of the eMRTD (see ICAO 9303 [1], [2], [3], [4] and [5]);
- The electronic inspection of the eMRTD (see ICAO 9303 [6], [7] and [8] and BSI TR03110 [9] and [10]).

Smoke testing was executed by the expert's team while the documents were being registered. As soon as a set of documents from a participant was registered, labelled and put into a labelled envelope, the envelope was passed on to the experts team who picked up randomly one of the samples from the envelope and tested it. If smoke test was successful, that sample from the set of five submitted by the applicant was set aside for the test in the test room on the inspection systems test stations and by test laboratories.

3.5.1 Software

Application software with the following characteristics was used for the electronic inspection part of the smoke test:

- Use with a PCSC reader;
- Importation of cryptographic material (certificates, keys and CRLs) for Passive Authentication (PA) and Terminal Authentication (TA) v1;
- Exportation of the Data Groups (DGs) and Document Signer Certificate (CDS) in the eMRTD for further analysis;

Additional software was used to check and process cryptographic material sent by the participants:

- OpenSSL version 0.9.8, for the conversion of certificates to a uniform format.
- Notepad++ with Hex plugin, for inspection of the cryptographic material in binary format.
- One in-house JRC tool, for the generation of the TA v1 certificate chain when only the CVCA certificate and its private key were available.

3.5.2 Hardware

Five test stations were used for the smoke test.

Three different PCSC readers were used in the five test stations:

- Omnikey 5421 contactless reader (default baud rate of 106 kbps);
- SCM Microsystems Inc. SDI011G contactless reader;
- SCM Microsystems Inc. SDI010 contactless Reader.

Each expert team member used their own test workstation with their own PCSC reader.

In order to get more homogenous results from the smoke test, it would be advisable to use the same version of the inspection software configured in the same manner and the same PCSC reading device. However, no major inconsistencies were reported during the smoke tests.

3.5.3 Criteria

The smoke test phase was considered successful if the eMRTD executed:

- PACE protocol successfully;
- Chip Authentication successfully, if the protocol was present in the eMRTD;

- Active Authentication successfully, if the protocol was present in the eMRTD;
- Read-out of basic data successfully;
- Passive Authentication successfully, including the verification of the CDS signature using the CSCA public key;
- Terminal Authentication v1 successfully, if the protocol was present in the eMRTD;
- Read-out of sensitive data successfully, if present in the eMRTD.

With the special considerations:

- eMRTDs, which did not include a booklet (e.g. an eMRTD with the contactless chip in a cardboard support) or not implementing a minimal set of optical security features, were accepted;
- eMRTDs showing random communication errors but which finally managed to finalize the smoke test phase were accepted;
- eMRTDs showing ASN.1 coding errors in DGs different than DG1, DG2 and DG3 were accepted;
- eMRTDs coding zero instances of biometric sensitive data (e.g. see ICAO 9303/10 [6], 6.3.2.2) were accepted;
- eMRTDs returning error SWs (not according to the SWs specified in ICAO 9303/10 [6]) for EF.ATR/INFO or EF.DIR were accepted.

The smoke test phase was considered unsuccessful for the following scenarios:

- eMRTDs without PACE support;
- If the participant did not provide the full set of cryptographic material (with the exception of the CRL).

3.5.4 Results

Forty-two models were received and labelled from d01 to d42.

Two were rejected by the smoke test phase because they did not fulfil all the requirements for participation to the test.

The analysis of the smoke test results can be found in Annex B.

3.5.5 Smoke tests considerations and recommendations

Analysis of the Implementation Conformity Statements and smoke test data indicate that the details reported in the ICS are not always consistent with the details of the algorithms and protocols actually supported by the chips. This might have an influence on the results of the conformity tests depending on how much the configuration of the test cases is affected by the ICS provided by the applicant.

It is recommended that applicants double-check the conformity declarations; alternatively, if enough time is scheduled for the smoke tests, ICS should be amended after the execution of the smoke test by the expert's team.

3.6 Conformity tests execution

Conformity tests were executed on a subset of the test cases defined in the document ICAO TR RF Protocol and Application Test Standard for e-Passports, Part 3" (Version 2.10). In particular, tests in the following test units were executed:

Test scope	Test Unit	OSI Layer
Security Conditions for PACE-enabled eMRTDs	ISO7816_O	6
Password Authenticated Connection Establishment	ISO7816_P	6
Select and Read EF.CardAccess	ISO7816_Q	6

Select and Read EF.CardSecurity	ISO7816_S	6
Matching between EF.DG14 and EF.CardAccess	LDS_E	7
Structure of EF.CardAccess	LDS_I	7
Structure of EF.CardSecurity	LDS_K	7
SOD LDS Object (Passive Authentication)	LDS_D_06	7

Table 2. Conformity test cases subset.

Test laboratories were asked to report the results in a comma separated values log file for each document under test. The following data were logged for each test case executed:

Lab_id, doc_id, test_case_id, test_result

Possible test result values were **Pass, Fail, Not applicable,** to be recorded as **“P”, “F”, “N”.**

3.7 Conformity tests: analysis of the results

3.7.1 Results pre-processing

Each laboratory at the end of the test delivered 39 files each one containing the results of the execution of the selected test cases on each specific document. One document was not submitted to the conformity test by decision of the experts’ team.

In order to process the data and provide the summaries and statistics presented in the following paragraphs, the process outlined below was followed.

- All the files produced by each test laboratory were concatenated into one single file.
- The **lab_id** was modified into the string "**lab0x**", where "**x**" is a number identifying each laboratory.
- The **doc_id** was modified into "**d0x_y**", where "**x**" is the number identifying a document and "**y**" is the number identifying the sample selected for the test among the five samples provided by each document producer.
- The separator was modified in "**;**" if "**,**" had been used instead.
- The result value "**NA**" was modified in "**N**".
- End of line character was harmonised.

The modifications indicated above were necessary to ensure that the labels used to report the results were consistent in the files produced by the three laboratories.

All modifications were made using UNIX command line text processing tools.

In some cases, the test reports included outcomes for some test cases which have been removed in the last version of the ICAO standard. These tests were removed.

Finally, the three files were concatenated into a single file, the header line:

LAB_ID; DOC_ID; TEST_ID; RESULT

Was added at the beginning of the file and the resulting file was imported into the "R" processing system for the statistics and the graphics.

3.7.2 Overall results

A total number of 18.135 test cases were executed on the samples by the three test laboratories.

The resulting figures are listed below, results separated by layer are also provided.

Overall results (18.135 test cases):

Passed: 11563 (63.76 %)

Failed: 155 (0.86 %)

Not applicable: 6417 (35.38 %)

Layer 6 (16.614 test cases executed):

Passed: 10.884 (65.51 %)

Failed: 123 (0.74 %)

Not applicable: 5607 (33.75 %)

Layer 7 (1.521 test cases executed)

Passed: 679 (44.64 %)

Failed: 32 (2.10 %)

Not applicable: 810 (53.25 %)

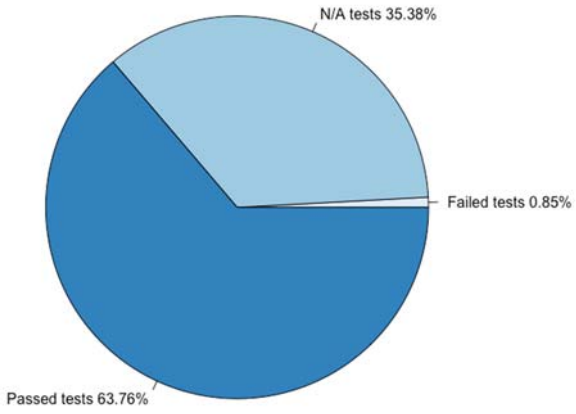

Figure 7: Test results

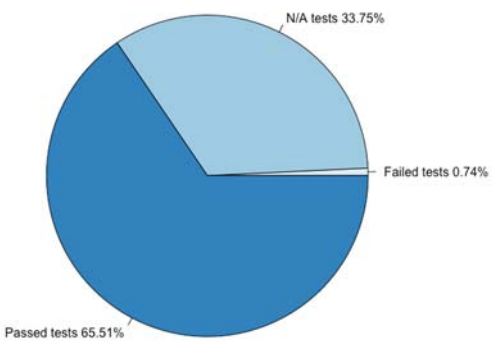

Figure 8: Test results for layer 6

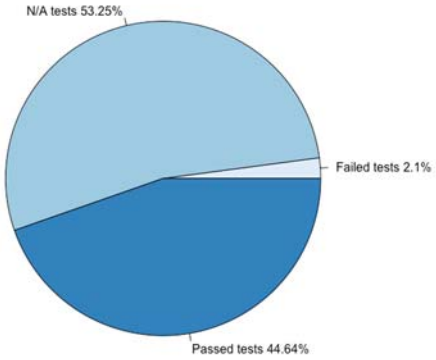

Figure 9: Test results for layer 7

Figure 10 shows the results (pass, fail, not applicable) for each document. Each line represents the results for a single document in all the tests executed. The diagram is order in decreasing order of number of "P".

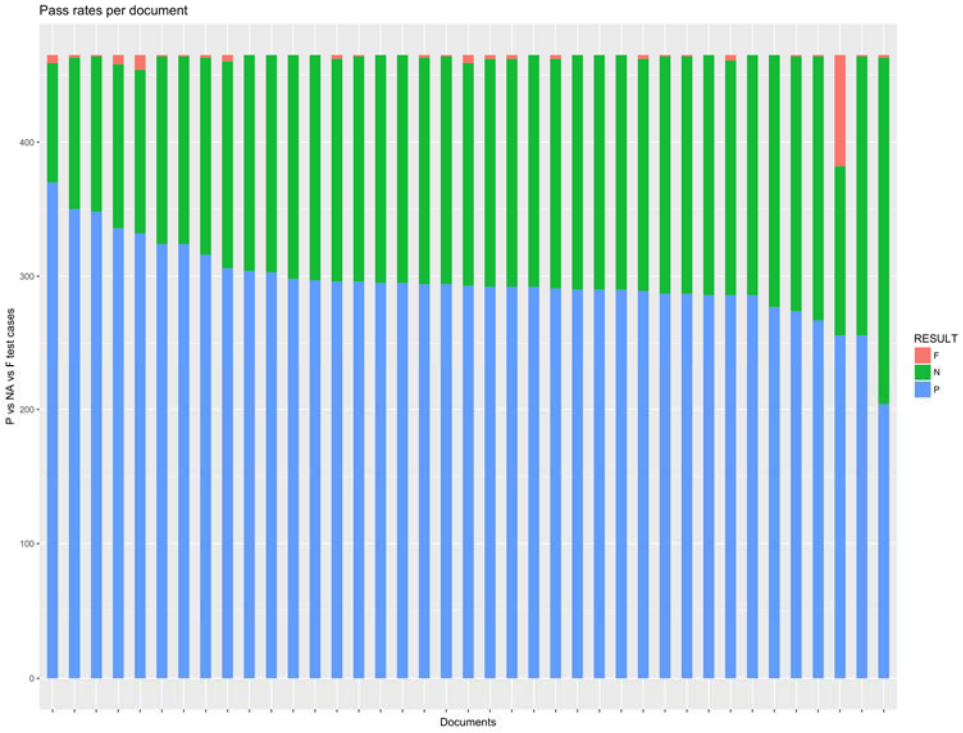

Figure 10: Pass, Not Applicable (Executed) and Fail results in decreasing order by number of tests passed

The diagram in Figure 11 is constructed following the same logic as the diagram in Figure 10 but with data for layer 6 tests only. The diagram is ordered in the same order as the diagram in Figure 10, i.e. in decreasing number of overall "P"s for each document.

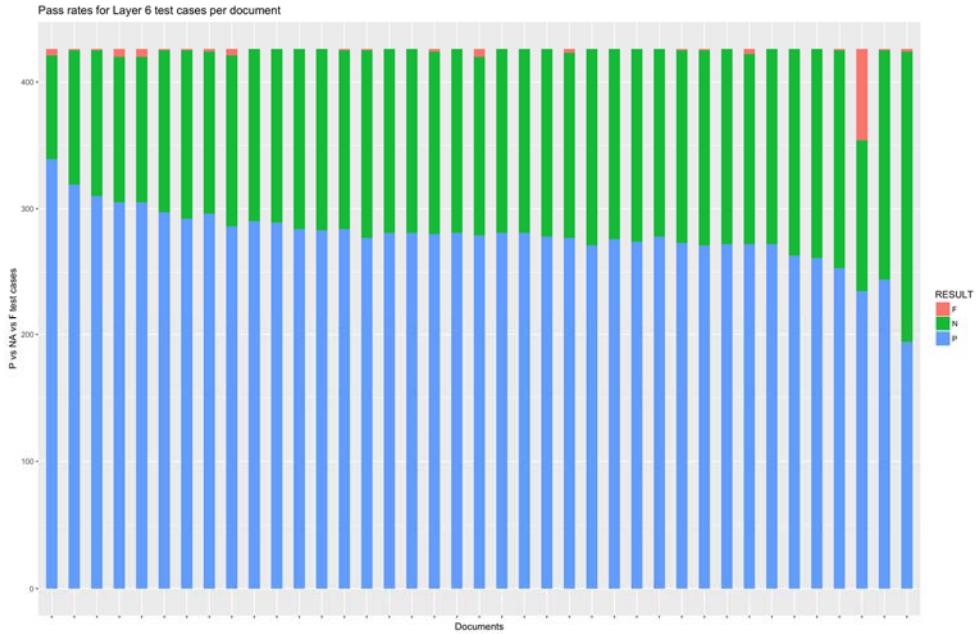

Figure 11: Pass, Not Applicable (Executed) and Fail results for Layer 6 tests in decreasing order by number of tests passed

The diagram in Figure 12 is constructed following the same logic as the diagram in Figure 11 but with data for layer 7 tests only. The diagram is ordered in the same order as the diagram in Figure 10, i.e. in decreasing number of overall "P"'s for each document.

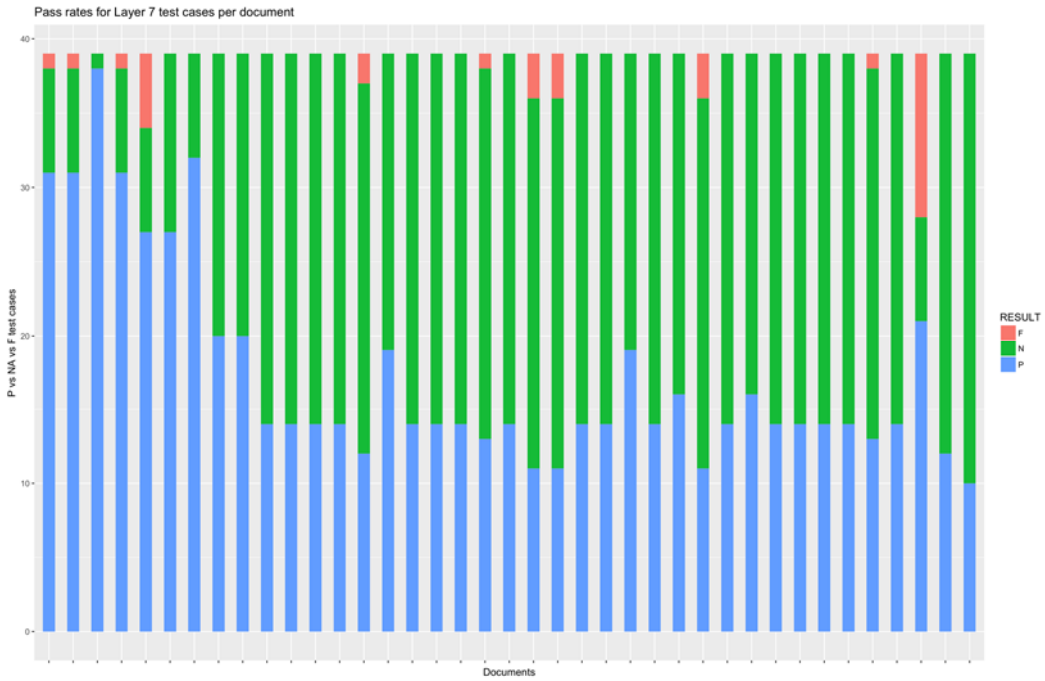

Figure 12: Pass, Not Applicable (Executed) and Fail results for Layer 7 tests in decreasing order by number of tests passed

Figure 13 shows only the number of fails per each document. The diagram is ordered in decreasing number of "F"s, i.e. the first document in the list is the one for which the highest number of failed tests was reported. The highest number of fails reported for a single document was over 80, then 15 documents follow with a number of fails from 10 to 2, while for the rest of the documents either 1 or no fails were reported.

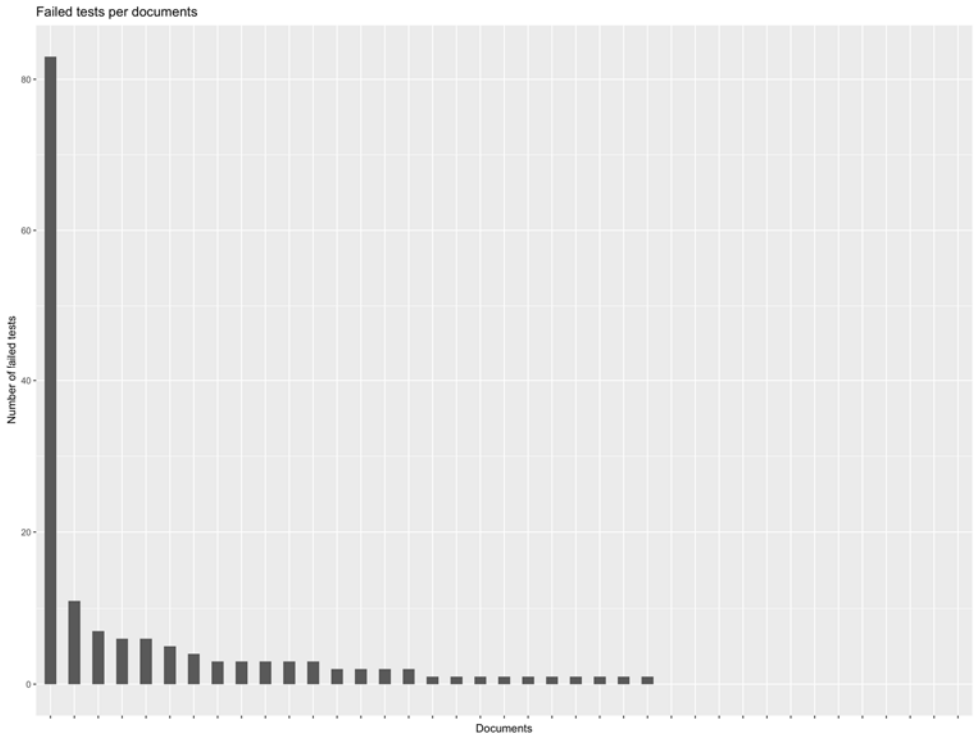

Figure 13: Failed tests per document

The pie chart in Figure 14 shows how the total counts of failures are distributed in the documents, i.e. the percentage of documents for which 0, 1, 2 or more fails were reported. The diagram is cumulative for the three laboratories.

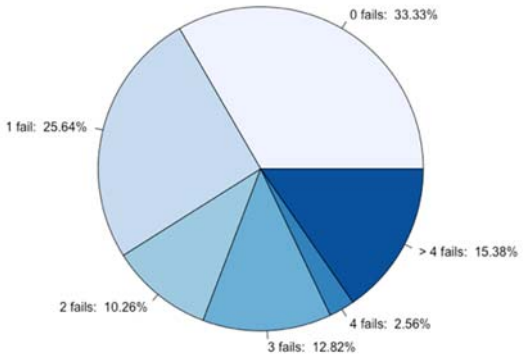

Figure 14: Distribution of number of fails in documents

The diagrams in Figure 15 and Figure 16 are similar to the diagram in Figure 14, but are focused respectively on layer 6 test cases and layer 7 test cases.

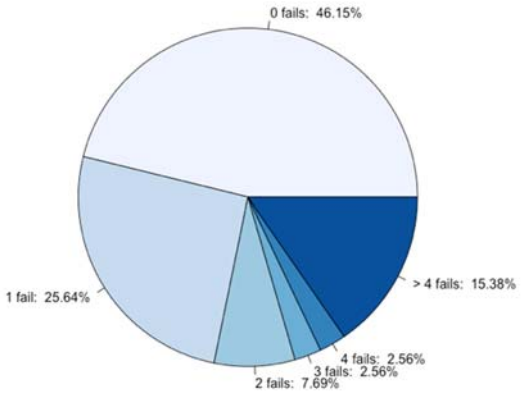

Figure 15: Distribution of number of fails in documents for layer 6 tests

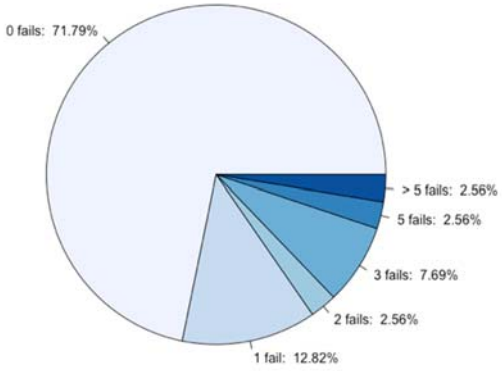

Figure 16: Distribution of number of fails in documents for layer 7 tests

The diagram in Figure 17 shows the results of the tests from the point of view of the test cases, i.e. it shows in decreasing order, the test cases which counted the highest number of fails.

The test case that failed most often was ISO7816_P_02, which is aimed at testing a valid PACE protocol with CAN password.

