FRONTEX

LIBERTAS SECURITAS JUSTITIA

European Agency for the Management of Operational Cooperation at the External Borders
of the Member States of the European Union

Operational and Technical security of Electronic Passports

Warsaw, July 2011

Legal notice

The contents of this publication do not necessarily reflect the official opinion of any institution or body of the European Union. Neither Frontex nor any person or company acting on behalf of Frontex is responsible for the use that may be made of the information contained in this report.

All rights reserved

Information about the European Union is available on the Internet. It can be accessed through the Europa server (www.europa.eu)

Frontex Agency
Rondo ONZ 1
00-124 Warsaw
Poland
Tel: +48 22 544 9500
Fax: +48 22 544 9501
Web: www.frontex.europa.eu
Enquiries: frontex@frontex.europa.eu

Introductory Note by Frontex

In 2010 Frontex — also formally known as European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union — commissioned a study on the Security of Electronic Passports (e-Passports) in Europe.

In the following paragraphs we briefly describe why and how this was done.

Frontex Research and Development Unit

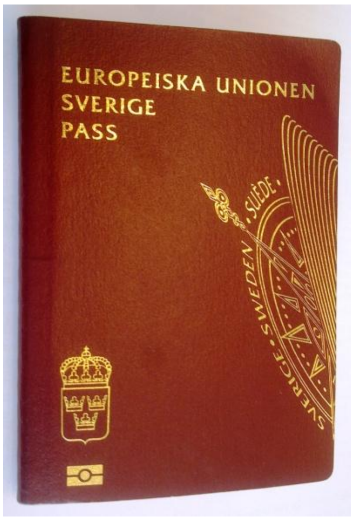
As part of the Capacity Building Division at Frontex, the Research and Development Unit (RDU) is tasked to follow up on developments in research relevant to border control and disseminate this information to the end-users.

The Unit's objectives according to the Frontex Multi Annual Plan 2010-2013 are in particular:

a) to drive the process of harmonization and development of standards, both technical and operational, for border control;
b) to provide for adequate representation of the common interests of the Member States in European border security research;
c) to keep Member States informed concerning new technical/technological developments in the field of border control.

The Unit produces guidelines and commissions studies to assess the value of new technology and to help establish priorities for the development of future capabilities for European border security.

Examples of the guidelines and studies produced, or in production, by the Unit include "*Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Crossing Systems (2011)*", "*BIOPASS – Study on Automated Border Crossing systems for Registered Passengers at Four European Airports*", "*BIOPASS II – Automated Biometric Border Crossing Systems Based on Electronic Passports and Facial Recognition: RAPID and SmartGate*", "*Ethics of border control*", "*Anti-corruption measures in EU border control*".



e-Passport, as identified by the symbol at bottom-left.

Since August 2006 the 27 Member States of the European Union have been required to issue e-Passports that contain a digital facial image, and since June 2009 they have been obliged to issue second generation e-Passports that also include two fingerprints. The purpose of mandating issuance of e-Passports has been to strengthen the link between the passport and the carrier of the passport, as well as to make it easier to verify the authenticity of the passport. Other European biometric initiatives include the Visa Information System currently being rolled out, which is used for 3rd country nationals applying for a visa to the Schengen area.

With the increase in the numbers of e-Passports in circulation in the European Union the need arises to assess the security impact of the new technology. Border guards will be encountering e-Passports in ever greater numbers, and in some cases – most notably the Automated Border Control (ABC) systems already in operation in several major European airports – the added functionality of these passports is already being put to use for travel facilitation of European citizens.

Meanwhile, the added security that e-Passports can provide, with the proviso that they are used correctly, will likely mean that fraudulent travelers will move away from falsified passports and instead seek to subvert the border control system either by attempting look-alike fraud using genuine documents, or by trying to subvert the issuance process in order to be fraudulently issued with genuine e-Passports.

The Schengen borders-code, and also the Schengen handbook, provide instructions on how to conduct border checks and border surveillance, but does not deal with biometrics to any larger extent. In view of this, coupled with the widespread dissemination of e-Passports, the Frontex Research and Development Unit commissioned a study on the "*Operational and Technical security of E-passports*" in 2010.

The tender for the study was awarded to PriceWaterhouseCoopers, working together with Collis and the digital-security group of Radboud University, Nijmegen, the Netherlands. The study group began their work in mid 2010 and the study was completed by the spring of 2011.