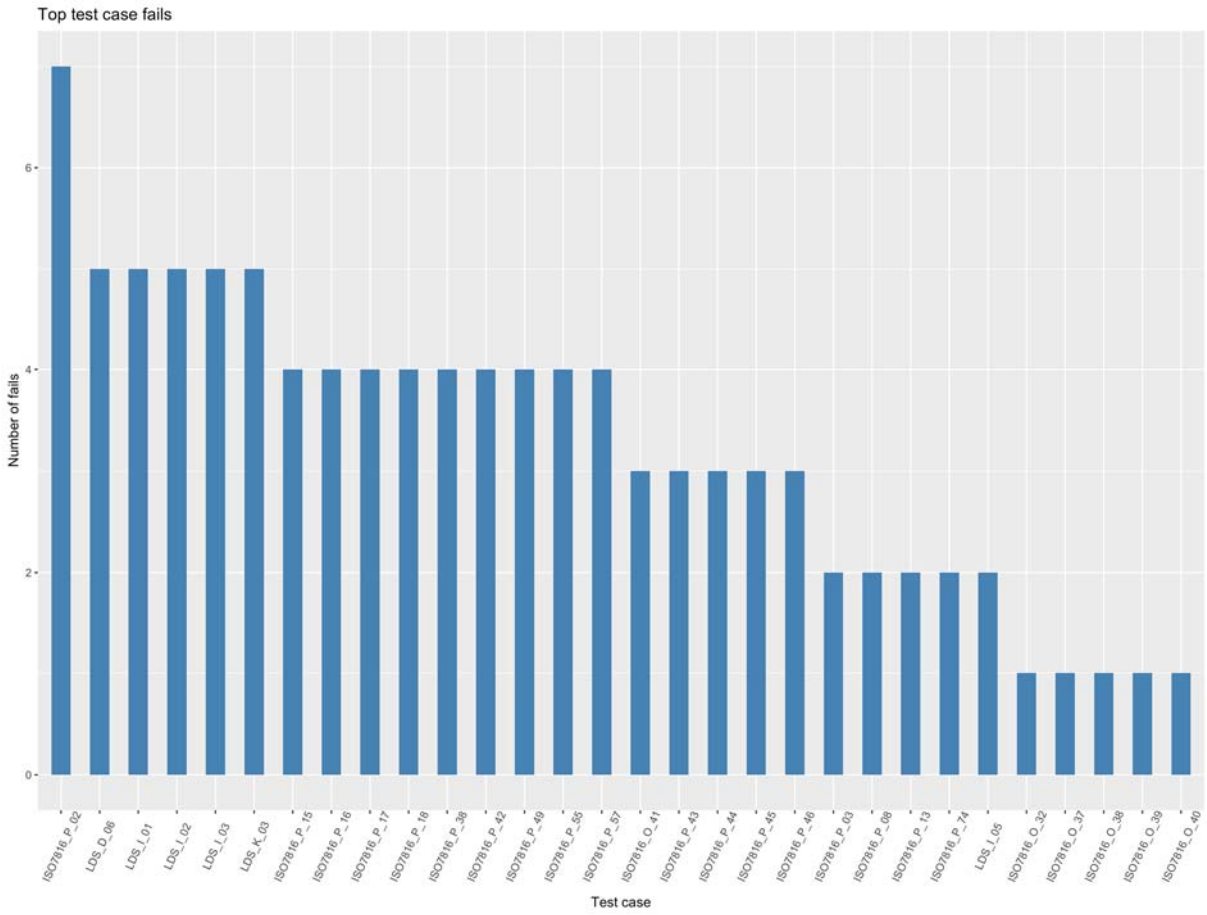

Figure 17: Fails per test case

The diagram in Figure 18 shows in decreasing order the test cases which more often were marked as "Not applicable". Most of them are in the ISO7816_O test unit, which is related to the security conditions of a PACE-protected eMRTD, followed by some test cases in the ISO7816_P test unit.

Finally, the diagram in Figure 19 shows the distribution of pass, fail and not applicable in the eight data units considered for the test event. It shows at a glance that the ISO7816_O test unit was the one with the highest number of "not applicable", while the ISO7816_P test unit was the one with the highest number of fails (this is most probably due to tests involving the use of CAN).

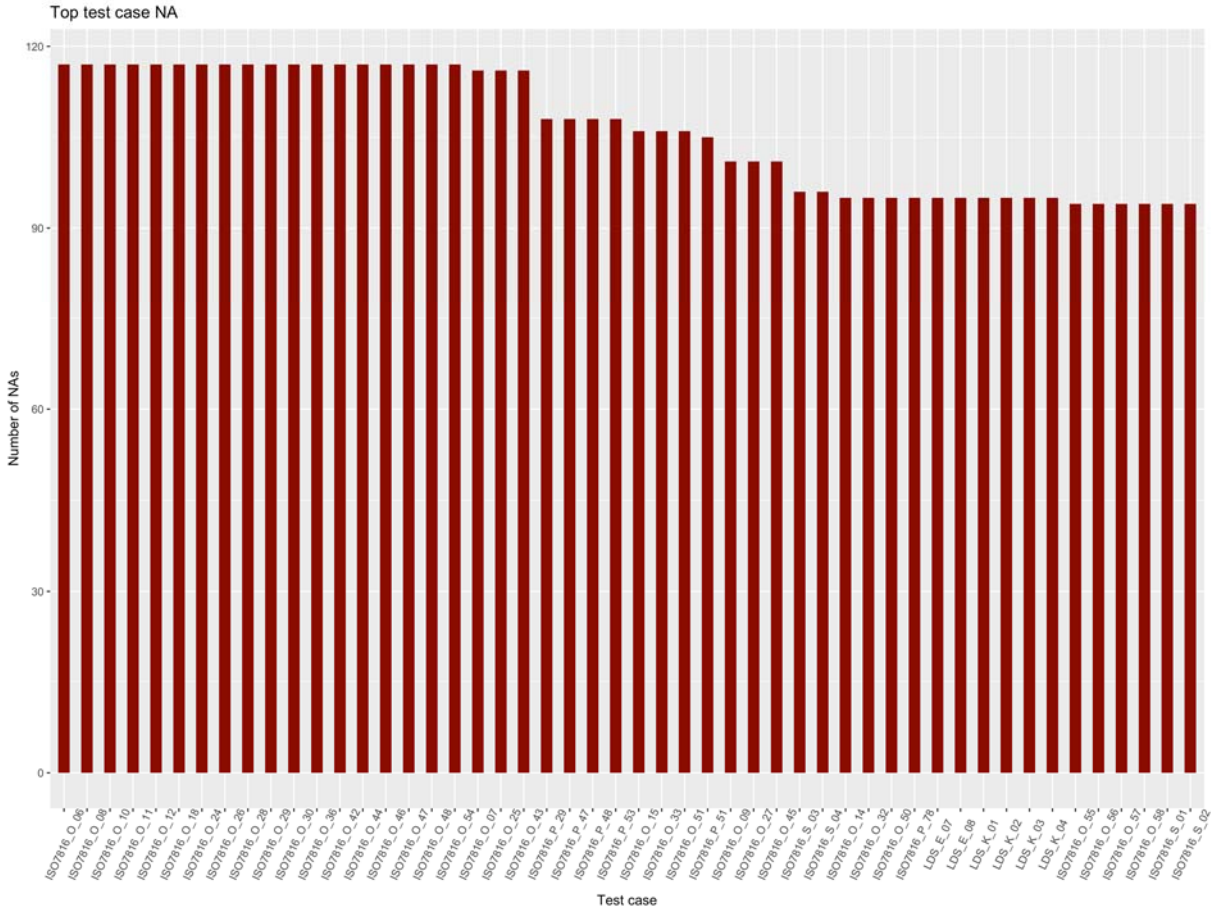

Figure 18: Not applicable test cases

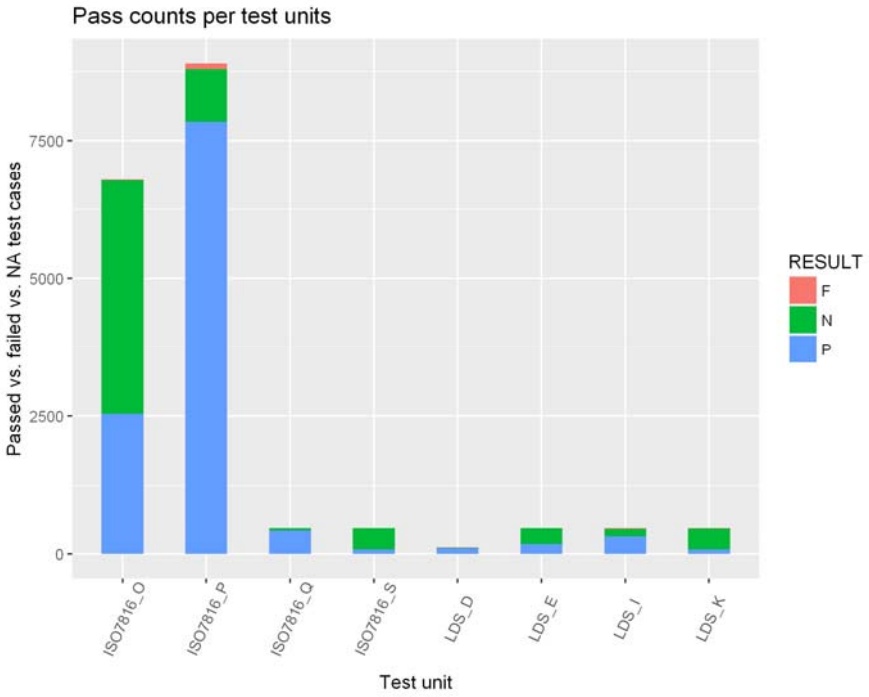

Figure 19: Results in each test unit

In some cases, for some documents, there is a discrepancy among the results reported for the same test by different laboratories. The diagram in Figure 20 shows in decreasing order the number of differences in the reports of the test laboratories for each document, while the diagram in Figure 21 shows the test cases for which a different result is reported. There is no indication in these diagrams about the type of difference, i.e. if it was an "N" reported as an "F" or something different.

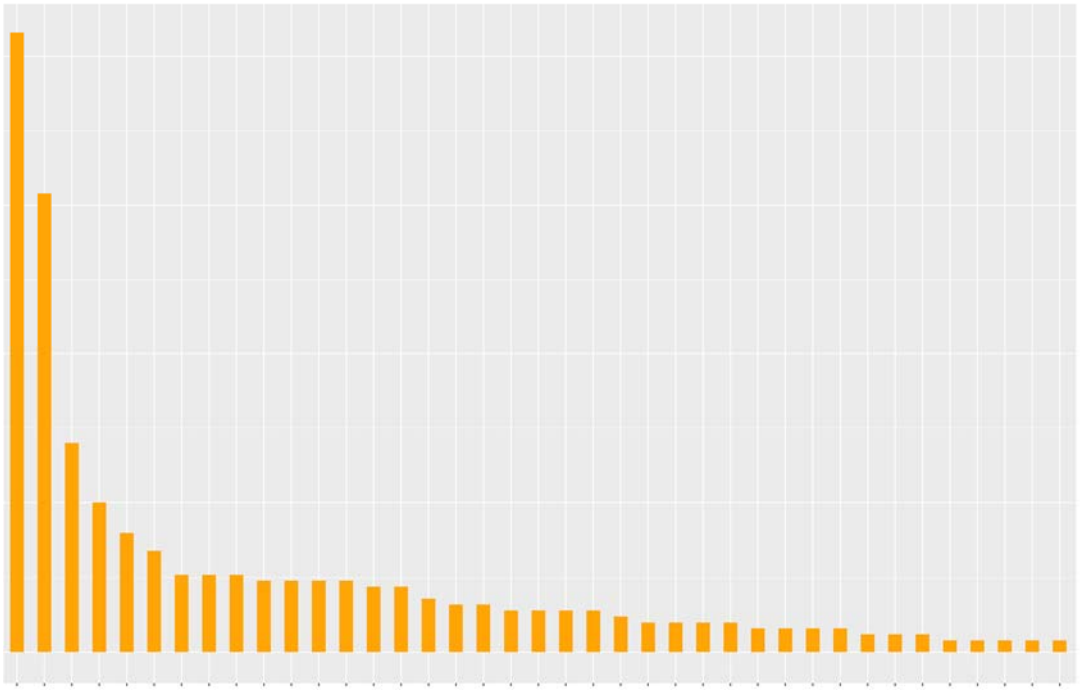

Figure 20: Number of different result per document

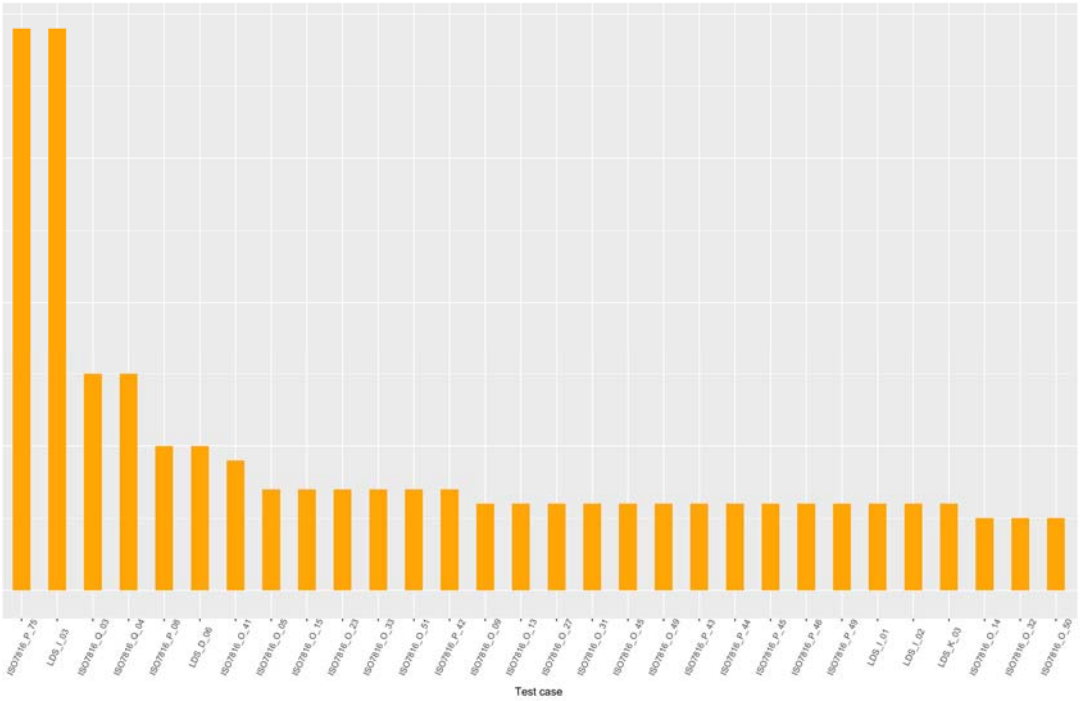

Figure 21: Test cases which present the highest number of differences among the laboratories

3.7.3 Conformity tests considerations and recommendations

Overall the conformity test results are very good: less than 1% of the total number of tests failed. This indicates a very high quality for the chips and the personalisation. It also indicates that the specifications are stable since implementations contain very few and small deviations. The failure rate was slightly higher for the layer 7 tests (related to personalisation) than for layer 6 tests (related to the chip operating system). However, there were some changes in the way some of the results were reported by the different laboratories, for instance the absence of CAN as basis for PACE was reported as "F" in some cases and as "N" in other cases. There was also the case of one document on which there was a great discrepancy in the results reported by the different laboratories. However, without the APDU trace for the tests we are not able to provide a more detailed analysis on the reasons for reporting different results for some test cases on some documents.

In order to address these kinds of issues, it is recommended that a follow-up session is held with the test laboratories in order to analyse the reasons for the discrepancies.

It is also recommended that extra-time is available, after the tests have been completed and the preliminary results delivered to the document providers, for bilateral discussions and clarifications between the test laboratories and the document providers.

3.8 Crossover tests execution

Crossover tests consisted in verifying that all document samples selected after the execution of the smoke tests could be successfully processed by the document verification systems.

Since there is no standard for crossover tests which indicates how the test should be conducted, a test report format which could guide the verification process was prepared and distributed to the document verification system providers. The structure of the test report is described in section 2.4.2, while the full detail is provided in Annex A.

A total number of 16 different document verification systems participated to the test.

The document samples (40 in total) were distributed into 20 envelopes each containing 2 samples and the envelopes were circulated from one test station to the next. Each test station had 20 minutes to complete the tests on the two different samples and complete the test report. At the end of the 20 minutes slot each station had to move the envelope to the next testing station.

At the end of each day, the test report files produced were collected.

At the end of the second day, the test report files were processed in order to be imported into an SQL database and preliminary results and indications on the outcome of the tests were provided to test participants at the closing conference.

3.9 Crossover tests: analysis of the results

3.9.1 Results pre-processing

The files containing the test results were converted into text files and imported into an SQL database.

A total number of 640 files (corresponding to 40 files per 16 test stations) was imported in the SQL database. The results reported in the following sections of this report were extracted with SQL queries from the database.

A subset of the data (i.e. the yes/no/na type of replies) was exported from the database and converted into an "R" data frame with the following structure:

- Inspection_system Document_Id.
- Chip_type
- Successful_CSCA_certificate_import
- Successful_CRL_import
- Successful_CVCA_certificate_import
- Successful_DV_certificate_import
- Successful_IS_credentials_import
- PA_executed
- PA_successful
- BAC_executed
- BAC_successful
- PACE_executed
- PACE_successful
- Active_Authentication_executed
- Active_Authentication_successful
- Chip_Authentication_executed
- Chip_Authentication_successful
- PACE-CAM_executed
- PACE-CAM_successful
- Terminal_Authentication_executed
- Terminal_Authentication_successful
- Comparison_of_conventional_MRZ(OCR-B)_and_IC-based_MRZ(LDS)
- DG2_Facial_image_displayed_correctly
- DG3_Fingerprint_image(s)_displayed_correctly
- DG4_Eye_image(s)_displayed_correctly
- DG5_Portrait_displayed_correctly
- DG7_Signature_or_usual_mark_displayed_correctly
- DG11_Additional_Personal_Detail(s)_decoded_correctly
- DG12_Additional_Document_Detail(s)_decoded_correctly
- DG16_Person(s)_to_Notify_decoded_correctly
- EF.ATRInfo_decoded_correctly
- EF.COM_decoded_correctly

Such data frame was used to produce the diagrams in the following sections using the "R" data processing environment.

3.9.2 Overall results

3.9.2.1 Processing of certificates and CRLs

The first step in the execution of the crossover test was to import the certificates, CRLs and private keys required to execute Passive Authentication and access the fingerprints (i.e. execute Terminal Authentication).

The test report form contained a section dedicated to the results related to certificate processing (the complete test report form is provided in Annex A).

The expectation was that all document verification system would report CSCA import as successful; this was the default value in the test report sheet.

However, CSCA import was reported as unsuccessful in 33 cases, 30 of these results were reported by the same document inspection system and in 18 cases a reason was provided for the unsuccessful result and the reason was "**Not supported**", while in eight cases the reason was "**certificate.error.signature"** and in one case the reason was **"Certificate not available".** Therefore, it would seem that this particular document verification system did not support importing the CSCA certificate and therefore did not execute Passive Authentication.

Leaving out the **"Certificate not available"** case which should be attributed to human error in the reporting (since we know that CSCA certificates were available and provided for all the documents submitted to the test), it would be worthwhile to investigate if the lack of support for the CSCA certificate import functionality is due to the fact that the inspection system software was a prototype, or if it is to be considered as one component of a complete system in which this functionality is responsibility of a different component of a system which was not fully represented in the test environment. This is one of the cases in which a preliminary test on the document verification systems before the test would have provided additional insight into this particular issue.

In the case of the CRLs, their import was reported as unsuccessful in 410 cases. This was below the expected value which was 560, i.e. the number of documents for which the CRL was available multiplied by the number of test stations (the CRL was available for

five documents only). This result indicates that in 150 cases the default value "successful" was kept in the report form, which is an indication that the compilation of the test report for the crossover test was not 100% accurate. This, in turn, might indicate that more time should be allocated to crossover tests. A guided online tool for reporting would also help in ensuring more consistent results.

Still on the CRL import functionality, the following can be observed from the data processed in the SQL database:

- *CRL import was reported as **successful** when **no CRL** was available in **172 cases***
- *CRL import was reported as **unsuccessful** when **CRL** was available in **22 cases***
- *CRL import was reported as **successful** when **CRL** was available in **58 cases***
- *CRL import was reported as **unsuccessful** when **no CRL** was available in **388 cases***

Only in 294 cases, a reason was given for the unsuccessful import of the CRL and the reason was indicated correctly as "**CRL.notAvailable**". In the other cases, a reason was neither provided nor selected from the available drop-down menu.

3.9.2.2 PACE execution

One section in the test report was dedicated to the execution of the access control security mechanism.

Both PACE and BAC were listed in this section. For both protocols, two questions were asked:

1. If the protocol was executed, with possible answers: yes/no
2. If the execution was successful, with possible answers: yes/no/not applicable

The logic was that if a protocol is executed, then report about the result, which can be either successful or not. Otherwise if a protocol is not executed the reply to the second question should be "Not applicable".

The reason for non-execution could be that the other, alternative protocol was used.

For this reason, the following values were given as defaults:

- BAC executed: NO
- BAC successful: NOT APPLICABLE
- PACE executed: YES
- PACE successful: YES

After evaluation of the results reported on the execution of the PACE access control mechanism, we find that:

- PACE is reported as **executed** and **successful 549 times**
- PACE is reported as **executed** and **not successful 38 times**
- PACE is reported as **NOT executed** and **successful** once
- PACE is reported as **NOT executed** and **NOT successful** once
- PACE is reported as **executed** and result of execution is **unknown (NA) 14 times**
- PACE is reported as **NOT executed** and result of execution is **unknown (NA) 5 times**

In red, the cases where the report is not consistent with the process indicated in section 2.4.2.

PACE_CAM was reported as executed and not successful in 12 cases only, but it was also reported as unsuccessful in 45 cases when it was also reported as "not executed". This latter case looks again like an error in reporting. According to the logic of the test report tool, if a protocol is not executed, it cannot be reported as successfully or unsuccessfully executed but the result of the execution should be reported as "not applicable".

The list below is an example of the reasons which were provided in the 38 cases where PACE was executed and not successful:

- document.notSupported/EF.CardAccess.notFound
- APDU.ERROR.GENERAL_AUTHENTICATE.mutualAuthentication
- APDU.ERROR.GENERAL_AUTHENTICATE.mappingNonce
- APDU.ERROR.GENERAL_AUTHENTICATE.encryptedNonce
- Reader's Problem: Extended length is not supported
- Only IM failed, GM successful
- ISO14443.error
- APDU.ERROR.SELECT.EF.CardAccess
- Chip requires more power than mobile reader can support
- APDU.ERROR.READ_BINARY.EF.CardAccess
- InspectionSystem.cryptographicModule.internalError
- DH algorithms are not supported by the verification system
- IS internal error : PACE - CAM error

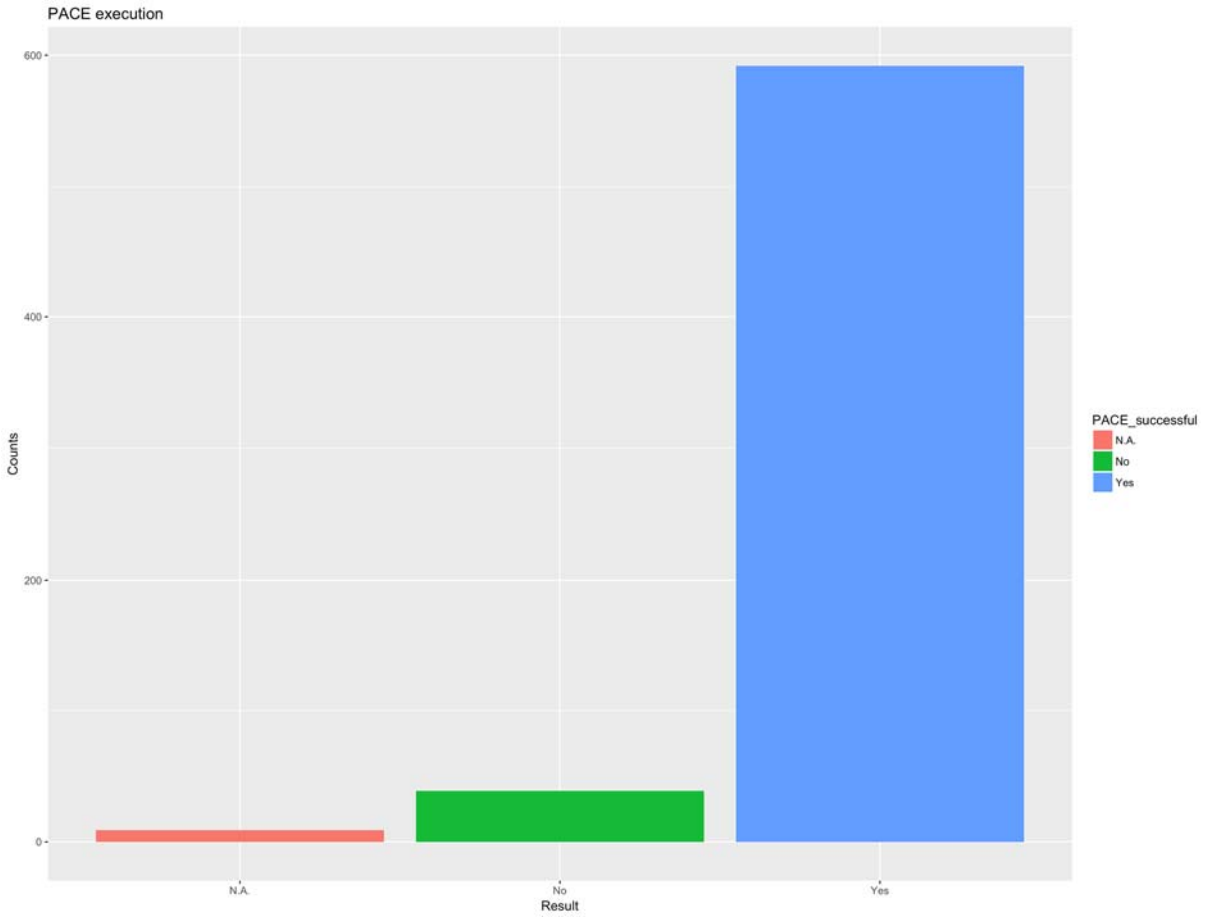

Figure 22: Successful execution of PACE

The diagram in Figure 22 shows the total number of "NA", "No" and "Yes" results as reported by the test stations.

Since it was reported that in the past a different behaviour had been observed in some cases between type A and type B chips, we provide here diagrams also separated by

"type A" and "type B" chips. For information for the chip type we relied on the ICS compiled by the applicants. Since not all applicants provided information about the chip type, a third diagram indicates the data for those chips for which the chip-type was unknown.

The three diagrams in Figure 23, Figure 24 and Figure 25 show the total number of "NA", "No" and "Yes" results as reported by the test stations by chip type.

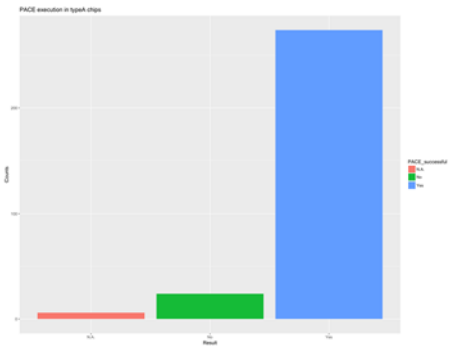

Figure 23: Successful execution of PACE in type A chips

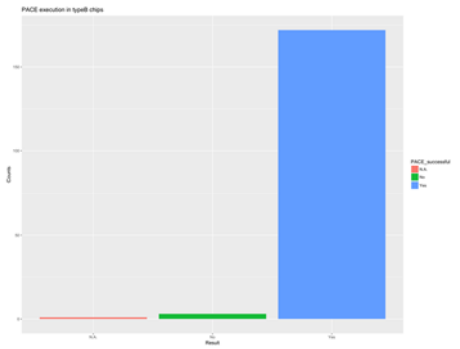

Figure 24: Successful execution of PACE in type B chips

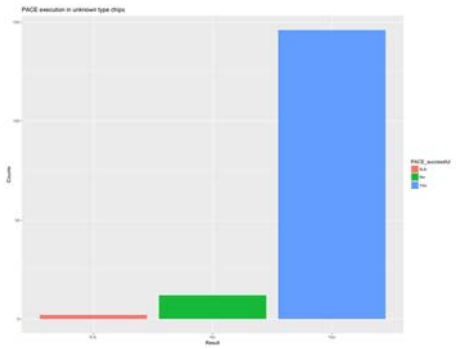

Figure 25: Successful execution of PACE in chips the type of which was not specified in the ICS

The diagram in Figure 26 shows a stacked bar plot indicating the number of "yes", "No" and "NA" as results of the PACE algorithm execution as reported by the test stations. The diagram is ordered by decreasing number of "Yes". Eighteen (18) documents were reported as successfully executing PACE by all test stations. The rest were reported as either not successful or not executed by at least one test station.

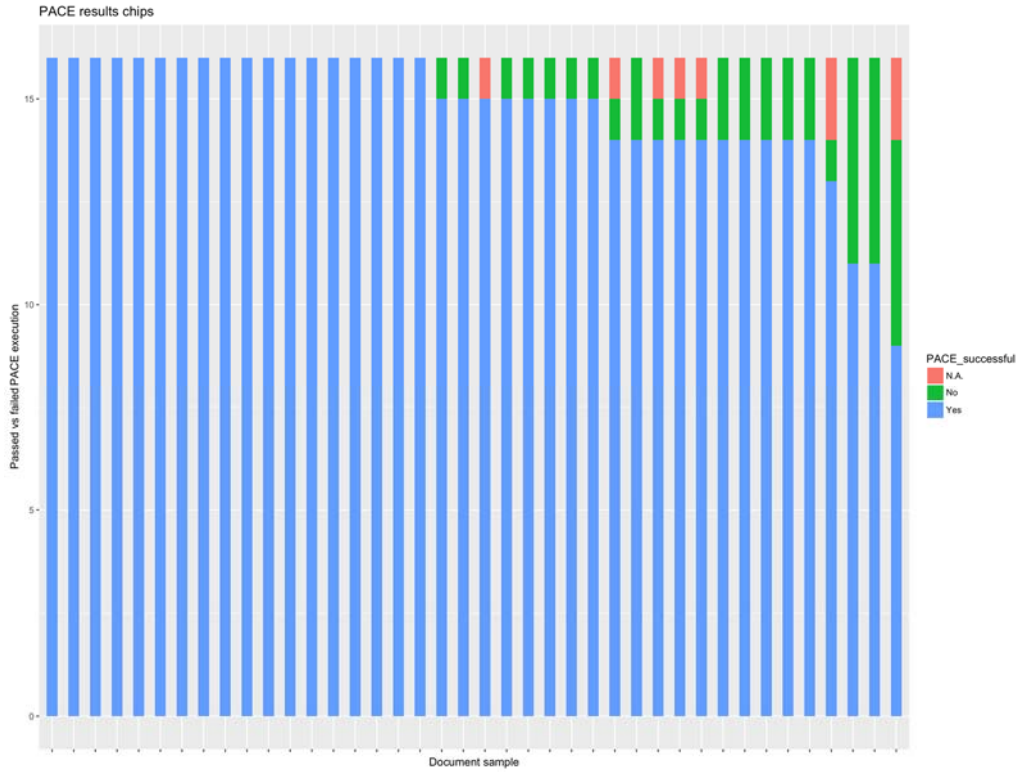

Figure 26: Results of PACE execution by document

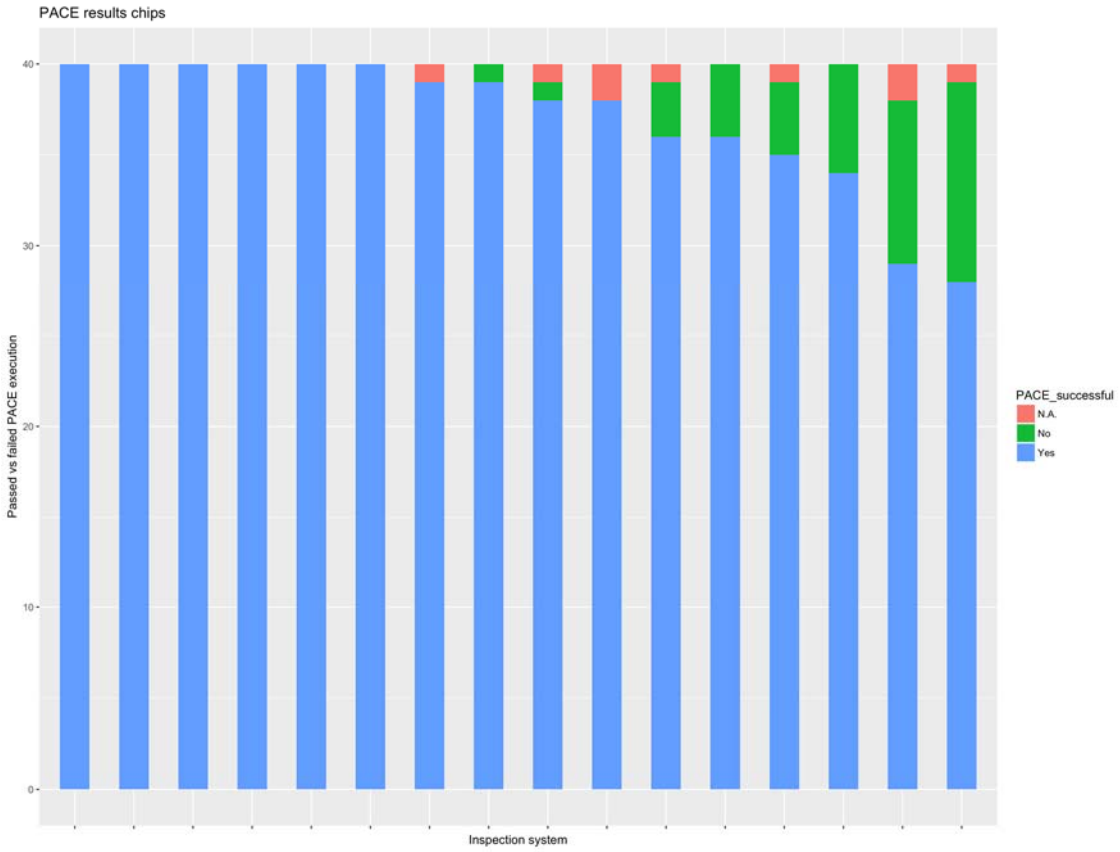

Figure 27: Results of PACE execution by inspection system

The diagram in Figure 27 shows a stacked bar plot indicating the number of "yes", "No" and "NA" as results of the PACE algorithm execution reported by the test stations. The diagram is ordered by decreasing number of "Yes". Six (6) test stations reported a successful execution of PACE on all documents. The rest reported PACE as either not successful or not executed on at least one document.

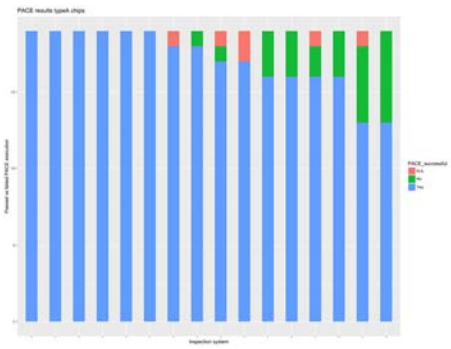

Figure 28: Results of PACE execution by inspection system (type A chips)

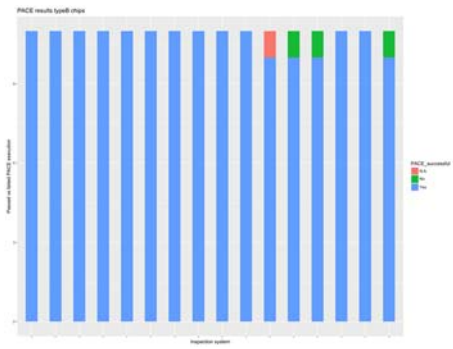

Figure 29: Results of PACE execution by inspection system (type B chip)

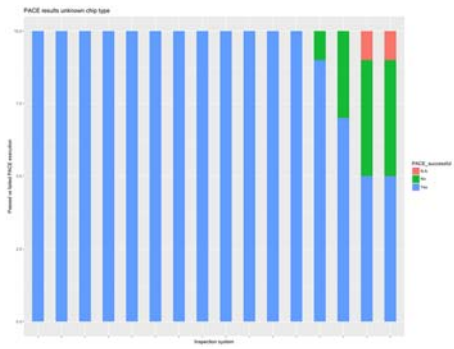

Figure 30: Results of PACE execution by inspection system (unspecified chip type)

Similarly to Figure 23, Figure 24 and Figure 25, Figure 28, Figure 29 and Figure 30 show the same diagram as Figure 27 but partitioned by chip type. The order of the inspection systems on the x-axis is the same as in Figure 27.

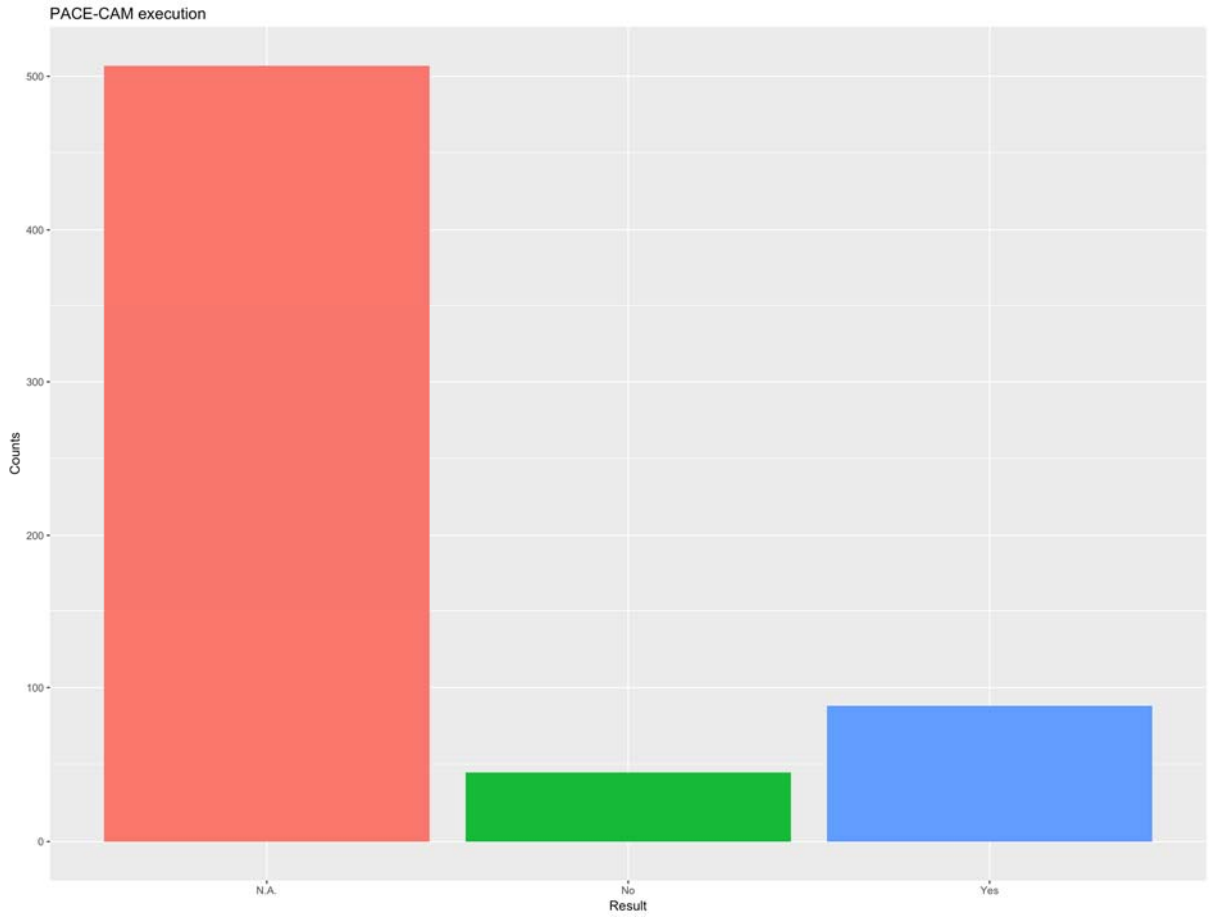

Figure 31: Successful execution of PACE-CAM

The diagram in Figure 31 shows the results of the PACE-CAM execution. Most of the documents are reported as not supporting PACE-CAM.

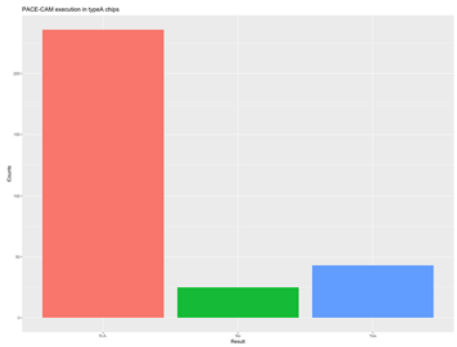

Figure 32: Successful execution of PACE-CAM in type A chips

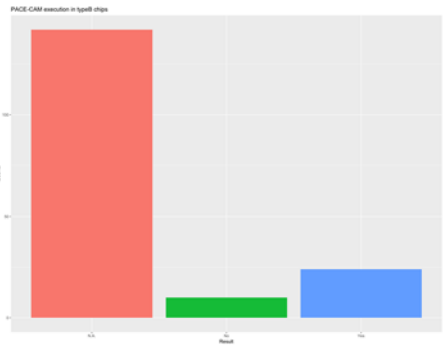

Figure 33: Successful execution of PACE-CAM in type B chips

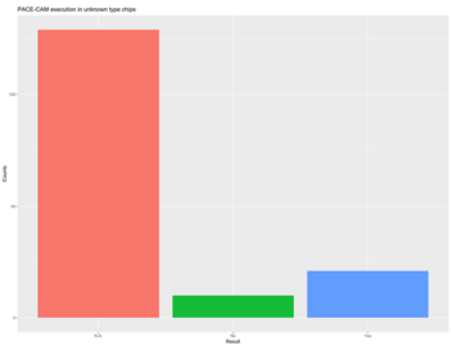

Figure 34: Successful execution of PACE-CAM in chips the type of which was not specified in the ICS

Figure 32, Figure 33 and Figure 34 show the same information as in Figure 31 but partitioned by chip type. No major difference can be observed between the results reported for type-A and type-B chips.