The specific objectives of the study, as stated in the terms of reference, were as follows:

a) to establish an inventory of security relevant issues in the context of the application for, production, and use of electronic passports (BAC and EAC) in Europe;

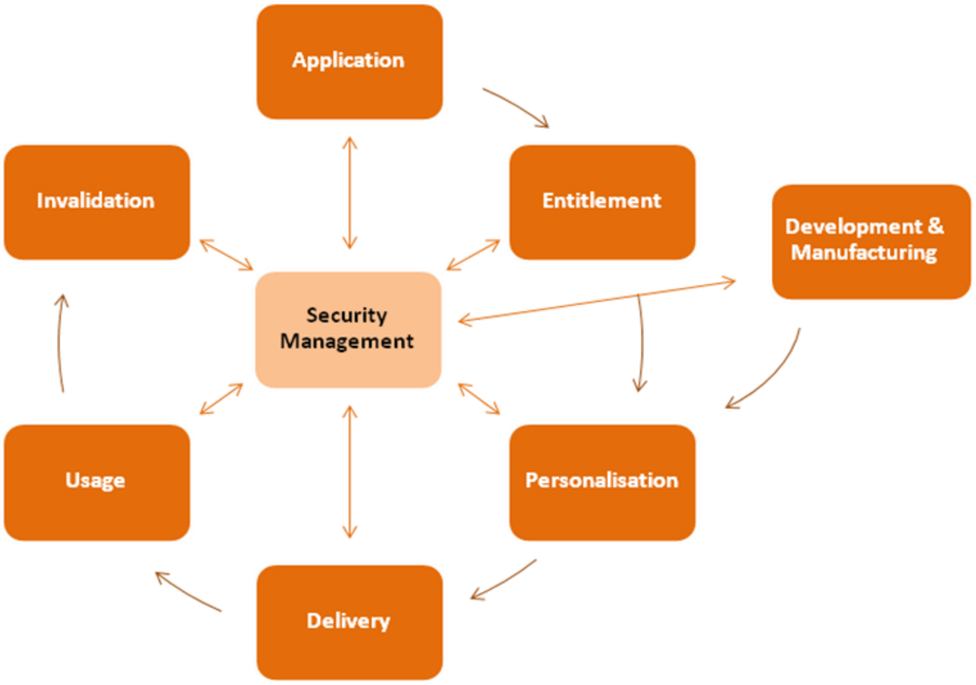
b) to individuate differences among EU/Schengen member States and highlight eventual problems for interoperability when the passports are used for identification at external borders;

c) to identify best practices related to the issuance processes;

d) to suggest a set of recommendation to redress security gaps in the issuance process.

The study included direct interviews with selected experts and a questionnaire answered by European authorities, and was concluded with a risk-analysis workshop attended by experts selected by the EU/Schengen Member States national authorities.

The resulting report covers not only security but also interoperability and follows the e-Passport through all the steps of its life-cycle, from application to invalidation.



e-Passport life-cycle.

Interesting issues that unfortunately had to be left outside the scope of the study include technical issues specific for e-Passport readers or the accuracy of biometric technologies.

The final report of the study is presented here as it was delivered to Frontex by the study group, with only some cosmetic modifications. Frontex supported the work of the study group with guidance and contacts, but did not in any way affect the production of the report as regards conclusions and recommendations.

During the concluding risk analysis workshop it was found that the attending experts in some cases held differing views on vulnerabilities and priorities, so the study should be seen as an initial wide probe into the issue of European e-Passport security.

Future activities

At the time of writing some of the topics under consideration by the Frontex Research & Development Unit for future action as a consequence of the study are:

a) standards for evaluation of biometric systems in Europe;

b) PKI technical implementation surveys;

c) e-Passport interoperability;

d) recommendations for e-Passport inspection procedures;

e) gap analysis for border control (not limited to e-Passports).

Table of contents

Executive summary

This study on the technical and operational security of electronic passports was commissioned by Frontex and executed by the study consortium, consisting of PwC, Collis and Radboud University Nijmegen during the period June 2010-March 2011. The study was performed in a number of consecutive stages:

1. A document study based on currently available literature was performed (Chapter 2).
2. A number of e-passport experts throughout Europe were interviewed (Chapter 3).
3. Based on the document study and the interviews, an e-passport lifecycle was compiled on which a rudimentary risk analysis was performed to identify the security risks in issuance and usage of e-passports and on the technical security risks in the e-passport chip itself (Chapter 3).
4. A questionnaire based on the first three steps to validate and improve the results of these steps, most notably on the security risks identified in the previous step, was sent out (Chapter 4).
5. An expert workshop in January 2011, in which all EU/Schengen Member States were asked by Frontex for participation with their experts, was held to validate the results of the questionnaire and to identify high-risk/priority issues (Chapter 6).
6. A small sample of actual e-passports was read and analysed (Chapter 7).
7. A final report was compiled, of which this document is the result.

For more information on the approach and results of these stages, we refer to the respective chapters of this report.

To get a good understanding of the issues and a validation of our results, the e-passport community in Europe was heavily involved in the realisation of this study. Also, known experts and stakeholders throughout Europe participated in the study. Given the vast extent of the electronic passports community, the 30 different Schengen/EU Member States and the limited time for this study, not all were fully and equally represented; however, we strived to give a view as balanced as possible and provide factual basis for conclusions and recommendations.