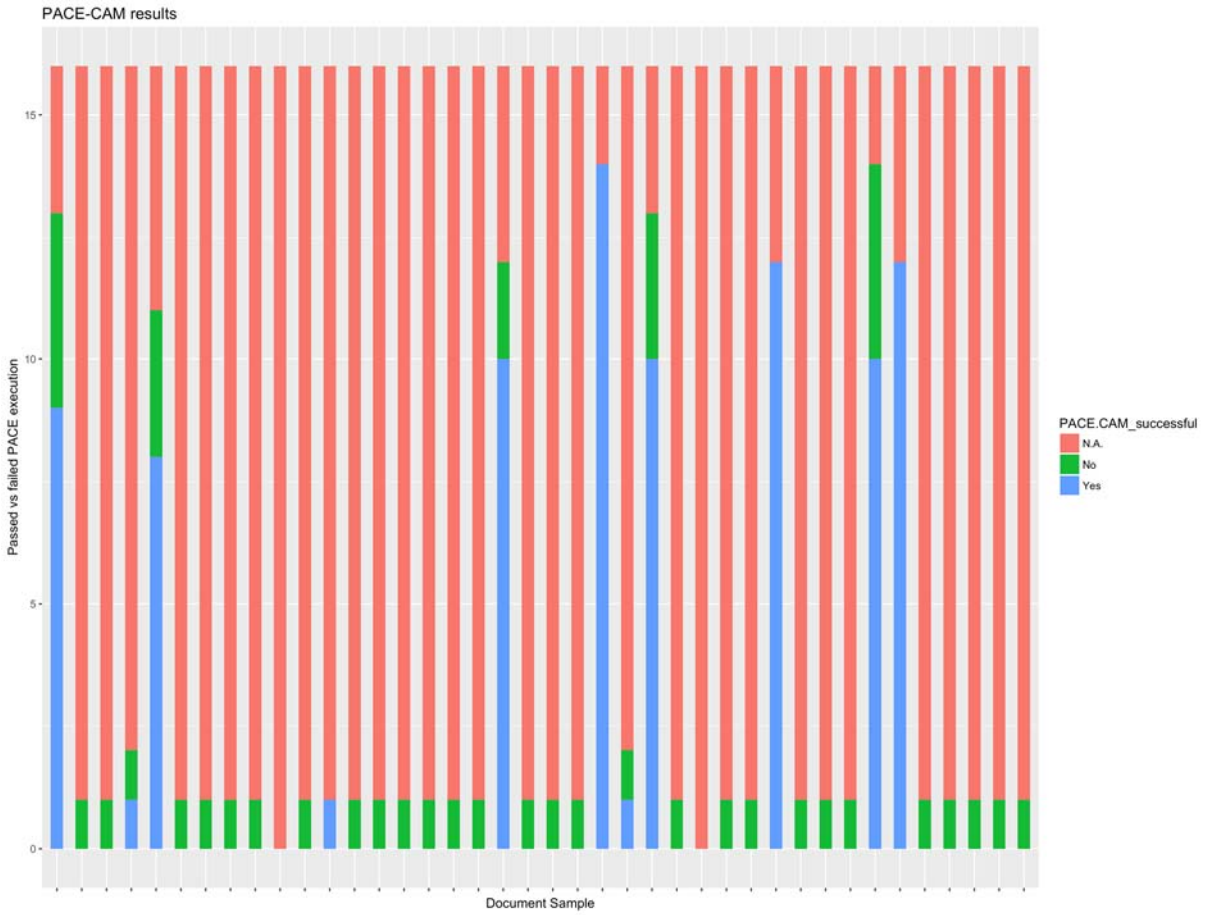

Figure 35: Results of PACE-CAM execution by document

The diagram in Figure 35 shows a stacked bar plot indicating the number of "yes", "No" and "NA" as results of the PACE-CAM algorithm execution as reported by the test stations. The documents on the x-axis are given in the same order as in Figure 26. No document is reported as successfully executing PACE-CAM by all test stations, but indeed there are documents which are reported as successfully executing PACE-CAM by some test stations, so it seems there is no agreement between test stations as to whether a particular document executes successfully or not PACE-CAM. In order to explain this behaviour further investigation with the test station (document inspection system producer) is needed in order to understand whether this is due to wrong reporting or issue with the document inspection system software. In this case, a smoke test of the document inspection systems software would probably provide useful information for a more in depth analysis.

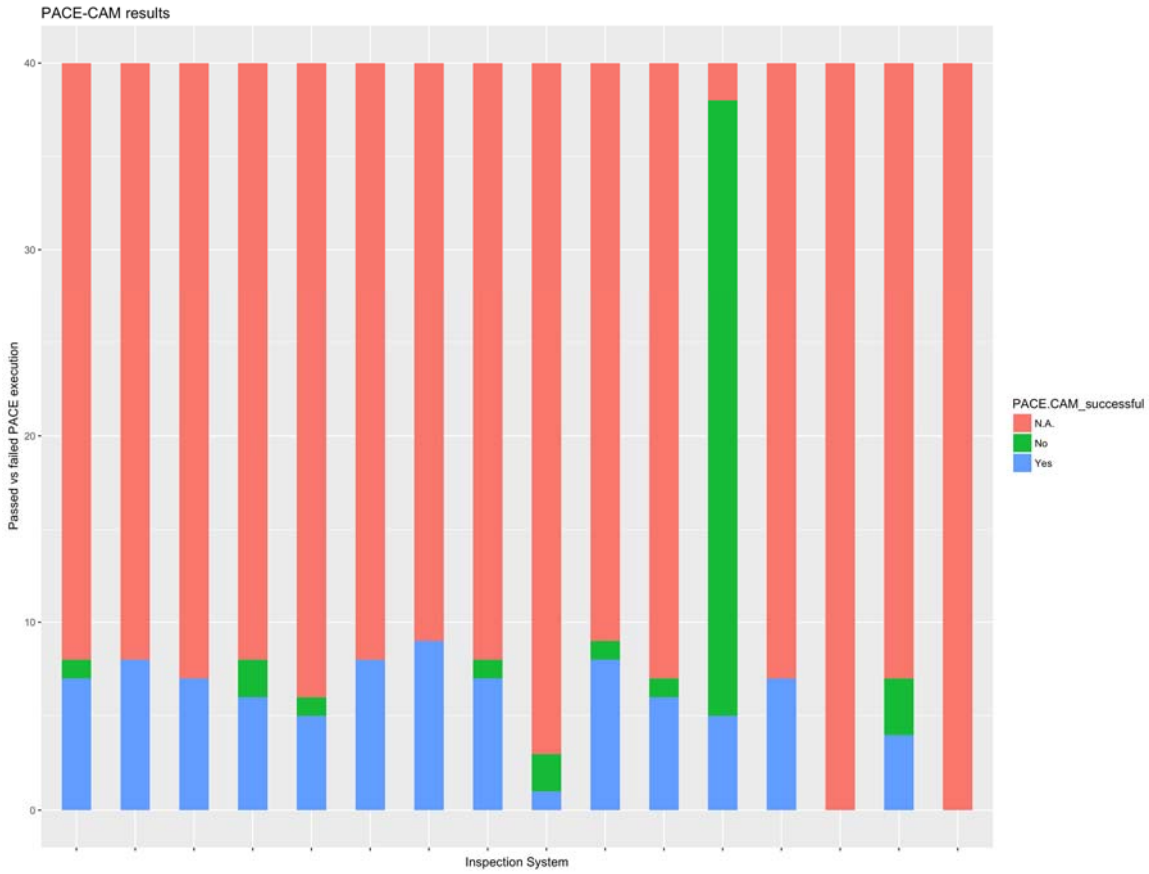

Figure 36: Results of PACE-CAM execution by inspection system

The diagram in Figure 36 provides another view of the results of PACE-CAM execution and shows a stacked bar plot indicating the number of "yes", "No" and "NA" as results of the PACE-CAM algorithm execution reported by the test stations. The test stations on the x-axis are given in the same order as in Figure 27.

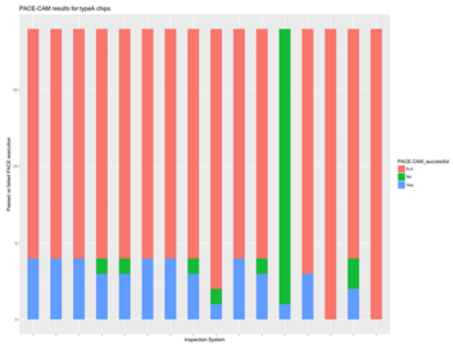

Figure 37: Results of PACE-CAM execution by inspection system (type A chips)

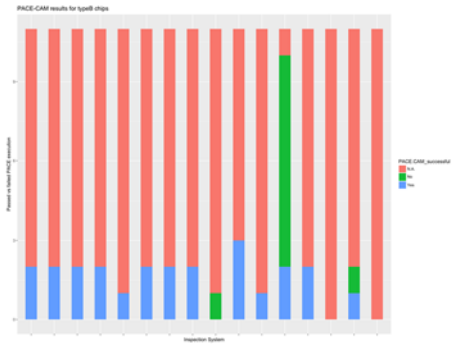

Figure 38: Results of PACE-CAM execution by inspection system (type B chips)

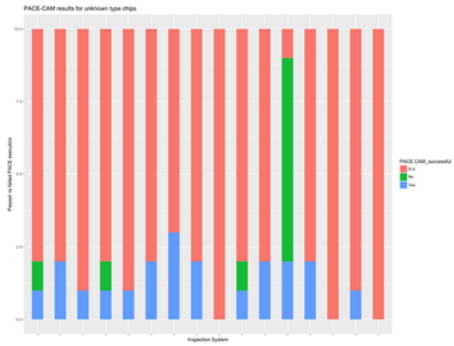

Figure 39: Results of PACE-CAM execution by inspection system (unspecified chip types)

Figure 37, Figure 38 and Figure 39 show the same information as in Figure 36 but partitioned by chip type.

3.9.2.3 Terminal Authentication execution

Looking at the results reported for the execution of EAC (execution of TA is considered here as the protocol representative for EAC, since CA can be implemented without TA being implemented thus not allowing the complete execution of the extended access control protocol), we see that:

- **TA** is reported as **executed** and **successful 413 times**
- **TA** is reported as **executed** and **not successful 48 times**
- **TA** is reported as **not executed** and **successful 7 times**
- **TA** is reported as **not executed** and **not successful 22 times**
- **TA** is reported as **executed** with **unknown (N.A.) result 147 times**
- **TA** is reported as **not executed** with **unknown (N.A.) result 147 times**

In red, the cases where the report is not consistent with the process described in section 2.4.2.

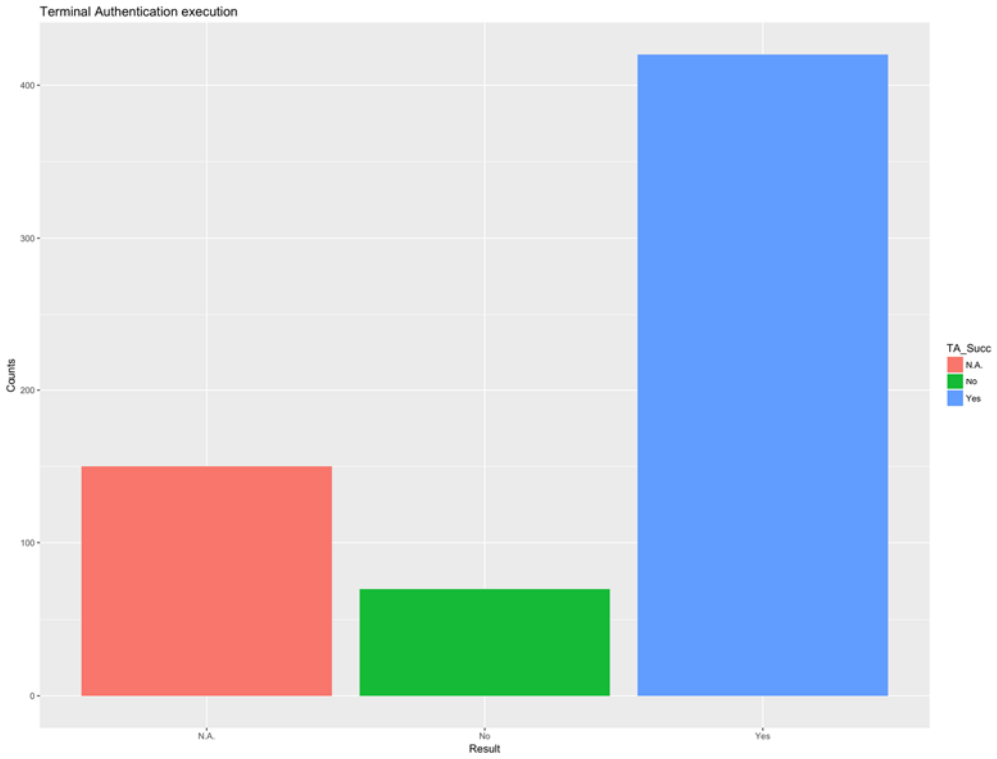

Figure 40: Successful execution of Terminal Authentication (TA)

The diagram in Figure 40 shows the results of the Terminal Authentication execution.

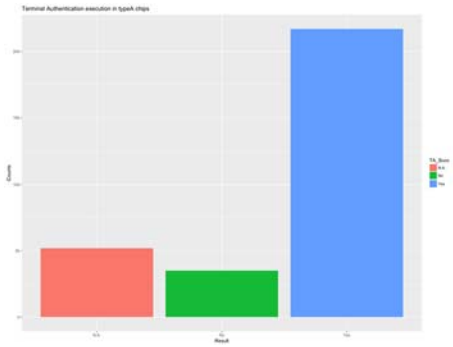

Figure 41: Successful execution of Terminal Authentication (TA) (type A chips)

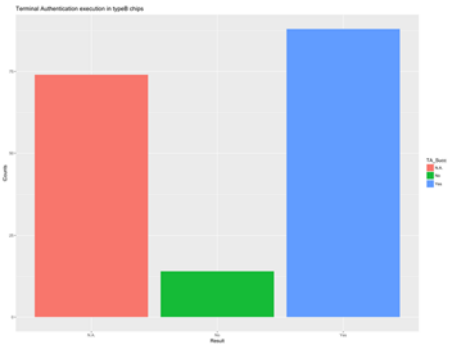

Figure 42: Successful execution of Terminal Authentication (TA) (type B chips)

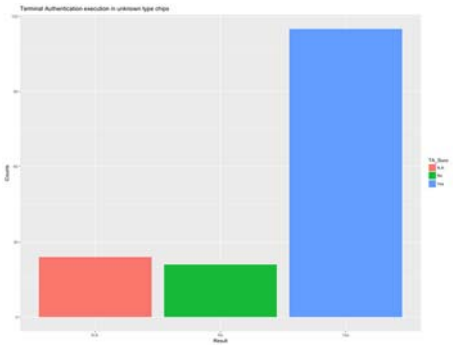

Figure 43: Successful execution of Terminal Authentication (TA) (unknown chip type)

As for the previous sections, Figure 41, Figure 42 and Figure 43, show the same information as Figure 40 but partitioned by chip type. Again no major difference can be observed in the reports for different chip types.

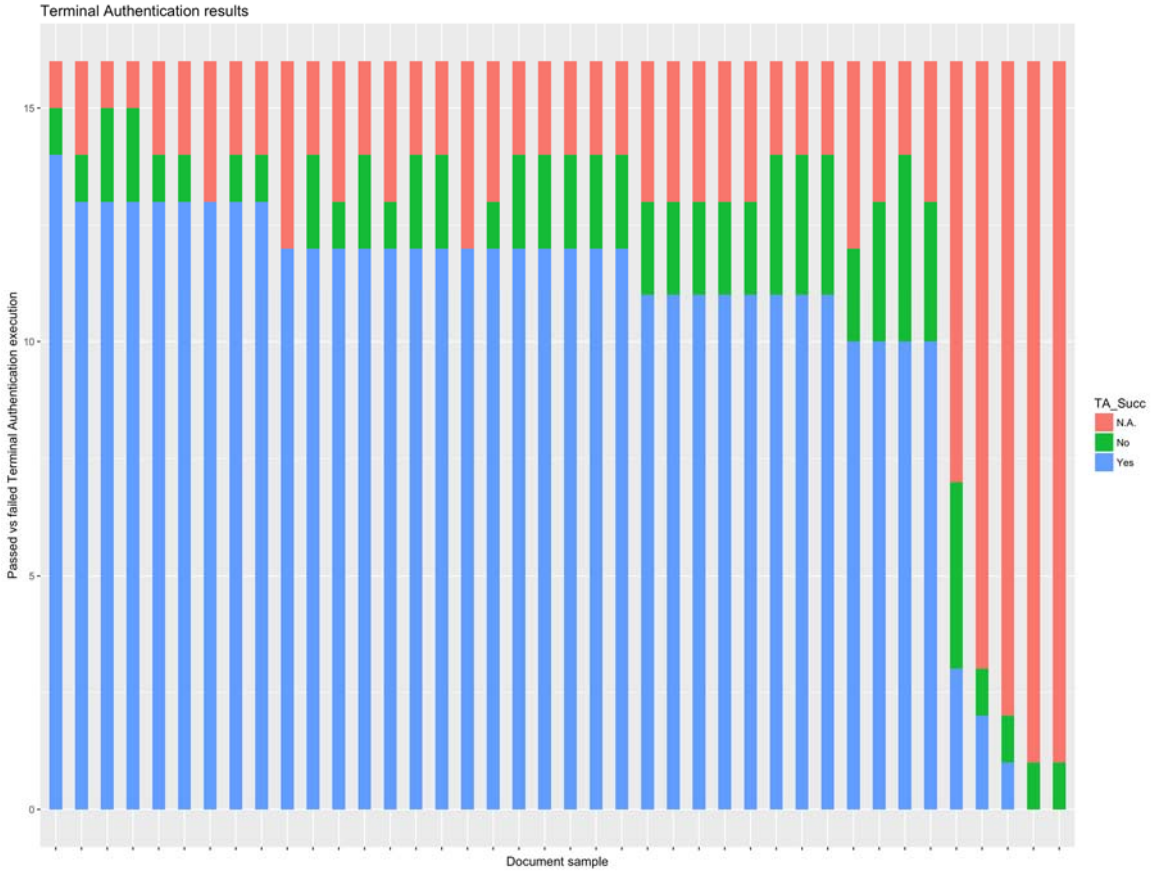

Figure 44: Results of Terminal Authentication execution by document

The diagram in Figure 44 shows a stacked bar plot indicating the number of "yes", "No" and "NA" as results of the TA algorithm execution as reported by the test stations. The diagram is ordered by decreasing number of "yes". No document is reported as successfully executing TA by all test stations, but this may be due to the fact that some of the inspection systems participating to the test might not implement extended access control at all. In addition, in this case, if a smoke test of the document inspection systems software had been executed prior to starting the crossover test, we would be able to provide more insight into the issue.

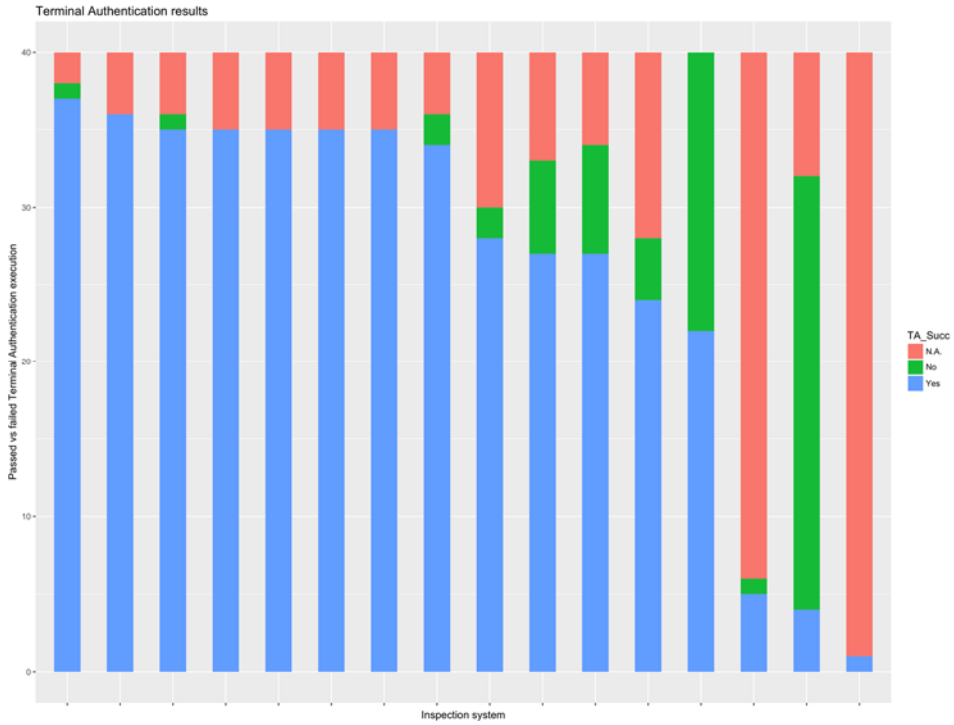

Figure 45: Results of Terminal Authentication execution by inspection system

The diagram in Figure 45 shows a stacked bar plot indicating the number of "yes", "No" and "NA" as results of the TA algorithm execution reported by the test stations. The diagram is ordered by decreasing number of "Yes". The fact that there is no test station which reported successful execution of TA on all documents is normal as not all documents implemented extended access control. However, the fact that one test station does not report any "not available" seems to indicate that this test station has reported absence of EAC as failed Terminal Authentication. Another interesting observation about this diagram is that all test station report at least one successful TA execution which would contradict the hypothesis that some inspection systems in the test do not implement EAC. This might be due to human error in compiling the report and again smoke test execution on the inspection systems software would have helped interpreting these results.

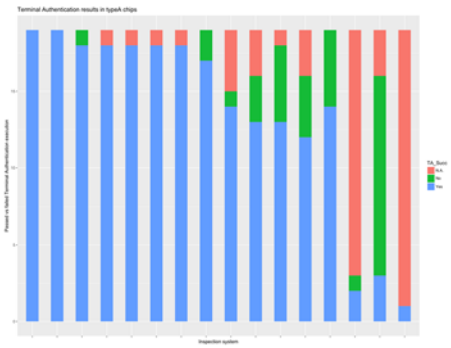

Figure 46: Results of TA execution by inspection system (type A chips)

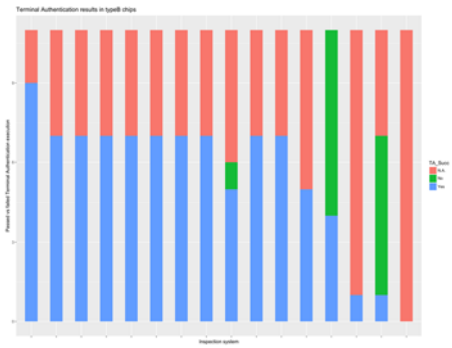

Figure 47: Results of TA execution by inspection system (type B chips)

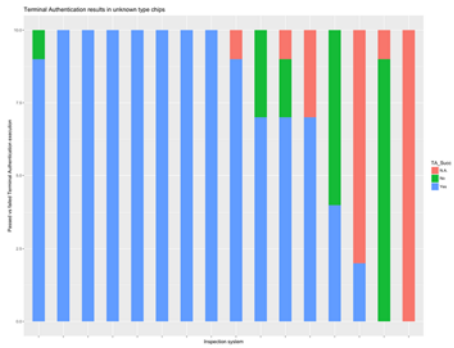

Figure 48: Results of TA execution by inspection system (unknown chip type)

As for the previous sections, Figure 46, Figure 47 and Figure 48, show the same information as Figure 45 but partitioned by chip type.

3.9.2.4 EF.ATR/INFO decoding

The EF.ATR/INFO can be used by the chip to store information about properties of the chip that can be useful for the inspection system. For example, information about support for extended length and buffer size can be provided here. An inspection system which can read and interpret correctly the information contained in this field is able to use, for example, an optimal buffer size for transferring data.

Looking at the results reported for the decoding of the EF.ATR/INFO field, we see that:

- ATR.INFO was reported as decoded correctly 187 times
- ATR.INFO was reported as not decoded correctly 10 times
- ATR.INFO was reported as not present 443 times

The data in the last row appears to be inconsistent with the data about support for the EF.ATR/INFO field as it was examined during the smoke test and reported in Annex B.

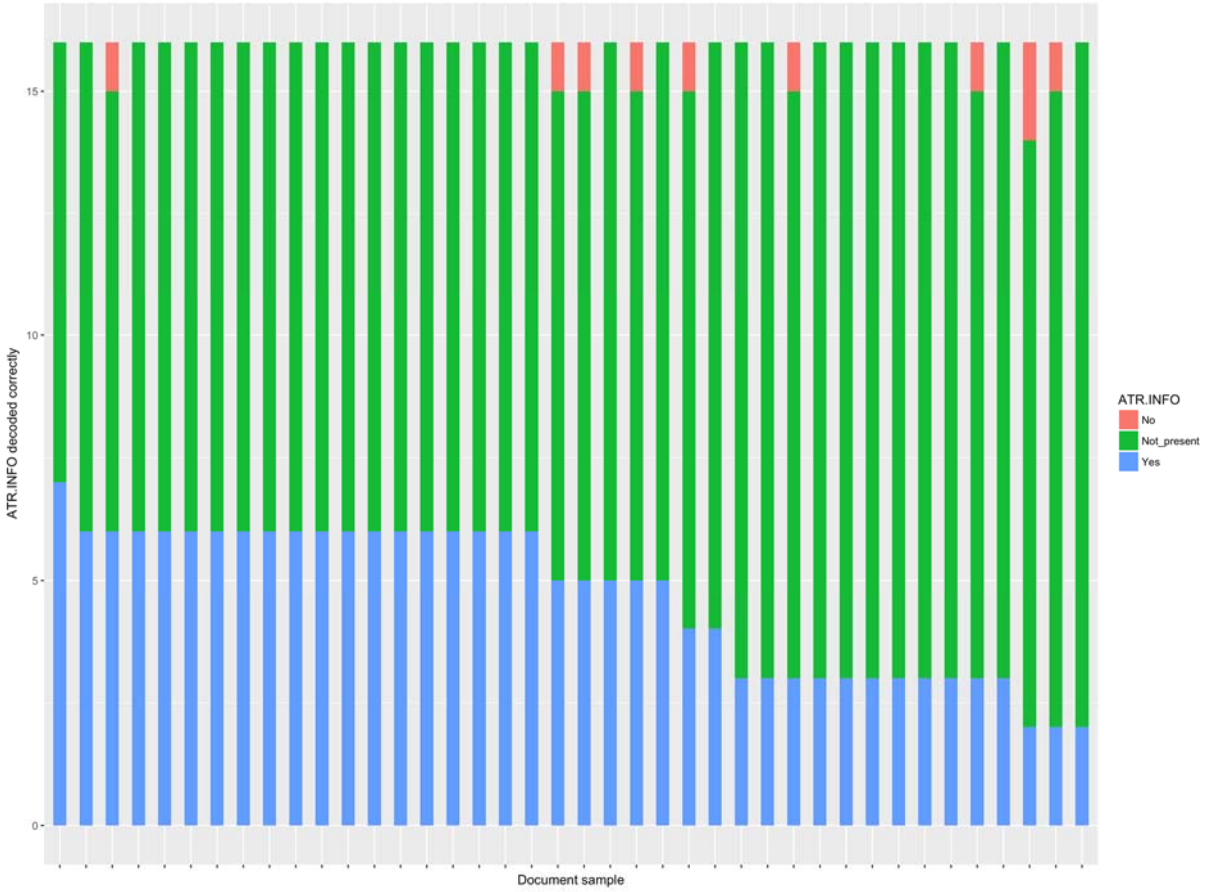

Figure 49: EF.ATR/INFO decoded correctly by the inspection system

The diagram in Figure 49 shows a stacked bar plot indicating the number successful decoding of the EF.ATR/INFO fields in the chip. The diagram is ordered by decreasing number of "yes".

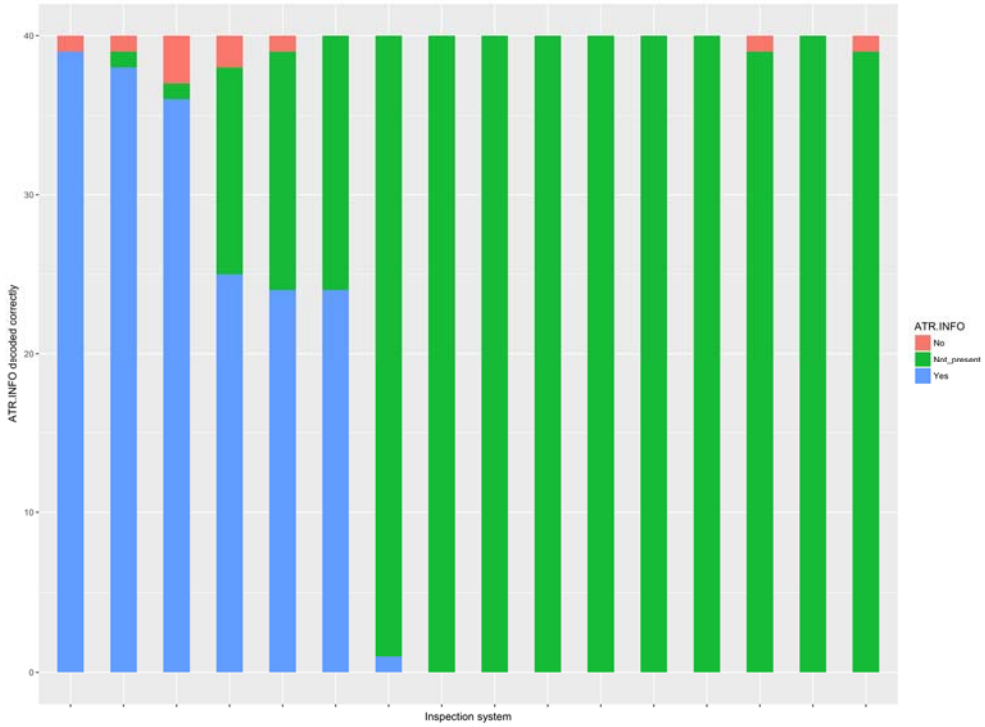

Figure 50: EF.ATR/INFO decoded correctly by the inspection system

The diagram in Figure 50 shows a stacked bar plot providing an overview of the results regarding the correct decoding of the EF.ATR/INFO field by the test stations. The diagram is ordered by decreasing number of "Yes".

3.9.2.5 Support for mandatory data groups

The following questions on the test report form are considered as related to mandatory data groups:

1. if the match of the scanned MRZ and the MRZ contained in DG1 was executed and in case it was if the result was successful
2. if DG2 was present and in case it was if its content was displayed correctly
3. if DG3 was present and in case it was if its content was displayed correctly

The results reported for the questions above are the following:

Question1:

In 480 cases, the comparison was done and was successful

In 160 cases, the comparison was not done. The reason was provided only in a few of these cases and in all cases where it was provided it was **InspectionSystem.notSupported**.

Question 2:

In 604 cases, DG2 was displayed successfully

In 36 cases, an error was reported. Some examples of the reasons for failure, which were reported, are:

- Biometric.template.error.ISO/IEC.7816.Part11.Profile

- Image.error.blankImage
- Could not decode image
- Biometric.content.error.ISO/IEC.19794.Part5.Profile (Image data type not indicated by the image data itself)
- Biometric.template.error.ISO/IEC.7816.Part11.Profile (Biometric type is encoded in three bytes instead of one)
- EF.DG.error.ICAOProfile (Object with tag 84 personalized)

Question 3:

In 373 cases, DG3 was displayed successfully

In 144 cases, DG3 was reported as "Not present"

In 123 cases DG3 was reported as not displayed successfully

3.9.2.6 Support for optional data groups

Replies to the questions related to support for optional data groups indicated that not all inspection system support (decode and display) optional data groups.

3.9.3 Crossover tests considerations and recommendations

A preliminary evaluation provided at the end of the event indicated that the behaviour and quality of both documents and readers with the PACE protocol had improved considerably from 2014 (Madrid, ICAO Interop test [35]).

All document verification systems implemented the reading procedure according to the ICAO rule:

- PACE first and BAC only as a fall-back solution

However, some test stations read the documents twice using both access control mechanisms (PACE and BAC) in order to provide a report for BAC execution as well. This was communicated to the experts' team by some test stations.

A more in-depth analysis of the results reported by the test stations, which was possible only after the event, shows that there are some inconsistencies in the results which can only be explained by assuming that in some cases the reporting was not without human error.

While there exist specifications for conformity testing for inspection systems [30][31], conformity test of inspection systems has not been considered in any of the interoperability test events so far, including this one. Conformity testing for inspection systems would provide more information and objective results about the current status of the implementation of the specifications and therefore give more precise indications on interoperability between readers and documents.

However, even without considering the option to test inspection systems for conformity, better results from crossover tests could be obtained by improving the reporting in such a way that it is more consistent among the different test stations.

In order to improve test results for crossover testing, the following is recommended:

- To execute a smoke test for inspection systems before the crossover test starts. Cards with "certified" implementation of the specifications should be used, but

also with situation with "macroscopic" defects could be evaluated as well (for instance related to certificates or CRL processing)

- To give a detailed presentation to test stations on how the test reporting tool should be used, allowing also enough time for a Q&A session
- To provide an online test-reporting tool which guides the reporting in such a way that the possibility of introducing human errors is minimised.
- To allow for a results discussion session after the preliminary evaluation of the results or by organising a follow-up event to discuss the results.

4 FINAL CONSIDERATIONS AND RECOMMENDATIONS

4.1 Organisation of the event

All the replies received with the questionnaire circulated after the event indicated that participants were happy with the organisation of the event and with the information they had received before the event. However, there are a few points where the organisation of an interoperability event can be improved.

First of all, there is the issue that document providers, once they have handed over their documents at the registration desk, have no active part in the test process and therefore it is necessary to provide for alternative activities for them. In this event document producers were offered the possibility to visit the JRC visitors centre and some of the cybersecurity laboratories, while in the second day they could participate to the conference.

On the other hand, document verification systems producers and test laboratories did not have the possibility to take part in the conference since they were busy with the tests.

Another aspect to be considered is that, once the test is completed, while a preliminary processing of the results gives the possibility to present the outcome at the conference, additional time should be allocated after the conference for a more in depth examination and discussion of the results bilaterally and in plenary with both the document verification systems and document producers.

4.2 Processing of the test data

Since the formats of the test results are defined prior to the test, it is possible to prepare in advance all the scripts, programs and databases that will be necessary to process the data and obtain the preliminary results. Such processing material should be shared, scrutinised and agreed by all the members of the organising/experts' team who are responsible for the delivery of the preliminary test reports to participants and for preparing the presentation of the results to be given at the end of the event.

4.3 Discussion of the results and follow-up

Either at the end of the test, after processing the test data, or in a separate follow-up event, it is important that results are discussed with the test laboratories in order to understand the reasons for inconsistencies in the results, if any, and between document producers and inspection systems producers to clarify the reasons for failures or incoherent behaviour in the inspection process.

4.4 Testing the inspection systems

The process followed during this and previous test events focused mainly on analysing whether implementations of the specifications in the document chips were correct. Conformity testing was limited to documents and did not include inspection systems. There was no check on the document verification systems that participated to the crossover test. For this reason, the results of the crossover tests should not be considered in absolute terms as there is no baseline against which they can be checked. In other words, there is no way to state whether an issue reported in a crossover test result is due to the implementation in the chip, in the inspection system application or due to human error in reporting.

4.5 Recommendations

As a lessons learned from the experience of this interoperability test event, in order to get the maximum benefit and useful information from these events, the following recommendations are made:

- Result report discrepancies were observed for some test cases, in order to address these kinds of issues, and understand the reasons, it is recommended that a follow-up session is held with the test laboratories in order to analyse the different results.
- Additional time for, possibly bilateral, discussions on the results should be available, after the tests have been completed and the preliminary results delivered.
- Smoke test should be done on inspection systems (document verification system) as well as on documents submitted for the test.
- At least half a day should be dedicated only to smoke testing. A sufficient number of test experts/engineers should be available depending the number of documents/document verification systems.
- Smoke test on the inspection systems should be done using a set of "reference" documents. The cross-over test protocol should be executed by the test experts/engineers during the smoke test using the "reference documents".
- Ideally, an online reporting system which guides the compilation of the test results for the testers should be provided. This would minimise the possibility of introducing human error.

In addition, the possibility to introduce conformity testing for inspection systems should be analysed and considered for future test events. Tests specifications for inspection systems are available and have been published by ICAO [30] and BSI [31], although the implementation and execution of the test cases would require a test setting environment which is slightly more complex than the one required for conformity testing of the documents.

Annex A: Crossover test report form

Handling of certificates	Default value in red	Reason (drop-down menu list)
Successful CSCA certificate import	radio-box: Yes/ No	certificate.error.coding.ASN1 certificate.error.field certificate.error.extension certificate.error.publicKey certificate.error.signature certificate.isExpired certificate.isRevoked certificate.notAvailable
Successful CRL import	radio-box: Yes/ No	CRL.error.coding.ASN1 CRL.error.field CRL.error.extension CRL.error.signature CRL.notAvailable
Successful CVCA certificate import	radio-box: Yes/ No	cvc.error.coding.ASN1 cvc.error.field cvc.error.publicKey cvc.error.signature cvc.isExpired cvc.notAvailable
Successful DV certificate import	radio-box: Yes/ No	cvc.error.coding.ASN1 cvc.error.field cvc.error.publicKey cvc.error.signature cvc.isExpired cvc.notAvailable
Successful IS credentials import	radio-box: Yes/ No	credentials.notAvailable cvc.error.coding.ASN1 cvc.error.field cvc.error.publicKey cvc.error.signature cvc.isExpired cvc.notAvailable privateKey.error privateKey.error.coding.ASN1 privateKey.notAvailable

Authentication of data	Default value in red	Reason (drop-down menu list)
PA executed	radio-box: Yes/ No	
PA successful	radio-box: Yes/ No/ N.A.	APDU.ERROR.READ_BINARY.EF.SoD APDU.ERROR.SELECT.EF.SoD DocumentSignerCertificate.error.coding.ASN1 DocumentSignerCertificate.error.field DocumentSignerCertificate.error.extension DocumentSignerCertificate.error.publicKey DocumentSignerCertificate.error.signature DocumentSignerCertificate.isExpired DocumentSignerCertificate.isRevoked DocumentSignerCertificate.notFound DG.hash.notEqual.to.EF.SoD.hash EF.CardAccess.securityInfo(s).notFoundIn.EF.DG14 EF.SoD.error.coding.ASN1 EF.SoD.error.ICAOProfile EF.SoD.error.notFound EF.SoD.error.signedData EF.SoD.error.signedData.LDS_securityObject EF.SoD.error.signedData.signerInfo
		InspectionSystem.cryptographicModule.internalError ISO14443.error

Access to the contactless IC	Default value in red	Reason (drop-down menu list)
BAC executed	radio-box: Yes/ No	InspectionSystem.notSupported PACE.executed
BAC successful	radio-box: Yes/ No/ N.A.	APDU.ERROR.GET_CHALLENGE APDU.ERROR.EXTERNAL_AUTHENTICATE APDU.ERROR.SELECT_APPLICATION InspectionSystem.cryptographicModule.internalError ISO14443.error
PACE executed	radio-box: Yes/ No	BAC.executed document.notSupported/EF.CardAccess.notFound InspectionSystem.extendedLength.notSupported InspectionSystem.notSupported InspectionSystem.password.notAvailable PACEDomainParameterInfo.explicitDomainParameters.notSupported PACEInfo.domainParameter.notSupported PaceInfo.keyAgreementMethod.notSupported PaceInfo.MAC_algorithm.notSupported PaceInfo.mappingMethod.notSupported PaceInfo.PACE-CAM.notSupported PaceInfo.protocol.notSupported PaceInfo.symmetricCipher.notSupported
PACE successful	radio-box: Yes/ No/ N.A.	APDU.ERROR.GENERAL_AUTHENTICATE.encryptedNonce APDU.ERROR.GENERAL_AUTHENTICATE.keyAgreement APDU.ERROR.GENERAL_AUTHENTICATE.mappingNonce APDU.ERROR.GENERAL_AUTHENTICATE.mutualAuthentication APDU.ERROR.MANAGE_SECURITY_ENVIRONMENT.SET_AT APDU.ERROR.READ_BINARY.EF.CardAccess APDU.ERROR.READ_BINARY.EF.CardSecurity APDU.ERROR.SELECT.EF.CardAccess APDU.ERROR.SELECT.EF.CardSecurity APDU.ERROR.SELECT_APPLICATION ChipAuthenticationPublicKeyInfo.error EF.CardAccess.error.coding.ASN1 EF.CardAccess.error.ICAOProfile EF.CardSecurity.error.coding.ASN1 EF.CardSecurity.error.ICAOProfile IFD.publicKey.equalTo.IC.publicKey InspectionSystem.cryptographicModule.internalError ISO14443.error PACEDomainParameterInfo.error PaceInfo.error.field.version

Authentication to the contactless IC	Default value in red	Reason (drop-down menu list)
Active Authentication executed	radio-box: Yes/ No	ActiveAuthentication.publicKey.notSupported document.notSupported/EF.DG15.notFound document.extendedLength.notSupported/EF.ATR.INFO.notDeclared InspectionSystem.extendedLength.notSupported InspectionSystem.notSupported signature.algorithm.notSupported
Active Authentication successful	radio-box: Yes/ No/ N.A.	ActiveAuthentication.error.publicKey ActiveAuthentication.error.signature ActiveAuthenticationInfo.error APDU.ERROR.INTERNAL_AUTHENTICATE APDU.ERROR.READ_BINARY.EF.DG14 APDU.ERROR.READ_BINARY.EF.DG15 APDU.ERROR.SELECT.EF.DG14 APDU.ERROR.SELECT.EF.DG15 EF.DG14.error.coding.ASN1 EF.DG14.error.ICAOProfile EF.DG14.error.notFound EF.DG15.error.coding.ASN1 EF.DG15.error.ICAOProfile InspectionSystem.cryptographicModule.internalError ISO14443.error
Chip Authentication executed	radio-box: Yes/ No	ChipAuthenticationInfo.keyAgreementMethod.notSupported ChipAuthenticationInfo.MAC_algorithm.notSupported ChipAuthenticationInfo.protocol.notSupported ChipAuthentication.publicKey.notSupported ChipAuthenticationInfo.symmetricCipher.notSupported document.notSupported/EF.DG14.notFound document.notSupported/EF.DG14.ChipAuthenticationInfo/ChipAuthenticationPublicKeyInfo.notFound inspectionSystem.notSupported inspectionSystem.PACE-CAM.executed