Conclusions and recommendations

We represent the conclusions and related recommendations (in *italics*) of the study briefly here. A more detailed discussion of these conclusions and recommendations can be found in Chapter 8.

The conclusions and recommendations are those of the study consortium, based on the documentation studied, their impressions from the interviews, the questionnaire results, and the discussions at the workshop. As such, they will not necessarily be shared or endorsed by all persons who have participated in the study (interviews, workshop, questionnaire).

In performing the study for Frontex, the consortium did not limit itself to the scope of Frontex's authority, so in some respects its conclusions and recommendations might stray beyond the limits of the remit of Frontex.

The reliability of the e-passport issuance process is vital for EU border control. (C1)

Further promote structural information exchange between the issuance community and the border control community on e-passport security matters (R1.1)

Provide training (and possibly tool provisioning) for the verification of breeder documents by issuance officers (R1.2)

Compile and structure good practices from the various Member States on the issuance process (R1.3)

Discuss voluntary EU/Schengen common guidelines for issuance of e-passports (R1.4)

Investigate the possibility of voluntary inter-country review of the e-passport issuance process (R1.5)

Lookalike fraud with e-passports is a substantial risk for EU/Schengen border control. (C2)

Investigate the benefits for border control to further improve the quality of the digital facial image (R2.1)

Investigate the future of the usage of fingerprints in border control (R2.2)

The usage of e-passport functionality by Member States at border control is currently limited and not uniform. (C3)

Provide training of border guards on the specifics of e-passport inspection (R3.1)

Investigate deployment of e-passport inspection (usage) at the border (both manual and automated border inspection) (R3.2)

Investigate harmonisation of the e-passport inspection procedure (R3.3)

Collect real-life performance data from Automated Border Control (ABC) system pilots (R3.4)

Many Member States experience operational difficulties in deploying e-passport inspection infrastructures. (C4)

Further investigate the obstacles Member States are facing in employing or deploying the public key infrastructures supporting the e-passport inspection (R4.1)

Investigate formalising the de facto practice of placing the document signing certificates in the e-passports (R4.2)

Further investigate the usage of "defect lists" in inspection systems, enabling inspection systems to recognise e-passports with known defects and enabling them to interpret the (technically wrong) responses (R4.3)

Cloning of e-passport chips is a serious concern. (C5)

Stimulate the adoption of mechanisms for authenticating the chip in all EU e-passports (R5.1)

National identity cards of Member States are also accepted as travel documents at the EU/Schengen border. As the security of national identity cards is not standardised, they might be considered as a weak link in border control. (C6)

Further investigate the security role of national ID cards in border control (R6.1)

Not all Member States seem to be in the process of phasing out the usage of the SHA-1 secure hash function as part of signing e-passport information. (C7)

Press for SHA-1 phase out for Passive Authentication (R7.1)

1. Introduction to the study

In the previous years the focus of ICAO and the European Union has been on improving the passport itself through the addition of a chip with biometrics and security features. Now that passport (technical) security (i.e. its resilience against forgery) has improved significantly, this study focuses on the security of issuance and inspection of the e-passport throughout the EU/Schengen area. The study is commissioned by Frontex to:

- Establish an inventory of security-relevant issues in the context of the procedure for issuance (including production) and use of electronic passports (e-passports) in Europe.
- Individuate differences among EU/Schengen Member States, highlighting possible interoperability issues when using electronic passports for identification at the external borders.
- Identify good practices and recommendations addressing the identified security issues.

The study was performed along three lines: a) the issuance of e-passports, b) the usage of e-passport in border control and c) technical security of e-passports. In the study, the following steps were conducted:

1. A document study based on currently available literature was performed (Chapter 2).
2. A number of e-passport experts throughout Europe were interviewed (Chapter 3).
3. Based on the document study and the interviews we compiled an e-passport lifecycle on which we performed a rudimentary risk analysis to identify the security risks in issuance and usage of e-passports and on the technical security risks in the e-passport chip itself. (Chapter 3).
4. A questionnaire based on the first three steps to validate and improve the results of these steps, most notably on the security risks identified in the previous step (Chapter 4).
5. An expert workshop in January 2011, in which all EU/Schengen Member States were asked by Frontex for participation with their experts, to validate the results of the questionnaire and to identify high-risk/priority issues (Chapter 6).
6. A small sample of actual e-passports was read and analysed (Chapter 7).
7. A final report was compiled, of which this document is the result.

This report is authored by representatives from PriceWaterhouseCoopers, Collis, and Radboud University, Nijmegen, the Netherlands.

2. E-passport document study

Summary

In this chapter, we report on the results of the document study we performed on issuance and usage of European e-passports and the inspection infrastructure. For the purposes of this study, we define an e-passport as the composition of the chip, the operating system and application running on the chip, the information stored in the chip and the security mechanisms that are implemented. The inspection infrastructure consists of an inspection system (IS) which is connected to other systems which provide the IS with signing and verifying PKI certificates. We have focused on issues in the context of border security (i.e. establishing a bearer's identity at a border check point), not on privacy.