Chip Authentication successful	radio-box: Yes/ No/ N.A.	APDU.ERROR.GENERAL_AUTHENTICATE.Key_Agreement.static APDU.ERROR.MANAGE_SECURITY_ENVIRONMENT.SET_AT APDU.ERROR.MANAGE_SECURITY_ENVIRONMENT.SET_KAT APDU.ERROR.READ_BINARY.EF.DG14 APDU.ERROR.SELECT.EF.DG14 ChipAuthenticationInfo.error.field.version ChipAuthenticationPublicKeyInfo.error EF.DG14.error.coding.ASN1 EF.DG14.error.ICAOProfile InspectionSystem.cryptographicModule.internalError ISO14443.error
PACE-CAM executed	radio-box: Yes/ No	document.notSupported/EF.CardAccess.notFound document.notSupported/EF.CardAccess.securityInfo.PACE-CAM.notFound InspectionSystem.BAC.executed InspectionSystem.ChipAuthentication.executed InspectionSystem.notSupported InspectionSystem.password.notAvailable PACEDomainParameterInfo.explicitDomainParameters.notSupported PaceInfo.domainParameter.notSupported.EC PaceInfo.keyAgreementMethod.notSupported.ECKA PaceInfo.MAC_algorithm.notSupported.CMAC PaceInfo.protocol.notSupported.PACE_CAM PaceInfo.symmetricCipher.notSupported.AES
PACE-CAM successful	radio-box: Yes/No/ N.A.	APDU.ERROR.GENERAL_AUTHENTICATE.encryptedNonce APDU.ERROR.GENERAL_AUTHENTICATE.keyAgreement APDU.ERROR.GENERAL_AUTHENTICATE.mappingNonce APDU.ERROR.GENERAL_AUTHENTICATE.mutualAuthentication APDU.ERROR.MANAGE_SECURITY_ENVIRONMENT.SET_AT APDU.ERROR.READ_BINARY.EF.CardAccess APDU.ERROR.READ_BINARY.EF.CardSecurity APDU.ERROR.SELECT.EF.CardAccess APDU.ERROR.SELECT.EF.CardSecurity APDU.ERROR.SELECT_APPLICATION ChipAuthenticationPublicKeyInfo.error EF.CardAccess.error.coding.ASN1 EF.CardAccess.error.ICAOProfile EF.CardSecurity.error.coding.ASN1 EF.CardSecurity.error.ICAOProfile IFD.publicKey.equalTo.IC.publicKey InspectionSystem.cryptographicModule.internalError ISO14443.error PACEDomainParameterInfo.error PaceInfo.error.field.version

Authentication of the Terminal	Default value in red	Reason (drop-down menu list)
Terminal Authentication executed	radio-box: Yes/ No	cvc.publicKey.notSupported document.notSupported/EF.DG14.notFound document.notSupported/EF.DG14.terminalAuthenticationSecurityInfo.notFound InspectionSystem.cryptographicMaterial.notAvailable InspectionSystem.notSupported
Terminal Authentication successful	radio-box: Yes/ No/ N.A.	APDU.ERROR.EXTERNAL_AUTHENTICATE APDU.ERROR.GET_CHALLENGE APDU.ERROR.MANAGE_SECURITY_ENVIRONMENT.SET_AT APDU.ERROR.MANAGE_SECURITY_ENVIRONMENT.SET_DST APDU.ERROR.PERFORM_SECURITY_OPERATION APDU.ERROR.READ_BINARY.EF.CVCA APDU.ERROR.READ_BINARY.EF.DG14 APDU.ERROR.SELECT.EF.CVCA APDU.ERROR.SELECT.EF.DG14 cvc.chain.error cvc.error.publicKey EF.CVCA.error.BSIProfile EF.CVCA.error.coding.ASN1 EF.CVCA.error.notFound EF.DG14.error.coding.ASN1 EF.DG14.error.ICAOProfile InspectionSystem.cryptographicModule.internalError ISO14443.error TerminalAuthenticationSecurityInfo.error

Optical check	Default value in red	Reason (drop-down menu list)
Comparison of conventional MRZ (OCR-B) and IC-based MRZ (LDS)	radio-box: Yes/ No	comparison.error InspectionSystem.cannotRead.MRZ InspectionSystem.notSupported ISO14443.error

Biometric pictures	Default value in red	Reason (drop-down menu list)
DG2 facial image displayed correctly	radio-box: Yes/ No	APDU.ERROR.READ_BINARY APDU.ERROR.SELECT Biometric.content.error.ISO/IEC.19794.Part5.Profile Biometric.template.error.ISO/IEC.7816.Part11.Profile EF.DG.error.coding.ASN1 EF.DG.error.ICAOProfile Image.error.blankImage ISO14443.error notPresent
DG3 fingerpring image(s) displayed correctly	radio-box: Yes/ No/ Not present	APDU.ERROR.READ_BINARY APDU.ERROR.SELECT Biometric.content.error.ISO/IEC.19794.Part4.Profile Biometric.template.error.ISO/IEC.7816.Part11.Profile EF.DG.error.coding.ASN1 EF.DG.error.ICAOProfile Image.error.blankImage ISO14443.error TerminalAuthentication.notExecuted
DG4 Eye image(s) displayed correctly	radio-box: Yes/ No/ Not present	APDU.ERROR.READ_BINARY APDU.ERROR.SELECT Biometric.content.error.ISO/IEC.19794.Part6.Profile Biometric.template.error.ISO/IEC.7816.Part11.Profile EF.DG.error.coding.ASN1 EF.DG.error.ICAOProfile
		Image.error.blankImage ISO14443.error TerminalAuthentication.notExecuted

Data groups	Default value in red	Reason (drop-down menu list)
DG5 portrait displayed correctly	radio-box: Yes/ No/ Not present	APDU.ERROR.READ_BINARY APDU.ERROR.SELECT EF.DG.error.coding.ASN1 EF.DG.error.ICAOProfile Image.error.blankImage Image.error.type.unknown ISO14443.error
DG7 signature or usual mark displayed correctly	radio-box: Yes /No/ Not present	APDU.ERROR.READ_BINARY APDU.ERROR.SELECT EF.DG.error.coding.ASN1 EF.DG.error.ICAOProfile Image.error.type.unknown Image.error.blankImage ISO14443.error
DG11 additional personal details decoded correctly	radio-box: Yes /No/ Not present	APDU.ERROR.READ_BINARY APDU.ERROR.SELECT EF.DG.error.coding.ASN1 EF.DG.error.ICAOProfile Image.error.type.unknown Image.error.blankImage ISO14443.error
DG12 additional document details	radio-box: Yes /No/ Not present	APDU.ERROR.READ_BINARY APDU.ERROR.SELECT EF.DG.error.coding.ASN1 EF.DG.error.ICAOProfile Image.error.type.unknown Image.error.blankImage ISO14443.error
DG16 person to notify decoded correctly	radio-box: Yes /No/ Not present	APDU.ERROR.READ_BINARY APDU.ERROR.SELECT EF.DG.error.coding.ASN1 EF.DG.error.ICAOProfile ISO14443.error

Elementary files	Default value in red	Reason (drop-down menu list)
EF.ATRinfo decoded correctly	radio-box: Yes/ No/ Not present	APDU.ERROR.READ_BINARY APDU.ERROR.SELECT error.coding.ASN1 field.error.cardServiceData field.error.cardCapabilities field.error.extendedLengthInformation field.error.initialAccessDataField ISO14443.error
EF.COM decoded correctly	radio-box: Yes/ No	APDU.ERROR.READ_BINARY APDU.ERROR.SELECT EF.DG.error.coding.ASN1 EF.DG.error.ICAOProfile ISO14443.error notPresent

Annex B. Smoke Test: Analysis of the results

This section reports about the results of the smoke tests.

Charts in this part of the technical report were generated using R, a free software environment for statistical computing and graphics.

In the sections that follow, the term "Official documents" has been used to indicate documents that were submitted to the test by countries, however this must not be considered as an indication that the document submitted is indeed a sample of any document actually in circulation. We have no indication regarding their status in this respect.

The term "Non-Official documents" has been used to indicate documents that were submitted to the test by industry.

The reason to differentiate between these two sets is that "Non-Official documents" may contain feature which can still be considered as experimental (such as, for instance, support for a wide range of algorithms for PACE).

In the diagram in Figure 51, however, we provide an overview of the type of documents that were submitted to the test, showing the distribution of passports vs. eRPs and EAC vs non-EAC documents.

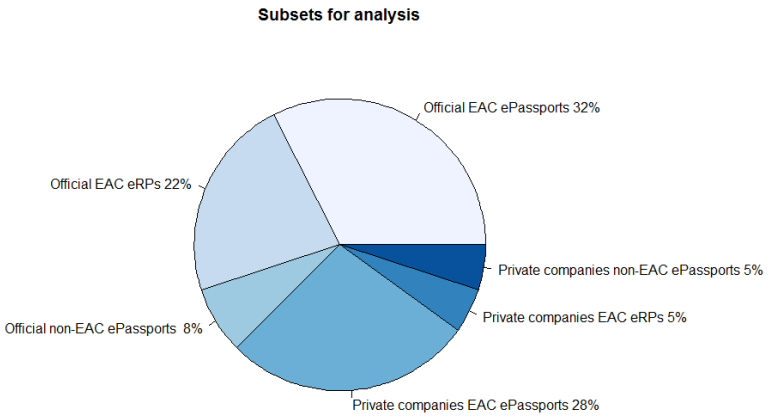

Figure 51. Subsets for documents submitted to the test.

B.1 Analysis criteria

For each subset, we provide an analysis for the following features:

- Smoke test phase inspection time and amount of data exchanged between the eMRTD and the terminal;
- ISO Application-independent cards services that eMRTDs must respect because they must be compliant with ISO 7816/4 [11] and that , properly used, speed-up the inspection process;
- ICAO features:
    - LDS versions;
    - DGs presence;
    - ICAO Passive Authentication: CSCA and CDS signature and public key algorithms;
    - ICAO PACE protocol:
        - Mapping types;
        - Key exchange mechanisms and Domain Parameters;
        - Algorithms.
    - ICAO Active Authentication: signature and public key algorithms;
    - ICAO-BSI TR03110 Chip Authentication:
        - Key exchange mechanisms and Domain Parameters;
        - Algorithms.
    - BSI TR03110 Terminal Authentication: signature and public key algorithms;
    - ISO 7816-4 Secure Messaging.

B.2 Performance

The following table shows the result of the inspection performance during the Smoke Test.

The average eMRTD had an inspection time of ≈10 s and the terminal needed to send ≈1.8 Kb and needed to fetch ≈36.9 Kb.

The bitrate selected by two of the PCSC readers used in the smoke test is unknown, so the summary presented here does not take into account differences among the PCSC readers, if there were any.

For the Inspection time, we also list the median because one of the official documents supported only a small bitrate with a slow cryptographic protocol (DH).

Average total data sent by terminal (bytes)	Average total data sent by eMRTD (bytes)	Inspection time average (s)	Inspection time median (s)
1.877	37.767	10.06	9.63

Table 3: Smoke Test performance with amount of data exchanged

B.3 ISO Application-independent card services.

The purpose of card services is to provide interchange mechanisms between a card and an interface device knowing nothing about each other except that they both comply with ISO 7816/4 [11].

For a PICC using the RF physical interface, card services result from the combination of the contents of ATS, EF.ATR/INFO and EF.DIR.

The ATS information was lost due to the use of a PCSC reader for the Smoke Test phase, so the data presented could be distorted to the missing information from the ATS.

Statistics have been generated for the following features:

- EF.ATR/INFO presence;
- EF.DIR presence;
- Card Capabilities: Extended Length Fields support;
- Card Capabilities: Extended Length Information;
- Card Capabilities: Short File Identifier (SFI) support;
- Card Capabilities: Command chaining support.

B.3.1 EF.ATR/INFO

This optional EF indicates operating characteristics of the card, mainly:

- Card capabilities and
- Other characteristics (e.g. the Application Family Identifier) which usually are not used by eMRTDs and are not considered in this TR.

The table below shows the presence of EF.ATR/INFO in the documents submitted to the test.

Only 60% of the documents had EF.ATR/INFO personalized.

B.3.2 EF.DIR

This optional EF indicates a list of applications supported by the card.

No model presented to the Interoperability test had EF.DIR personalized, which is consistent with a single application product as the eMRTD.

B.3.3 Card capabilities: Extended length support.

By default, an ICC compliant with ISO 7816/4 [11] handles only short length fields (L_c and L_e):

- The L_c field codes the number of bytes in the command data field.
- The L_e field codes the maximum number of bytes expected in the response data field.

A short L_c field has a range from one to 255 bytes.

A short L_e field has a range from one to 256 bytes.

Depending on the size of the cryptographic objects (e.g. public keys, signatures) a terminal must use APDUs with extended length fields to send data to the eMRTD chip. E.g., a terminal selecting a PACE protocol using Diffie-Hellman PKCS3 key agreement with the group "2048-bit MODP with 256 prime order subgroup" would need to send an ephemeral public key of 256 bytes to the eMRTD and this would imply the use of an extended L_c field. Extended length fields are defined in ISO 7816/4 [11].

Depending of the size of the biometric data encoded in the eMRTD, a terminal could use APDUs with extended length field to recover the complete biometric data in one command or in fewer commands than using default short fields. Thus, the use of extended L_e fields speeds-up the inspection process.

An extended L_c field has a range from one to 65 535.

An extended L_e field has a range from one to 65 536.

If the card explicitly states its capability of handling extended L_c and L_e fields in the historical bytes (ATS) or in EF.ATR/INFO then the card handles short and extended length fields.

For eMRTD chips, support of extended length is conditional. If the cryptographic algorithms and key sizes selected by the issuing State require the use of extended length, the eMRTD chips shall support extended length.

In the context of eMRTDs, a terminal should examine whether or not support for extended length is indicated by the eMRTD. See ICAO 9303/10 [6].

Because the smoke test was executed using a PCSC reader, the ATS information was not recorded thus, we can only provide statistics for extended length fields support based on the inspection of EF.ATR/INFO.

About 58% of the models presented to the Interoperability Test declare support for extended length fields.

B.3.4 Card capabilities: Extended length information.

The Extended length information is the data object that codes the command and response APDU (C-APDU and R-APDU) size limitations. It can be present in EF.ATR/INFO and/or in the FMD of any application DF. Values specified in the application FMD only apply to that application, possibly superseding values specified in the EF.ATR/INFO.

According to ICAO 9303/10 [6], a terminal must not use extended length for APDUs other than the following commands unless the exact input and output buffer sizes of the eMRTD chip are explicitly stated.

- MSE:Set KAT;
- General Authenticate.

None of the samples received coded extended length information in the FMD of the ePassport application.

The table below shows how many models declare extended length information in EF.ATR/INFO and the values declared.

About 53% of the models presented to the Interoperability Test declared extended length information. For "Non-official documents", the percentage was 60%, which could be interpreted as a sign that industry is willing to offer models with more RAM to enhance the performance of the inspection process.

For the C-APDU buffer, about 19% of such models offered the maximum extended value and the rest offered an average buffer of ≈1.310 bytes. Such buffers are big enough given the typical size of the cryptographic objects in an eMRTD.

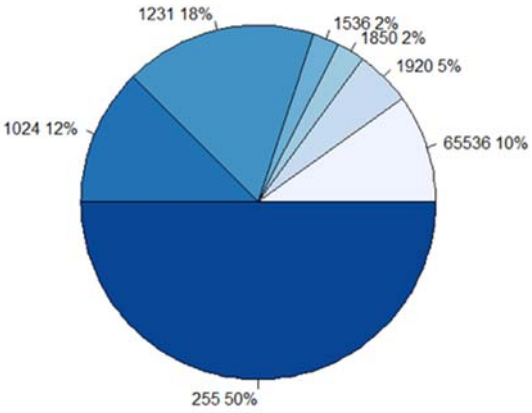

Figure 52. CAPDU buffer size.

CAPDU buffer size (bytes)	Samples	Extended length information present
65536	4	21/40 (52.5%)
1920	2	
1850	1	
1536	1	
1231	7	
1024	6	

Table 4. C-APDU buffer size declared in EF.ATR/INFO.

For the R-APDU buffer, a 50% of such models offered a value very close to the maximum extended value and the rest offered an average buffer of 1.555 bytes. Therefore, assuming a secure message established using 3DES, 50% of the samples can recover any biometric data using a single command, and the other 50% would need ≈ 13 commands to recover the content of a typical DG3 file. By contrast, models not declaring extended length information would need ≈ 81 commands to recover the content of a typical DG3 file.

RAPDU buffer size (bytes)	Samples	Extended length information present
65536	4	20/40 (50%)
65535	1	

65530	**1**	
65450	**4**	
1920	**2**	
1850	**1**	
1440	**2**	
1396	**5**	

Table 5. R-APDU buffer size declared in EF.ATR/INFO.

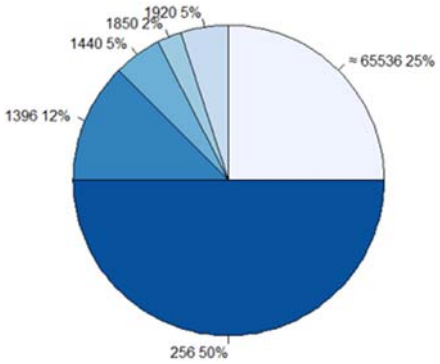

Figure 53. RAPDU buffer size.

B.3.5 Card capabilities: Short File Identifier support.

ISO 7816/4 [11] introduces the selection of an EF by short EF identifier (SFI). If supported, selection by short EF identifier shall be indicated:

- In the historical bytes or in EF.ATR/INFO;
- If a short EF identifier Data Object (DO), '88' is present in the CPs of an EF.

Thus, the eMRTD supports two structure selection methods that are file identifier and short EF identifier. According to ICAO 9303-10 [6] selection using SFI is required for the eMRTD.

Only about 58% of the models presented to the Interoperability Test declared SFI support in EF.ATR/INFO. Again, the data could be distorted because of the missing ATS information.

B.3.6 Card capabilities: Command chaining support.

Chaining procedures are used either to support payload fragmentation or for a process involving several consecutive C-RPs.

A command payload is data of arbitrary length to be sent to the card in order to be processed together. A payload is oversize if its length is larger than available in a data field; chaining is needed to transmit such a payload. Chaining of commands supports the transmission to the card of an oversize command payload. The payload is fragmented; each fragment is a command data field that complies with size limitations. If the card supports the mechanism, then it shall indicate it in the ATS historical bytes or in EF.ATR/INFO.

According to ICAO 9303-10 [6] command chaining must be used for the PACE General Authenticate command to link the sequence of commands to the execution of the protocol. Command chaining must not be used for other purposes unless clearly indicated by the eMRTD.

Only about 38% of the models presented to the Interoperability Test indicate support for command chaining. Again, the data could be distorted because of the missing ATS information.

B.4 ICAO Data Groups (DGs)

B.4.1 LDS versions

The table below shows the LDS versions for the documents received. 95% of the samples used v1.7, for official samples the value was 100%.

LDS version V1.7	LDS version V1.8
38/40 (95%)	2/40 (5%)

Table 6. LDS versions.

B.4.2 Mandatory DGs DG1 and DG2

All the models received implement the mandatory DGs. The average size for DG2 (facial image) was 14.6 Kb.

B.4.3 DG3 (Additional Identification Feature — Finger(s))

All the EAC models implemented DG3. Non-EAC models did not personalize DG3.

Most of the models (about 86%) coded two instances of fingerprints, about 9% of the models coded one single instance of fingerprints and two models (about 6%) coded zero instances of fingerprints i.e. the DG was filled with random data. The average size for DG3 was 20.3 Kb.

B.4.4 DG7 Displayed Signature or Usual Mark

Only about 18% of the models had this file personalized with an average size of 4.800 bytes.

One of the documents coded a Card Holder Portrait Image (Tag 0x5F40) instead of a Card Holder Hand Written Signature Image (Tag 0x5F43) and thus, it has not been taken into account in the statistics.

B.5 ICAO Passive Authentication

For the Passive authentication, we checked CSCA and CDS algorithms for signatures and public keys characteristics.

B.5.1 CSCA certificate

The table below shows the CSCA signature algorithms and the signature hash algorithms used in the documents submitted to the test.

CSCA duplicates have been removed and are not shown in this table i.e. when two or more models shared the same CSCA only one instance has been taken into account for the statistics presented in this section. In total, there were 25 different CSCAs submitted to the Interoperability Test, 17 of them belonging to the "Official documents" subset. One CSCA certificate was used in both subsets therefore, the numbers in the tables below does not simply add for the total sum.

The typical CSCA certificate uses RSA PKCS#1 v1.5 (56%) or ECDSA (36%) using SHA-256 (60%) or SHA-384 (32%) as hash algorithm.

For RSA signatures, this does not follow the ICAO recommendation: "It is RECOMMENDED that issuing States or organizations generate signatures according to RSASSA-PSS", ICAO 9303-12 [8], 4.4.1. Only 8% of the models used RSA SSA PSS.

None of the CSCA certificates submitted to the Interoperability Test used DSA or ECDSA with characteristic-two-field.

Two CSCAs still use the forbidden SHA-1 as the signature hash algorithm (see ICAO 9303-12 [8], 4.4.4.) This case is highlighted in red in the table below.

CSCA signature algorithm	
RSA PKCS#1 v1.5	14/25 (56%)
RSA SSA PSS	2/25 (8%)
ECDSA	9/25 (36%)

Table 7. CSCA signature algorithms.

CSCA signature hash algorithm	
SHA-384	8/25 (32%)
SHA-256	15/25 (60%)
SHA-1	2/25 (8%)

Table 8. CSCA signature hash algorithms.