The document study in this chapter, in parallel with the whole study, is divided along three topics:

- **Technical security** of e-passports, focusing on possible vulnerabilities to change/clone the e-passport after issuance.
- **Issuance security** of e-passports, focusing on possible vulnerabilities in the issuance process of the e-passport.
- **Usage security** of e-passports, focusing on possible usage and interoperability issues for the e-passport.

The documents that were used in our analysis originate from a number of international standards, EC decisions and guidelines as well as scientific literature in the field of e-passports.

We summarise the results of the study:

Technical security: From a border security perspective, the e-passport is equal to an electronically signed document of which

- the digital signature on the data forms a trustworthy link to the issuing country – Passive Authentication (PA) and
- the data forms a trustworthy link to the bearer –biometrics.

Passive Authentication (PA) is the mechanism for creating and verifying the digital signature. As such, it allows an IS to validate the authenticity of the data contained in the e-passport. It is, therefore, the essential security mechanism for e-passports. Vulnerabilities in this mechanism would directly threaten border security. Vulnerabilities in other security mechanisms (Basic Access Control or BAC, Extended Access Control or EAC, chip protection profile, etc.) can pose a risk for the bearer's privacy, but not directly for border security.

Issuance security: Because of improvement in the technical security of passports, there is a shift of fraudsters to be expected from counterfeited passports to attacks on the issuance process and/or lookalike fraud. As it is expected that biometrics will become increasingly available and will be continuously improved to combat lookalike fraud, the focus of fraudsters will be on the issuance process. Exploited vulnerabilities could be issuing staff errors, issuing staff fraud and flaws in operational security.

We have not been able to identify European information security regulations in place for the issuance of e-passports. The apparent reason for this is that the process of issuing passports is tightly linked to sensitive issues like national sovereignty and national citizenship.

However, there are a number of best practices. Of these, the ICAO Guide for Assessing Security of Handling and Issuance of Travel Documents [46] is the most comprehensive and best suited, as it is designed specifically for the passport issuance processes and procedures. Similar practices are also described in the ETSI TS 101 456 standard [42] and the ISO 27001 [47] and 27002 [43] standards. By looking at these practices (e.g. for the issuance of Qualified Certificates per ETSI TS 101 456) further improvements can be made to the ICAO set of best practices. This has been subject to further study in the interviews and the questionnaire part of the study.

Usage security: The passport's primary use is for border passage. The e-passport will be presented at border control where checks are performed to determine whether it is genuine, valid and belongs to the bearer. Additional checks may be performed on whether the person is allowed to enter the country based on e.g. visa or watch lists, but these are not related to the passport itself. The passport verification can be done by a border guard via visual inspection, by a border guard aided by an inspection system or by an automated border control system which is supervised by a border guard but where the border guard is not directly involved in the actual inspection. When first line border control fails, the passport and its holder will normally proceed to second line border control where more thorough and extensive checks on the e-passport will be performed.

The Schengen area common rules and procedures are described at high level in the Schengen Border Code [41] . The inspection process is described in ICAO Doc 9303 [3]. The chip inspection procedure is described in ICAO Doc 9303 [3] and in BSI TR-03110 [5].

During the course of our study, we have not been able to identify functional specifications or standards for inspection systems. This can be considered a serious gap for the security and interoperability of inspection hardware and software.

The passport also has other usage(s) besides border control. It serves as identification document and may be checked by regular police or in the criminal justice chain. It may be required to open a bank account or start in a new job. At airports it may be used for check-in, boarding, and/or luggage collection.

2.1. *Introduction*

Secure and trusted travel documents are an essential part of international security, as they allow states and international institutions to identify the movement of undesired or dangerous persons. At a national level, both governmental and non-governmental institutions depend on travel documents in order to establish a person's identity as well (e.g. when opening a bank account). A secure travel document is, thus, a significant means against identity fraud.

At the time of this writing, all EU Member States supplement newly issued regular travel documents with an electronically readable chip. Passports with such a chip are called e-passports. The chip contains a copy of all information on the bearer that is printed on the document page of the travel document. The chip is protected by a number of security mechanisms. These are described in a number of international standards and EU regulations. The documentation and security mechanisms are discussed in this Chapter. Although originally intended as an addition to the traditional passport booklet, a number of use cases have emerged in which the chip is the de-facto primary travel document (e.g. in automated border crossing schemes).

An e-passport is, thus, composed of the passport booklet with its physically printed data and physical security (usually anti-forgery) measures, the electronic chip and the security mechanisms and data that are contained within the chip. For the purposes of this document study, however, we will focus on the chip and the security mechanisms and information it contains.