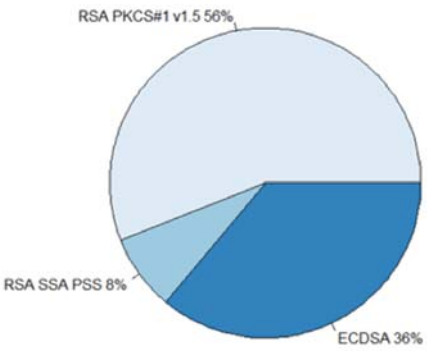

Figure 54. CSCA signature algorithm

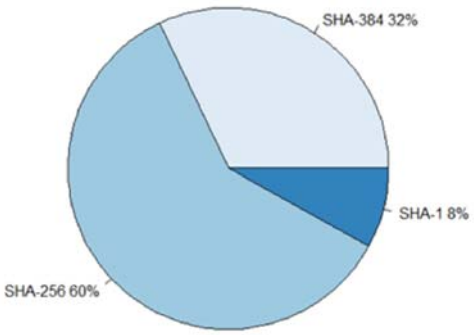

Figure 55. CSCA signature hash algorithm.

The table below shows the CSCA public key algorithm with their key lengths.

The typical CSCA uses a RSA public key (64%) with a key length of 4096 bits (about 63%).

One of the CSCAs submitted used as key RSA-1024 but this key length is not recommended by the cryptographic catalogues e.g. see NIST SP 800-57 Part 3 [12]. This case is highlighted in red in the table below.

CSCA public key algorithm		**CSCA public key length (bits)**	
RSA	16/25 (64%)	4096	10/16 (62.5%)
		3072	4/16 (25%)
		2048	1/16 (6.3%)
		1024	1/16 (6.3%)
EC	9/25 (36%)	384	5/9 (55.6%)
		256	4/9 (44.4%)

Table 9. CSCA public key algorithms and key lengths.

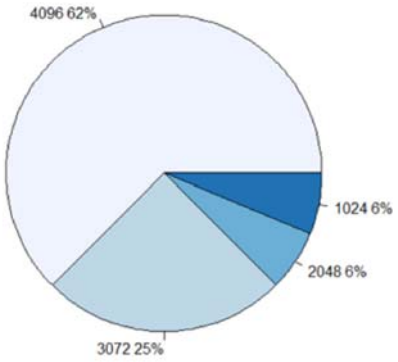

Figure 56. CSCA RSA public key length.

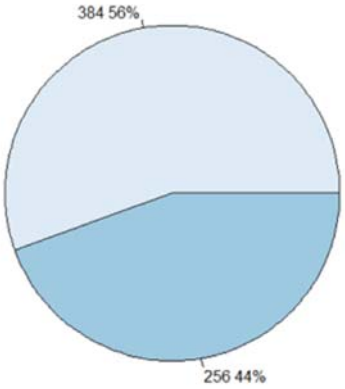

Figure 57. CSCA EC public key length.

Finally, for CSCA certificates, the table below shows the conformity against the latest ICAO profile defined in ICAO 9303-12 [8].

Only seven (28%) of the CSCA certificates were conformant to the latest ICAO profile (ICAO 9303 v7 Part 12 profiles). For "Non-official documents" CSCA certificates, only one of eight samples (about 13%) was conformant to the ICAO profile.

Non-conformity issues found:

Non-conformity	Occurrences
Extension: **Issuer Alternative name** is not present	11
Extension: **CRL distribution points** is not present	9
Extension: **Private key usage** is not present	9
Extension: **Subject alternative name** is not present	9
Extension: Subject alternative name Field: **Directory Name** is not present	6
Extension: **Issuer alternative name** is not present	5
Extension: Basic constraint Field: **Path length constraint** is not present	4
Extension: **Basic constraint** is not critical	3
Extension: **Key Usage** is not critical	3
Extension: Basic constraint Field: **Path length constraint** is different than zero	2
Field: Public key parameters. **Domain parameters** are not present	2
Field: **Issuer. Country name** is not upper case	1
Field: **Subject. Country name** is not upper case	1

Table 10. CSCA conformity to ICAO profile.

B.5.2 Document Signer certificate

The table below shows the CDS signature algorithm and the signature hash algorithm.

All the models submitted to the Interoperability Test had the CDS personalized in the SoD.

CDS duplicates were removed i.e. when two or more models shared the same CDS only one instance was taken into account. In total, there were 30 different CDSs submitted to the Interoperability Test, 22 of them belonging to the subset "Official documents". One CDS certificate was used in both subsets therefore, the numbers in the tables below does not simply add for the total sum.

The typical CDS uses RSA PKCS#1 v1.5 (about 53%) or ECDSA (about 37%) using SHA-256 (70%) as hash algorithm.

For RSA signatures, this does not follow the ICAO recommendation: "It is RECOMMENDED that issuing States or organizations generate signatures according to RSASSA-PSS", ICAO 9303-12 [8], 4.4.1. Only 10% of the models used RSA SSA PSS.

None of the models submitted to the Interoperability Test used DSA or ECDSA with characteristic-two-field for the CDS.

Three CDSs (10%) still use the forbidden SHA-1 as the signature hash algorithm, see ICAO 9303-12 [8], 4.4.4. This case is highlighted in red in the table below.

CDS signature algorithm	
RSA PKCS#1 v1.5	16/30 (53.3%)
RSA SSA PSS	3/30 (10%)
ECDSA	11/30 (36.7%)

Table 11. CDS signature algorithms.

CDS hash algorithm	
SHA-384	6/30 (20%)
SHA-256	21/30 (70%)
SHA-1	3/30 (10%)

Table 12. CDS hash algorithms.

The table below shows the CDS public key algorithm with their key lengths.

The typical CDS uses a RSA public key (about 68%) with a key length of 2048 bits (85%).

One of the samples submitted, belonging to the subset "Non-official documents", used as key RSA-1024 but this key length is not recommended by the cryptographic catalogues e.g. see NIST SP 800-57 Part 3 [12]. This case is highlighted in red in the table below.

CDS public key Algorithm		CDS public key length (bits)	
RSA	20/30 (67.7%)	3072	2/20 (10%)
		2048	17/20 (85%)
		1024	1/20 (5%)
EC	10/30 (33.3%)	384	1/10 (10%)
		256	8/10 (80%)
		224	1/10 (10%)

Table 13. CDS public key algorithms and key lengths.

Finally, for CDS certificates, the table below shows the conformity against the ICAO profile defined in ICAO 9303-12 [8].

Only 9 (40.9%) of the CDS certificates were conformant to the latest ICAO profile.

Non-conformity issues found in CDS certificates:

Non-conformity	Occurrences
Extension: **Document type** is not present	16
Extension: **Subject alternative name** is not present	15
Extension: **Issuer Alternative name** is not present	12
Extension: **CRL distribution points** is not present	11
Extension: **Private key usage** is not present	10
Extension: **Basic constraints** is present	5
Extension: Issuer alternative name Field: **Directory Name** is not present	5
Extension: Subject alternative name Field: **Directory Name** is not present	3
Field **Issuer.Country** name Does not match Subject.Country name	1
Extension: CRL distribution points Field: **URI is not present**	1
Field: Public key parameters. **Domain parameters** are not present	1
Field: **Issuer.Country name** is not upper case	1
Extension: **Subject directory** attributes is present	1

Table 14. CDS non-conformity to ICAO profile.

B.6 ICAO PACE

B.6.1 Mapping

The table below shows the PACE mapping type used by the documents submitted to the test.

About 98% of the documents supported PACE Generic Mapping, 10% supported PACE Integrated Mapping and about 7% supported PACE-CAM. Only one (2.5%) of the documents supported the three mapping types.

All the documents in the set "Official documents" supported PACE Generic Mapping, only one (about 8%) of the official models supported PACE Integrated Mapping and none of the official samples supported PACE-CAM.

Subset	PACE GM	PACE GM + CAM	PACE IM	PACE IM + CAM	PACE GM + IM + CAM
Official documents	25/25 (100%)	0/25 (0%)	1/25 (4%)	0/25 (0%)	0/25 (0%)
Non-official documents	14/15 (93.3%)	8/15 (53.3%)	3/15 (20%)	2/15 (13.3%)	1/15 (6.7%)
Total	**39/40**	**8/40**	**4/40**	**2/40**	**1/40**

	(97.5%)	(20%)	(10%)	(5%)	(2.5%)

Table 15. PACE mapping.

B.6.2 Key exchange mechanism

The table below shows the PACE key exchange mechanism used by the documents.

95% of the documents supported PACE ECKA, 7.5% supported PACE DHKA and only one (2.5%) supported both mechanisms.

PACE ECKA	PACE DHKA	PACE ECKA + DHKA
38/40 (95%)	3/40 (7.5%)	1/40 (2.5%)

Table 16. PACE key exchange mechanism.

B.6.3 PACE algorithm

The table below shows the PACE algorithms used by the documents.

About 77% of the PACE algorithms found in EF.CardAccess would establish an AES secure channel and about 23% of the PACE algorithms found in EF.CardAccess would establish a 3DES secure channel.

For AES the predominant key length is 128 bits (about 47%), followed by key lengths of 256 bits (about 39%) and key lengths of 192 bits (about 14%).

Three of the PACE algorithms defined in ICAO 9303-11 [7] could not be found in the Interoperability Test samples. They are:

- id_pace_dh_im_3des_cbc_cbc;
- id_pace_dh_im_aes_cbc_cmac_128;
- id_pace_dh_im_aes_cbc_cmac_192.

PACE algorithm	Number (percentage) of occurrences
id_pace_ecdh_gm_aes_cbc_cmac_128	15/66 (22.7%)
id_pace_ecdh_gm_aes_cbc_cmac_256	13/66 (19.7%)
id_pace_ecdh_gm_3des_cbc_cbc	10/66 (15.1%)
id_pace_ecdh_cam_aes_cbc_cmac_128	7/66(10.6%)
id_pace_dh_gm_3des_cbc_cbc	3/66 (4.5%)
id_pace_ecdh_im_aes_cbc_cmac_256	3/66 (4.5%)
id_pace_ecdh_cam_aes_cbc_cmac_192	2/66 (3.0%)
id_pace_ecdh_cam_aes_cbc_cmac_256	2/66 (3.0%)

Table 17. PACE algorithms.

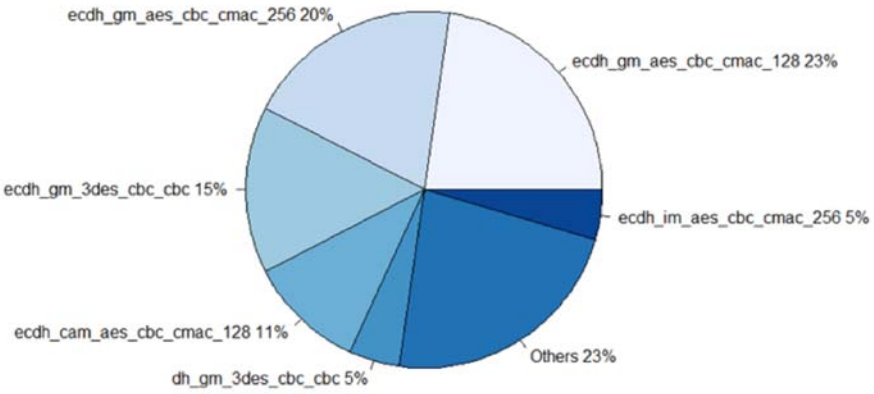

Figure 58. PACE algorithm.

The table below shows the first PACE algorithm in EF.CardAccess for all the models.

35% of the models offered id_pace_ecdh_gm_aes_cbc_cmac_128 as the first protocol, followed by id_pace_ecdh_gm_aes_cbc_cmac_256 (about 28%) and id_pace_ecdh_gm_3des_cbc_cbc (about 23%).

First PACE Algorithm in EF.CardAccess	
id_pace_ecdh_gm_aes_cbc_cmac_128	14/40 (35%)
id_pace_ecdh_gm_aes_cbc_cmac_256	11/40 (27.5%)
id_pace_ecdh_gm_3des_cbc_cbc	9/40 (22.5%)
id_pace_dh_gm_3des_cbc_cbc	3/40 (7.5%)
id_pace_ecdh_gm_aes_cbc_cmac_192	2/40 (5%)
id_pace_ecdh_im_3des_cbc_cbc	1/40 (2.5%)

Table 18. First PACE algorithm in EF.CardAccess.

The table below shows the number of algorithms (PACESecurityInfo) found in EF.CardAccess for all the models.

"Non-official documents" personalize several PACE algorithms probably in order to show compliance with the specifications.

PACE Algorithm count in EF.CardAccess	
10	1/40 (2.5%)
7	1/40 (2.5%)
3	1/40 (2.5%)
2	9/40 (22.5%)
1	28/40 (70%)

Table 19. PACE algorithm count in EF.CardAccess.

About 46% of the PACE algorithms used BrainpoolP256r1 and about 23% used nist_p_256_secp256r1. The mostly used DH domain parameter was 1024_MODP_Group_with_160_Prime_Order_Subgroup and it was selected by ≈ 8% of the PACE algorithms. None of the PACE algorithms found used explicit Domain parameters.

Four of the PACE standard domain parameters defined in ICAO 9303-11 [7] could not be found in the Interoperability Test samples. They are:

- 2048_MODP_Group_with_224_Prime_Order_Subgroup;
- BrainpoolP320r1;

- BrainpoolP512r1;
- nist_p_521_secp521r1.

B.7 ICAO Active Authentication

The table below shows which models had Active Authentication enabled and the signature algorithms used.

About 63% of the models had Active Authentication, 68% of them used as signature algorithm RSA ISO 9796-2 and a 32% used ECDSA. This fact probably shows a limitation in the personalization: for ECDSA signatures an ActiveAuthenticationSecurityInfo must be personalized in DG14 to code the signature hash algorithm but for RSA signatures the SecurityInfo is not needed (the hash algorithm is coded within the signature).

For the RSA signatures, about 71% used SHA-1 as the hash algorithm and ≈ 18% used SHA-256. One Smoke Test station did not have the AA option checked and therefore for two of the models the hash algorithm is unknown. This case is highlighted in red in the table below.

For the ECDSA signatures, about 38% used SHA-256 and a 25% used SHA-384 and SHA-1.

AA signature algorithm		AA signature hash algorithm
17/25 (68%)	SHA-256	3/17 (17.6%)
	SHA-1	12/17 (70.6%)
	Unknown	2/17 (11.8%)
8/25 (32%)	SHA-384	2/8 (25%)
	SHA-256	3/8 (37.5%)
	SHA-224	1/8 (12.5%)
	SHA-1	2/8 (25%)

Table 20. ICAO Active Authentication presence and signature algorithms.

The typical AA RSA public key had a length of 1536 bits (≈ 77%) and the maximum and minimum key lengths were 2048 and 1024 bits. The average value of the public key length implies that the typical eMRTD did not use extended length fields for the Internal Authenticate APDU. For AA, it should be noted that when using key lengths exceeding 1848 bits (if Secure Messaging with 3DES is used) / 1792 bits (if Secure Messaging with AES is used) the eMRTD chip and the Inspection System must support Extended Length APDUs.

The AA EC public key distribution for key length was 256 bits (≈ 38%), 384 bits (25%), 192 bits (25%) and 224 bits (≈ 13%). Maximum key length was 384 bits and minimum key length was 192 bits. 50% of the domain parameters were NIST and the other 50% of the domain parameters were Brainpool.

B.8 ICAO Chip Authentication

About 90% of the documents implemented Chip Authentication.

Of them, about 90% had only one ChipAuthenticationSecurityInfos in DG14, a ≈ 6% had two ChipAuthenticationSecurityInfos in DG14 and two documents (≈ 6%) had zero ChipAuthenticationSecurityInfos in DG14 but a ChipAuthenticationPublicKeySecurityInfo (according to BSI TR03110-3 [10], A.1.1. this is valid for ICCs implemented according to version 1.0.x of the specification).

B.8.1 Key exchange mechanism

The table below shows the Chip Authentication key exchange mechanism used by the documents.

About 83% of the samples supported ECKA, 10% of the samples supported DHKA and only one (2.5%) of the samples supported both mechanisms.

CA ECKA	CA DHKA	CA ECKA + DHKA
33/40 (82.5%)	4/40 (10%)	1/40 (2.5%)

Table 21. ICAO Chip Authentication key exchange mechanism.

B.8.2 CA algorithm

The table below shows the CA algorithms used by the samples.

About 63% of the CA algorithms found in DG14 would establish a 3DES secure channel and ≈ 37% of the CA algorithms found in DG14 would establish an AES secure channel.

For AES the predominant key length was 128 bits (≈ 69%), followed by key lengths of 256 bits (≈ 25%) and key lengths of 192 bits (≈ 6%).

Three of the CA algorithms defined in ICAO 9303-11 [7] could not be found in any of the Interoperability Test samples. They are:

- id_ca_dh_aes_cbc_cmac_128;
- id_ca_dh_aes_cbc_cmac_192;
- id_ca_dh_aes_cbc_cmac_256.

CA algorithm	
id_ca_ecdh_3des_cbc_cbc	44.4%
id_ca_ecdh_aes_cbc_cmac_128	30.6%
id_ca_dh_3des_cbc_cbc	11.1%
id_ca_ecdh_aes_cbc_cmac_256	11.1%
id_ca_ecdh_aes_cbc_cmac_192	2.8%

Table 22. Chip Authentication algorithms.

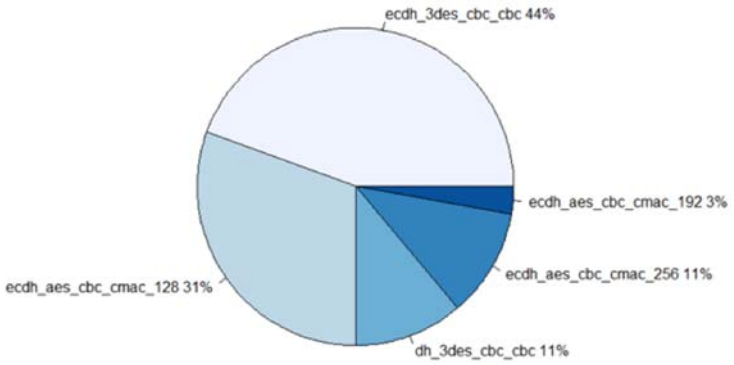

Figure 59. Chip Authentication algorithms.

B.9 BSI TR03110 Terminal Authentication V1

Terminal Authentication was implemented in 87.5% of the samples submitted to the test.

The table below shows the signature algorithms used for samples supporting TA.

About 94% of such documents used as signature algorithm ECDSA, a ≈ 6% used RSA PKCS#1 v1.5 and no document used RSA SSA PSS. This is consistent with the fact that

ECDSA signatures are smaller, for the same level of cryptographic strength, than RSA signatures.

SHA-256 (≈ 85%) was the most frequent hash algorithm. SHA-512 and SHA-384 were never found, which is consistent with the key lengths used by TA v1.

TA v1 signature algorithm		TA v1 signature hash algorithm	
RSA PKCS#1 v1.5	5.7%	SHA-512	0%
		SHA-256	100%
		SHA-1	0%
RSA SSA PSS	0%	SHA-512	0%
		SHA-256	0%
		SHA-1	0%
ECDSA	94.2%	SHA-512	0%
		SHA-384	0%
		SHA-256	78.8%
		SHA-224	12.1%
		SHA-1	9.1%

Table 23. Terminal Authentication signature algorithms.

The table below shows the TA public key algorithm with their key lengths. In case of EC public key, the domain parameter is also shown.

The typical TA EC public key had a length of 256 bits (≈ 85%) and the maximum and minimum key lengths were 256 and 224 bits. ≈50% of the domain parameters were NIST and the other 50% of the domain parameters were Brainpool.

TA v1 Public key length (bits)			TA v1 EC domain parameter	
RSA	2048	100%		
EC	256	84.8%	BrainpoolP256r1	50%
			nist_p_256_secp256r1	50%
	224	15.2%	BrainpoolP224r1	80%
			nist_p_224_secp224r1	20%

Table 24. Terminal Authentication public key length and EC domain parameters.

B.10 ISO 7816-4 Secure Message

Finally, for the ISO 7816-4 Secure Message established after PACE or Chip Authentication, we investigate the frequency of the different Secure Message types. There should be a trend defined of replacing 3DES with AES.

Still ≈ 23% of the samples only supported SM based on 3DES, ≈ 48% of the models had 3DES deprecated.

About 18 % of the samples made the switch moving from a SM based on AES after PACE protocol to a SM based on 3DES after the CA protocol.

B.11 Average eMRTD

In conclusion, the average eMRTD submitted to the Interoperability Test had the following features:

- Needed an inspection time of ≈10 s using a baud rate of 106 kbps;

- Had EF.ATR/INFO personalized with Extended length fields and SFI support (60%);
- Implemented LDS V1.7 (90%);
- Implemented the mandatory DGs 1 and 2 (100%) with DG2 having an average size of 14.6 Kb;
- Implemented EAC v1 and personalized DG3 (88%) with two fingerprints instances with an average size of 20.3 Kb;
- Implemented Passive Authentication (100%) using as PKI:
    - A CSCA using RSA PKCS v.15 or ECDSA with a public key length of 4096 or 384 bits;
    - A CDS using RSA PKCS v.15 or ECDSA with a public key length of 2048 or 256 bits;
- Implemented PACE (100%) using ECKA –Generic mapping- AES with BrainpoolP256r1 or nist_p_256_secp256r1 as domain parameters;
- Implemented Active Authentication (63%) using as signature RSA ISO 9796-2 with SHA-1 and a public key length of 1536 bits.
- Implemented Chip Authentication (90%) using ECKA-3DES with BrainpoolP256r1 or nist_p_256_secp256r1 as domain parameters;
- Implemented Terminal Authentication (≈ 88%) v1 using ECDSA-SHA256 with BrainpoolP256r1 or nist_p_256_secp256r1 as domain parameters.