Because of the security importance of the e-passport, there will always be fraudsters who are willing to spend significant resources in order to successfully attack the e-passport, allowing them to assume a false identity. For such an attack to be successful the fraudster will have to compromise the inspection process, the issuance process or the technical security of the e-passport. These are discussed below:

1. *Inspection of the e-passport*

   Inspection is the process by which the document itself is verified for authenticity and validity, as well as its link to the bearer who presents the document for inspection. The authenticity and validity of the e-passport can be established via physical and/or electronic characteristics as well as via a consultation of (inter)national registers. To verify the link between the e-passport and its bearer, usually biometrics is used. A comparison is made between the biometrics stored in the e-passport and biometrics captured during the inspection process.

2. *Issuance of the e-passport*

   Issuance is the process by which an e-passport is issued to the bearer. This process is usually initiated by the (aspirant) bearer, who applies for an e-passport. The process is concluded by either a rejection of the bearer's application or the issuance of a new e-passport to the bearer.

3. *Technical security of the e-passport*

   The technical security of an e-passport is the resistance (or at least the detection of the attack during an inspection) of the e-passport to changes and cloning. This is the traditional way to attack travel documents (e.g. by substituting the photograph), but is increasingly difficult because of the introduction of the security mechanisms in the e-passport.

The technical security measures become increasingly hard to circumvent and have been standardised to a high degree [3,4,5]. Therefore the focus of fraudsters is shifting towards the inspection and issuance procedures. The technical security measures and standards are extensively discussed in Section 2.2 and also in Section 2.3.

The inspection and issuance procedures of e-passports are usually under control of a national government and are, therefore, relatively difficult to subvert. However, a fraudulent person can exploit inherent weaknesses in the implementation of issuance and inspection procedures to pass inspection with an invalid e-passport or obtain an e-passport under a false identity. The issues related to issuance will be addressed in Section 2.4. The issues related to inspection are addressed in Section 2.5 of this document, which focuses on the usage and interoperability of e-passports.

2.2. E-passport documentation

2.2.1. E-passports in Europe

European Council Regulation EC 2252/2004 [1] states in article 1(1) that "passports and travel documents shall include a storage medium which shall contain a facial image. Member States shall also include fingerprints in interoperable formats in the e-passports. The data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data." The Council Regulation also states (3) that "The specifications of the International Civil Aviation Organization (ICAO), and in particular those set out in Document 9303 [3,4] on machine readable travel documents, should be taken into account."

The non-public Commission Decision C(2006) 2909 [2] contains as an Annex public specifications for EU passports. In these specifications, compliance to the BSI Technical Report on Advanced Security Mechanisms for Machine Readable Travel Documents [5] is required. In this BSI document a specific implementation of the Extended Access Control (EAC) security mechanism as mentioned in ICAO 9303 [3, 4] is given. EC 2252/2004 [1]and C(2006) 2909 [2] apply for all EU Member States except the United Kingdom and Ireland and apply also for Iceland, Norway and Switzerland as participants in the Schengen acquis.

The security mechanisms as specified in [3, 4, 5] are described below.

2.2.2. Security mechanisms of e-passports

E-passports come with a number of security mechanisms in order to protect the confidentiality, integrity and authenticity of (the data inside) the e-passport chip. Those mechanisms are introduced in the following sections.

2.2.2.1. Basic Access Control

The Basic Access Control (BAC) mechanism is meant to protect data in the chip against unauthorised reading and against eavesdropping on the contactless communication between the chip and the reader.

To be able to perform BAC, the IS needs access to the optically readable, personalised Machine Readable Zone (MRZ) of the document. The IS needs data from the MRZ, namely the document number, date of birth of the holder, and the expiration date of the document, to derive the symmetric cryptographic keys used in BAC. These keys give access to data in the chip (access control) and ensure the confidentiality (encryption) and integrity (signing) of messages in the contactless communication between IS and the Machine Readable Travel Document (MRTD).

The EU requires BAC for European electronic Machine Readable Passports (e-MRPs) and electronic Machine Readable Travel Documents (e-MRTDs). ICAO has specified BAC internationally as an optional mechanism for e-MRTDs. The consequence is that IS should be able to read both MRTDs that support BAC and those that do not.

All information needed to perform the (optional) Basic Access Control mechanism is present in the document. An IS, thus, does not need access to any external information to execute the Basic Access Control mechanism.

2.2.2.2. Passive Authentication

The Passive Authentication (PA) mechanism is used to verify the integrity of the data in the chip (has the data not been changed) and their authenticity (does the data originate from an official issuing authority). For this, the PA mechanism uses a dedicated public key infrastructure (PKI), also referred to as the “signing PKI”.

The chip contains a logical data structure (LDS), in which data is organised in data groups (DGs). To guarantee the integrity of the DGs, the issuing authority has calculated a hash-value over each DG separately and has placed these hashes in the document Security Object (SOd). The authenticity of these hash-values is guaranteed by a digital signature created by the issuing authority (Document Signer, DS) over the concatenation of the hash-values. Thus, the integrity and authenticity of all data in all data groups is ensured.

When an e-MRTD is offered at border control, the IS calculates the hash-values of each DG it has read and compares them to the hash-values in the SOd. To verify that these hash-values are unchanged and authentic, the IS verifies the signature. A matching signature ensures that the data in the data groups is unchanged and authentic.

To be able to perform PA, an IS needs the certificate of the DS that has created the signature over the data group hashes. This certificate contains the key that is necessary to check the validity of this signature. Usually, this DS certificate can be read from the e-MRTD. Otherwise, the DS certificate must be available from an external source. According to ICAO the preferred first line distribution mechanism for the DS certificate (C_{DS}) is via the ICAO PKD (see Figure 1). ICAO also recommends including the C_{DS} in the SOd on the e-MRTD. This is not a requirement however, probably to prevent a very large storage space requirement on the e-MRTD chip. It may also be more secure to obtain the C_{DS} in principle from an external source. The authenticity of the C_{DS} is guaranteed by the Country Signing Certification Authority (CSCA) of the issuing authority (IA). Therefore, in order to check the C_{DS}, the IS needs the (root) certificate of the corresponding CSCA. This certificate must be available from an external source and will be exchanged bilaterally, i.e. not via the ICAO Public Key Directory.

It is essential for a trustworthy Passive Authentication mechanism to ensure that the inspection infrastructure only contains certificates that are genuine and can be trusted.

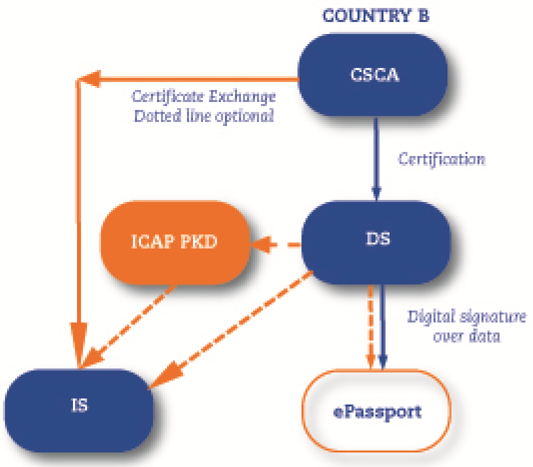


Figure 1 - Signing PKI hierarchy

2.2.2.3. Active Authentication

Active Authentication (AA) enables the IS to distinguish between original and cloned e-MRTDs, by verifying that the electronic data belongs to the physical document and to the physical chip. This mechanism is optional and, therefore, not present in all e-passports.

To verify that the data belongs to the physical document, ICAO requires that the *Machine Readable Zone* (MRZ) is compared to the MRZ data from data group (DG) 1.

To verify that the data belongs to the physical chip, a challenge-response protocol is performed between the chip and the IS. Use is made of the document public key stored in DG 15 and the corresponding private key in the secure part of the chip. The public key is available to the IS, but the private key cannot be read. Only the original e-MRTD has knowledge of this private key. The inspection system sends a challenge to the e-MRTD. The e-MRTD signs this challenge with the private key and sends the response to the IS for inspection. The IS verifies the response by checking the signature with the public key from DG 15. Because of the uniqueness of the key pair, the IS can determine from the signature that the e-MRTD has the correct private key and is, therefore, original.

All information needed to perform the (optional) Active Authentication (AA) mechanism is present in the document. An IS does not require external additional information for AA. The authenticity of the AA public key stored in DG 15 is guaranteed by the PA mechanism.

2.2.2.4. Extended Access Control (EAC)

ICAO advises that access to the more sensitive additional biometric data should be more restricted and states that this can be accomplished in two ways: EAC or data encryption. Although these options are mentioned by ICAO, ICAO does not propose or specify any standards or practices in these areas at this time. ICAO further says that the optional EAC mechanism is similar to the BAC mechanism already described, however, for EAC a document Extended Access key set is used instead of the document Basic Access keys. Defining the (chip-individual) document Extended Access key set is up to the implementing State. The document Extended Access key set may consist of either a symmetric key, e.g. derived from the MRZ and a National Master key, or an asymmetric key pair with a corresponding card verifiable certificate. Extended Access Control requires that the chip of the e-MRTD has processing capabilities.

An EAC-mechanism is described by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik (BSI)) in their Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11 [5]. This EAC mechanism is required by the European Union as an additional security measure for the protection of additional biometric information (fingerprint and iris) stored in the passport. EAC ensures that only IS authorised by the issuing authority of a passport can read that passport's fingerprint or iris information.

EAC adds functionality to establish the authenticity of both e-MRTD and IS. This enables the possibility to only provide access to authorised inspection systems. Besides, EAC provides stronger cryptographic mechanisms for securing the chip-reader communication than BAC.

EAC consists of two parts: Chip Authentication and Terminal Authentication.