References

[1] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 1 Introduction, Seventh Edition, 2015.

[2] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 2 Specifications for the Security of the Design, Manufacture and Issuance of MRTDs, Seventh Edition, 2015.

[3] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 3 Specifications Common to all MRTDs, Seventh Edition, 2015.

[4] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 4 Specifications for Machine Readable Passports (MRPs) and other TD3 size MRTDs, Seventh Edition, 2015.

[5] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 5 Specifications for TD1 size Machine Readable Official Travel Documents (MROTDs), Seventh Edition, 2015.

[6] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 10 Logical Data Structure (LDS) for storage of biometrics and other data in Contactless Integrated Circuit (IC), Seventh Edition, 2015.

[7] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 11 Security Mechanisms for MRTDs, Seventh Edition, 2015.

[8] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 12 Public Key Infrastructure for MRTDs, Seventh Edition, 2015.

[9] BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents, Part 1, Version 2.20 of 26 February 2015.

[10] BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 - Common Specifications, Version 2.20 of 3 February 2015.

[11] ISO/IEC 7816-4. Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange. Third Edition. 15.04.2013.

[12] NIST Special Publication 800-57 Part3. Revision 1. Recommendation for Key Management. Part3: Application-specific Key Management Guidance.

[13] FIPS 197. Announcing the ADVANCED ENCRYPTION STANDARD (AES). November 26, 2001.

[14] ISO/IEC 14443-4. Identification cards - Contactless integrated circuit cards - Proximity cards - Part 4: Transmission protocol. Third Edition. 01.06.2016.

[15] ITU-T X.690 SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS. ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

[16] ISO/IEC 7816-8. Identification cards - Integrated circuit cards - Part 8: Commands for security operations. Third Edition. 01.11.2016.

[17] RFC5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. May 2008.

[18] FIPS PUB 46-3. DATA ENCRYPTION STANDARD (DES). 1999 October 25.

[19] RFC2631. Diffie-Hellman Key Agreement Method. June 1999.

[20] RFC5114 Additional Diffie-Hellman Groups for Use with IETF Standards. January 2008.

[21] RFC5639. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. March 2010...

[22] FIPS 186-4. Digital Signature Standard (DSS). July 2013.

[23] BSI TR-03111. Elliptic Curve Cryptography. Version 2.0. 2012-06-28..

[24] RFC7468. Textual Encodings of PKIX, PKCS, and CMS Structures. April 2015.

[25] RFC8017. PKCS #1: RSA Cryptography Specifications Version 2.2. November 2016.

[26] ISO/IEC 9796-2 Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms. Third edition. 2010-12-15.

[27] FIPS PUB 180-4. Secure Hash Standard (SHS). August 2015.

[28] International Civil Aviation Organization (ICAO), RF Protocol and Application Test Standard for eMRTD Part 3 – Tests for Application Protocol and Logical Data Structure, v2.10. July 2016

[29] BSI TR-03105 Part 3.2: Test plan for eMRTDs with EACv1, v1.4.1. April, 2014.

[30] International Civil Aviation Organization (ICAO), RF and Protocol Testing Part 4 – Conformity Test for Inspection Systems, v2.10

[31] BSI TR-03105 Part 5.1: Test plan for ICAO compliant Inspection Systems with EACv1, v1.41

[32] ICAO, TR – Durability of Machine Readable Passports, v3.2, August 2006

[33] ICAO, TR – RF Protocol and Application Test Standard for ePassport Part 2 – Tests for Air Interface, Initialisation, Anticollision and Transport Protocol, v1.02, February 2007

[34] ISO ISO/IEC 18745-2. Information Technology - Test methods for machine readable travel documents (MRTD) and associated devices -- Part 2: Test methods for the contactless interface. First Edition. 15.08.2016

[35] Regional Seminar on MRTDs and Traveller Identification Management, Madrid, Spain, 25 to 27 June 2014. Results Interop-Test. Results Interop-Test

List of abbreviations and definitions

Definitions

- **Active Authentication:** cryptographic protocol, used in ICAO PKI, to authenticate the MRTD chip by signing a challenge sent by the IFD (inspection system) with a private key known only to the ICC. See ICAO 9303-11 (International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 11 Security Mechanisms for MRTDs, Seventh Edition, 2015).

- **AES:** a symmetric key specification for the encryption of electronic data established by the NIST. It is based on substitution-permutation network. There are three key lengths available (128, 192 and 256 bits). It is a block cipher with a block size of 128 bits. See FIPS-197 (FIPS 197. Announcing the ADVANCED ENCRYPTION STANDARD (AES). November 26, 2001).

- **APDU:** The communication unit between a smart card reader and a smart card. See ISO 7816-4 (ISO/IEC 14443-4. Identification cards - Contactless integrated circuit cards - Proximity cards - Part 4: Transmission protocol. Third Edition. 01.06.2016).

- **ATS:** PICC Answer to a Select. Codes communication parameters and general information in the form of historical bytes. See ISO 14443-4 (ISO/IEC 14443-4. Identification cards - Contactless integrated circuit cards - Proximity cards - Part 4: Transmission protocol. Third Edition. 01.06.2016).

- **Authentication:** a process that validates the claimed identity of a participant in an electronic transaction.

- **Authenticity:** (ICAO) the ability to confirm that the Logical Data Structure and its components were created by the issuing state or organization. See ICAO 9303-11 (International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 11 Security Mechanisms for MRTDs, Seventh Edition, 2015).

- **Distinguished Encoding Rules (DER):** for ASN.1, as defined in X.690 (ITU-T X.690 SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS. ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)). DER is a subset of BER.

- **Card Verifiable Certificates (CVC):** devices with limited computing power such as smart cards can process this type of digital certificates. The certificates use simple TLV (Tag Length Value) which encode fixed fields. Fixed fields means that each field in the certificate is of fixed, or maximum, length and each field comes in a well-defined order. This makes parsing easy, in contrast to ASN.1 parsing which requires more processing and has to keep fields of arbitrary length in memory while parsing nested content. [WIKIPEDIA]. See ISO 7816-8 (ISO/IEC 7816-8. Identification cards - Integrated circuit cards - Part 8: Commands for security operations. Third Edition. 01.11.2016).

- **Certificate**: a type that binds a subject entity's distinguished name to a public key with a digital signature. X.509 defines this type. This type also contains the distinguished name of the certificate issuer (the signer), an issuer-specific serial number, the issuer's signature algorithm identifier, a validity period, and an optional set of certificate extensions.

- **Certification Authority (CA):** an entity that issues digital certificates. See RFC 5280 (RFC5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. May 2008).

- **Chip Authentication:** cryptographic protocol, used in ICAO PKI, which provides secure communication and unilateral authentication of the eMRTD chip. Uses an ephemeral-static Diffie-Hellmann key agreement protocol. It is preferred to Active Authentication because it provides strong secure message keys and prevents challenge semantics attacks. See ICAO 9303-11 (International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 11 Security Mechanisms for MRTDs, Seventh Edition, 2015).

- **Country Signing Certification Authority (CSCA**): the CA responsible for issuing Country Signing Certificates. These are used to validate the Document Signing Certificates, which are signed by the CSCA. See ICAO 9303-12 (International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 12 Public Key Infrastructure for MRTDs, Seventh Edition, 2015).

- **Country Verifying Verification Authority (CVCA**): the CA root of the EAC infrastructure. It issues CVCA root certificates and DV certificates. See BSI TR-03110 (BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents, Part 1, Version 2.20 of 26 February 2015) and (BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 - Common Specifications, Version 2.20 of 3 February 2015).

- **Data Group:** a series of related Data Elements grouped together within the Logical Data Structure. See ICAO 9303-10 (International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 10 Logical Data Structure (LDS) for storage of biometrics and other data in Contactless Integrated Circuit (IC), Seventh Edition, 2015).

- **DES:** a symmetric key specification for the encryption of electronic data. Now it is considered insecure but it is considered practically secure in the 3DES from. It has been superseded by AES. It is based on a Feistel network with a block size of 64 bits. See FIPS 46-3 (FIPS PUB 46-3. DATA ENCRYPTION STANDARD (DES). 1999 October 25).

- **Diffie Hellmann Cryptography:** Asymmetric algorithm multiplicative based on the group of integers modulo p. It is based on the difficult of computing discrete logarithms in the group. See RFC2631 (RFC2631. Diffie-Hellman Key Agreement Method. June 1999.) and RFC5114 (RFC5114 Additional Diffie-Hellman Groups for Use with IETF Standards. January 2008.).

- **Domain parameters:** in Diffie-Hellmann or Elliptic Curve, a set of information for communication parties used to identify a certain group for use in cryptography. The use of standardized domain parameters is preferred. See RFC2631 (RFC2631. Diffie-Hellman Key Agreement Method. June 1999.), RFC5114 (RFC5114 Additional Diffie-Hellman Groups for Use with IETF Standards. January 2008.), RFC5639 (RFC5639. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. March 2010.) and FIPS 186-4 (FIPS 186-4. Digital Signature Standard (DSS). July 2013).

- **Extended Access Control Public Key Infrastructure (EAC-PKI):** the infrastructure required to control access to fingerprint biometrics on Passports and Travel Documents utilising Extended Access Control. See BSI TR-03110-3 (BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 - Common Specifications, Version 2.20 of 3 February 2015).

- **Digital Signature:** the result of a cryptographic operation enabling the validation of information by electronic means.

- **Document Signer (DS):** a Document Signer digitally signs data to be stored on eMRTDs; this signature is stored on the eMRTD in a Document Security Object. See ICAO 9303-12 (International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 12 Public Key Infrastructure for MRTDs, Seventh Edition, 2015).

- **Document Verifier (DV):** an entity within the EAC-PKI that requests certificates from CVCAs and, based on those certificates, issues certificates to Inspection Systems. See BSI TR-03110-3 (BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 - Common Specifications, Version 2.20 of 3 February 2015).

- **Elliptic Curve Cryptography:** Asymmetric algorithm using elliptic curves. It is based on the difficult of computing discrete logarithms in the group of points on an elliptic curve defined over a finite field. See BSI TR-03111 (BSI TR-03111. Elliptic Curve Cryptography. Version 2.0. 2012-06-28.).

- **Fingerprint(s):** One (or more) visual representation(s) of the surface of the holder's fingertip(s).

- **Hash**: a deterministic algorithm that takes an arbitrary block of data and returns a fixed-size bit string; the cryptographic hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message", and the hash value is sometimes called the "message digest" or simply "digest".

- **International Civil Aviation Organisation (ICAO):** a UN organisation tasked with fostering the planning and development of international air transport. In this role is sets international standards for MRTDs.

- **Inspection System (IS):** the operational system that reads fingerprint biometrics from MRTDs.

- **Integrity:** The ability to confirm that the Logical Data Structure and its components have not been altered from that created by the issuing State or organization.

- **ISO 14443 Communication interface**, **Type A:** In type A cards 100% ASK modulation with modified Miller coding is defined as the modulation procedure used for the transfer of data from reader to card. A load modulation procedure with subcarrier is used for data transfer from the smart card to the reader. The modulation of the initial subcarrier is performed by on/off keying of the subcarrier using a Manchester coded data stream.

- **ISO 14443 Communication interface**, **Type B:** In Type B cards 10% ASK modulation is used as the modulation procedure for the data transfer from reader to card. A simple NRZ coding is used for bit coding. A load modulation procedure with subcarrier is used for data transfer from the smart card to the reader. The subcarrier is modulated by 180◦ phase shift keying (BPSK) of the subcarrier using the NRZ coded data stream.

- **Issuing State:** The country issuing the MRTD.

- **Key agreement:** a cryptographic protocol whereby two or more parties can agree on a key in such a way that both influence the outcome. If properly done, this precludes undesired third parties from forcing a key choice on the agreeing parties. Protocols that are useful in practice also do not reveal to any eavesdropping party what key has been agreed upon.

- **Key pair:** the Private Key and its associated Public key.

- **Logical Data Structure (LDS**): The Logical Data Structure describes how data are stored and formatted in the contactless IC of an eMRTD. See ICAO 9303-10 (International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 10 Logical Data Structure (LDS) for storage of biometrics and other data in Contactless Integrated Circuit (IC), Seventh Edition, 2015).

- **Machine Readable Travel Document (MRTD):** an international travel document containing eye and machine-readable data. See ICAO 9303.

- **Mapping:** in the PACE protocol, a cryptographic mechanism used to map a nonce to a random generator of the group. The PACE-CAM mapping integrates Chip Authentication in the protocol. See ICAO 9303-11 (International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 11 Security Mechanisms for MRTDs, Seventh Edition, 2015).

- **Nonce:** In cryptography, a nonce is an arbitrary number that can only be used once. It is similar in spirit to a nonce word, hence the name. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks. They can also be useful as initialization vectors and in cryptographic hash functions.

- **PACE:** is a password authenticated Diffie-Hellman key agreement protocol that provides Secure Messaging between an eMRTD chip and an inspection system based on weak (short) passwords. It is used in eMRTDs to supersede the BAC protocol. See ICAO 9303-11 (International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 11 Security Mechanisms for MRTDs, Seventh Edition, 2015).

- **Passive Authentication (PA):** cryptographic protocol, used in ICAO PKI, to protect the MRTD chip against manipulation and forgery. See ICAO 9303-11 (International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 11 Security Mechanisms for MRTDs, Seventh Edition, 2015).

- **PCSC:** A smart card specification for integration of smart cards in computing environments.

- **PEM:** a de facto file format for storing and sending cryptography keys, certificates, and other data, based on a set of 1993 IETF standards defining "privacy-enhanced mail." It is a text format suitable for systems that only support ASCII. See RFC7468 (RFC7468. Textual Encodings of PKIX, PKCS, and CMS Structures. April 2015.).

- **Personalization:** The process by which the portrait, signature and biographical data are applied to the document.

- **Private Key:** the key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

- **Public Key:** the key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

- **Public Key certificate:** electronic document used to prove the ownership of a public key.

- **Rivest, Shamir and Adleman (RSA):** Asymmetric algorithm invented by Ron Rivest, Adi Shamir and Len Adleman. It is used in public-key cryptography and is based on the fact that it is easy to multiply two large prime numbers together, but hard to factor them out of the product. See RFC8017 (RFC8017. PKCS #1: RSA Cryptography Specifications Version 2.2. November 2016.).

- **Root Certificate:** the self-signed Certificate issued by the Root CA to identify itself.

- **RSA ISO 9796-2 signature**: A digital signature giving message recovery, if the message is sufficiently short, then the message recovery would be total because it is possible to include entirely the message in the signature. See ISO 9796-2 (ISO/IEC 9796-2 Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms. Third edition. 2010-12-15).

- **RSA Probabilistic Signature Scheme:** A digital signature with appendix in which the encoding method is randomized. Its usage is recommended. See RFC8017 (RFC8017. PKCS #1: RSA Cryptography Specifications Version 2.2. November 2016.).

- **RSA PKCS 1.5 Signature Scheme:** A digital signature with appendix in which the encoding method is not randomized. Its usage is not recommended. See RFC8017 (RFC8017. PKCS #1: RSA Cryptography Specifications Version 2.2. November 2016.).

- **Secure Message:** application of data confidentiality and data authentication to all or part of a C-RP, or a concatenation of consecutive data fields. See ISO 7816-4 (ISO/IEC 14443-4. Identification cards - Contactless integrated circuit cards - Proximity cards - Part 4: Transmission protocol. Third Edition. 01.06.2016).

- **Sensitive Data:** Finger and iris image data stored in the LDS Data Groups 3 and 4, respectively. These data are considered to be more privacy sensitive than data stored in the other Data Groups. See ICAO 9303-10 (International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 10 Logical Data Structure (LDS) for storage of biometrics and other data in Contactless Integrated Circuit (IC), Seventh Edition, 2015).

- **SHA-1** (**Secure Hash Algorithm 1**): is a cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST. SHA-1 produces a 160-bit (20-byte) hash value known as a message digest. Its usage is not recommended. See FIPS 180-4 (FIPS PUB 180-4. Secure Hash Standard (SHS). August 2015.).

- **SHA-2** (**Secure Hash Algorithm 2**): is a cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. See FIPS 180-4 (FIPS PUB 180-4. Secure Hash Standard (SHS). August 2015.).

- **Smoke Test**: also known as "Build Verification Testing", is a type of software testing that comprises of a non-exhaustive set of tests that aim at ensuring that the most important functions work. The results of this testing is used to decide to proceed with further testing.

- **Terminal:** for EAC PKI, a terminal is a reader component that contains the proximity coupling device (PCD) used for communication between terminal and MRTD. More than one reader component may be part of a single terminal. For example, all reader at the border control of an airport can be part of the same inspection system.

Terminal Authentication is done rather between the terminal and the MRTD than between the single reader and the MRTD. See BSI TR-031110 (BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents, Part 1, Version 2.20 of 26 February 2015) and (BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 - Common Specifications, Version 2.20 of 3 February 2015).

- **Terminal Authentication v1:** a two move challenge-response protocol that provides explicit unilateral authentication of the terminal. It enables the MRTD chip to verify that the terminal is entitled to access sensitive data. See BSI TR-031110 (BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents, Part 1, Version 2.20 of 26 February 2015) and (BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 - Common Specifications, Version 2.20 of 3 February 2015).

- **Terminal Certificate**: for EAC PKI, Terminal Authentication requires the Terminal to be equipped with at least one certificate, encoding the Terminal's public key and access rights. See BSI TR-031110 (BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents, Part 1, Version 2.20 of 26 February 2015) and (BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 - Common Specifications, Version 2.20 of 3 February 2015).

- **Trusted certification path:** a chain of multiple certificates needed to validate a certificate containing the required public key. For EAC-PKI, a certificate chain consists of one or more CVCA certificates, link certificates as appropriate, a DV certificate and the IS certificate. For ICAO-PKI, a certificate chain consists of one CVCA certificate and a DS certificate.

- **X.509 v3 certificate**: The internationally recognized electronic document used to prove identity and public key ownership over a communication network. It contains the issuer's name, user's identifying information, and issuer's digital signature. See RFC5280 (RFC5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. May 2008).

Acronyms

3DES	Triple DES
AA	Active Authentication
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
ASK	Amplitude Shift Keying
ASN.1	Abstract Syntax Notation 1
AT	Authentication Template
ATR	Answer To Reset
ATS	Answer To Select
BAC	Basic Access Control
BPSK	Binary Phase Shift Keying
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
CA	Certificate Authority
CA	Chip Authentication
CAN	Card Access Number
CAM	Chip Authentication Mapping
CAPDU	Command APDU
CBC	Cipher Block Chaining

CDS	Document Signer Certificate
CID	Card IDentifier
CMAC	Cipher based Message Authentication Code
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
C-RP	Command-Response Pair
CSCA	Country Signing Certificate Authority
CSV	Comma Separated Values
CVC	Card Verifiable Certificate
CVCA	Country Verifying Certificate Authority
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DIR	DIRectory
DF	Dedicated File
DG	Data Group
DH	Diffie Hellmann
DHKA	Diffie Hellmann Key Agreement
DO	Data Object
DS	Document Signer
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DV	Document Verifier
EAC	Extended Access Control
EC	Elliptic Curve
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
EF	Elementary File
ECKA	Elliptic Curve Key Agreement
eIDAS	Electronic IDentification And trust Services (EU Regulation No 910/2014)
eMRTD	electronic Machine Readable Travel Document
eRP	Electronic Residence Permit
EU	European Union
FIPS	Federal Information Processing Standards
FMD	File Management Data
GM	Generic Mapping
ID	IDentifier
ICAO	International Civil Aviation Organisation
IC	Integrated Circuit
ICC	Integrated Circuit Card
ICS	Implementation Conformance Statement
IEC	International Electrotechnical Commission
IFD	InterFace Device
IM	Integrated Mapping
IS	Inspection System
ISO	International Organization for Standardization
KAT	Key Agreement Template
L_c field	Length field for coding the number of bytes in the command data field
L_e field	Length field for coding the maximum number of bytes expected in the response data field
LDS	Logical Data Structure
MAC	Message Authentication Code
MODP	MODular exPonential
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
MSE	Manage Security Environment

N.A.	Not Applicable
NAD	Node ADress
NIST	National Institute of Standards and Technology
NTWG	New Technology Working Group
NRZ	Non Return to Zero
OCR	Optical Character Recognition
OID	Object Identifier
OSI	Open Systems Interconnection
PA	Passive Authentication
PACE	Password Authenticated Connection Establishment
PCSC	Personal Computer/Smart Card
PEM	Privacy-enhanced Electronic Mail
PICC	Proximity Integrated Circuit Card
PID	Participant IDentification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure for X.509 certificates
PSS	Probabilistic Signature Scheme
PUPI	Pseudo-Unique PICC Identifier, type B
RAM	Random-Access Memory
RAPDU	Response APDU
RF	Radio Frequency
RFC	Request For Comments
RFID	Radio Frequency IDentification
RFU	Reserved for Future Use
RND	RaNDom
RSA	Rivest, Shamir and Adleman
SFI	Short File Identifier
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SM	Secure Message
SOD	Document Security Object
SP	Special Publication
SW	Status Word
TA	Terminal Authentication
TR	Technical Report
TS	Technical Specification
UID	Unique Identifier, type A
URI	Uniform Resource Identifier
USB	Universal Serial Bus

List of figures

List of tables

KJ-NA-29216-EN-N

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/828262
ISBN 978-92-79-85687-7