EAC – Chip Authentication

The Chip Authentication mechanism is performed to protect the contactless communication between e-MRTD and IS in a better way than BAC does. This is realised by exchanging stronger symmetric keys. The key exchange mechanism is based on asymmetric cryptography, involving private-public key pairs of both the e-MRTD and the IS. Since Chip Authentication uses the private key of the e-MRTD, stored in secure memory, it also implicitly establishes the authenticity of the chip. This mechanism can, therefore, replace AA. The corresponding CA public key is stored in DG 14 and its authenticity is guaranteed by the earlier performed PA. Chip Authentication does not sign a challenge from the inspection system but is used to establish a secure channel between chip and inspection system. Therefore, it does not leave a signature in the inspection system, i.e. a proof that the passport has been used at the inspection system, which enhances the privacy of the passport holder.

All information necessary to perform Chip Authentication is present in the document. An IS does not depend on external additional information.

EAC – Terminal Authentication

The Terminal Authentication (TA) mechanism ensures only authorised terminals can have access to the specially protected biometric data in the e-MRTDs. A public key infrastructure (PKI) for TA, also called "Verifying PKI", is used for this (see section 2.2.2.5). Performing TA consists of two steps:

- The e-MRTD checks the validity of a certificate chain offered by the IS
- The e-MRTD checks whether the IS actually possesses the private key associated with the public key in the IS certificate it received in the first step.

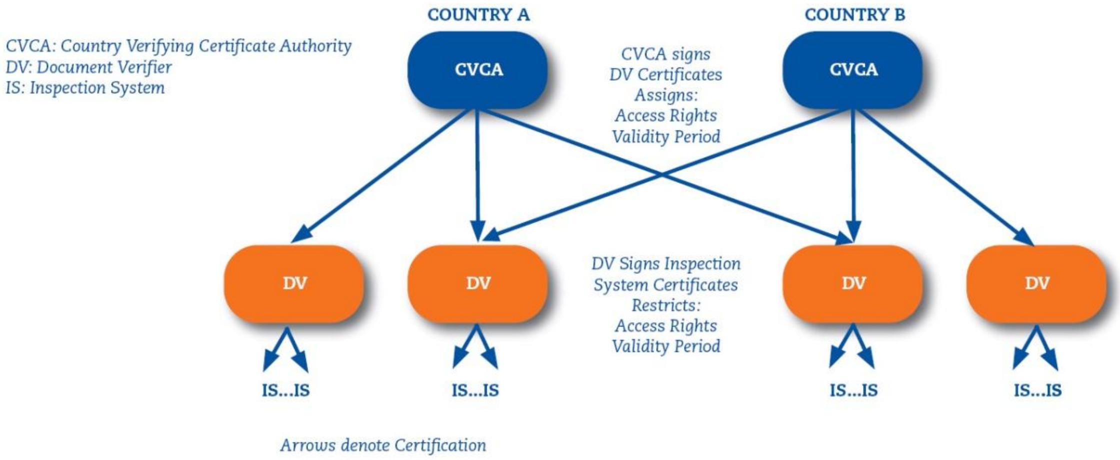


Figure 2 – Verifying PKI hierarchy

The first step of TA consists of the IS offering a certificate chain which is verified by the chip. The certificate chain (see Figure 2) consists of: (1) an IS certificate which is signed by a Document Verifier Certification Authority (DVCA), (2) a DVCA certificate which is signed by the current Country Verifying Certification Authority (CVCA) of the issuing country, (3) the current CVCA certificate of the issuing country and (4) optionally one or more CVCA link certificates. A link certificate is created when the CVCA starts to use a new key pair and is signed with the private key of the previous key pair of the CVCA — thus linking it to the previous key pair and CVCA public key certificate.

The certificate chain is checked against the CVCA trust points stored on the e-MRTD. In the e-MRTD two CVCA (link) certificates can be stored. These certificates are initially placed in the e-MRTD at personalisation. When the e-MRTD is used, the CVCA may have renewed its certificate one or more times. In that case, link certificates are required to link the certificates offered by the IS to the trust point in the e-MRTD. The trust points in the e-MRTD can be updated (replaced) with more recent CVCA link certificates provided these link certificates are received from a trustful source.

The chip will also update the current time it uses to verify the validity of certificates offered during TA. The chip itself has no internal clock. The time it uses is the time it extracts from certificates from trusted sources. It will use as best approximation of the current time the most recent time from which a trusted certificate is valid.

In the verifying certificates, access rights are indicated for reading the extra secured biometric data (DG3: fingerprints and/or DG4: iris). Before the e-MRTD provides access to these biometric data, the IS must prove that the offered IS certificate in fact belongs to the IS. To do this, the IS must prove it has access to the IS private key which belongs to the IS public key in the IS certificate. This is done in the second step of the TA mechanism. If this second step succeeds, the IS has proven that the access rights in the IS certificate were indeed granted to the particular IS.

The second step of TA consists of the IS signing some data known to the e-MRTD chip. The signature over this data will be sent by the IS to the e-MRTD. For creating this signature, the IS must use its private key. The e-MRTD then verifies the signature with the IS public key from the certificate offered in the first step. If this inspection is successful, the e-MRTD will give the IS the access rights to the extra secured biometrics indicated in the certificate chain.

To perform terminal authentication, an IS needs to have certificates issued under the responsibility of the CVCA of the issuing country of the MRTD.

Both the inspection system and e-MRTD are relying parties i.e. they require public keys issued and/or signed by other trusted parties on which they rely to verify the party they are dealing with (see Figure 3). The inspection system relies on the signing PKI and e-MRTD and needs the public keys of CSCA (and DS) to verify an e-MRTD. An inspection system contains several CSCA and DS keys. The e-MRTD relies on the verifying PKI and inspection system and needs the public key of the CVCA to verify the access rights of the inspection system; the e-MRTD only contains two CVCA keys.

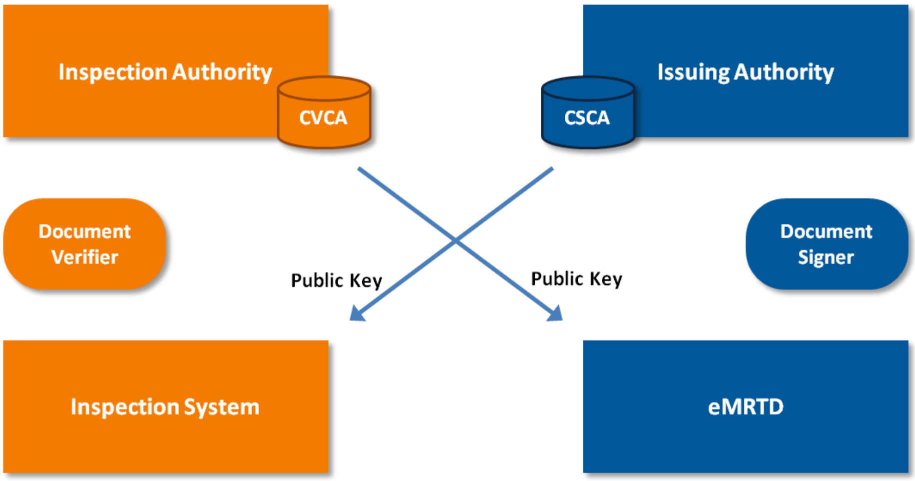


Figure 3 - PKI key distribution

2.2.2.5. Public key infrastructures (PKIs)

Three different PKIs are necessary for inspection of e-passports:

- Country signing PKI for Passive Authentication
- Country verifying PKI for Terminal Authentication
- PKI for communication security

Country signing PKI for Passive Authentication

The Passive Authentication mechanism is used in the inspection procedure of an e-MRTD to verify the integrity and authenticity of the information in the e-MRTD-chip. To perform PA, an IS needs certificates from the country signing PKI of the issuing authority. This can be a foreign authority.

A country signing PKI hierarchy consists of a Country Signing Certification Authority (CSCA) and one or more Document Signers (DS). CSCA en DS reside under the responsibility of the Issuing Authority. DS keys are used for a limited amount of time and sometimes also for a limited number of passports. ICAO recommends a maximum usage time of DS keys of 3 months. Some countries change the signing key after a certain maximum number of passports have been signed with a key even if the maximum usage period has not yet been exceeded. The DS certificates are valid for the usage time of the key pair plus the maximum validity period of the passport, which is normally 5 or 10 years. This means the DS certificates can be valid for a period of 10 years and 3 months.

The public key certificates of foreign signer hierarchies need to be available to the IS to be able to perform PA on foreign e-MRTDs. These foreign public key certificates can be obtained via bilateral exchange or from the ICAO Public Key Directory. CSCA root certificates will only be exchanged bilaterally, not via the ICAO Public Key Directory.

Country verifying PKI for Terminal Authentication

The Terminal Authentication mechanism is used in the inspection procedure of an e-MRTD to get access to the more sensitive biometric information which is protected by Extended Access Control (EAC). To perform TA, an IS needs a public-private key pair and a chain of public key certificates that can be verified by the e-MRTD chip.

A country verifying PKI hierarchy consists of a Country Verifying Certification Authority (CVCA), one or more Document Verifier Certification Authorities (DVCA) and Inspection Systems (IS). The verifying PKI is the responsibility of the verifying authority. To be granted access to extra secured biometric data in national or foreign e-MRTDs the IS requires keys and requires to request public key certificates with the national DVCA.

To grant an IS access to extra secured biometric data in *national* e-MRTDs, a DVCA requests a certificate from the national CVCA. Similarly, to grant an IS access to such data in *foreign* e-MRTDs, a DVCA needs a certificate from a foreign CVCA. The CVCA can restrict the access of the (foreign) document verifier (DV) country by setting only certain attributes in the DVCA certificate.

PKI for communication security

To exchange certificates and certificate requests with other countries, a Single Point of Contact (SPOC) is needed [6]. HTTPS (TLS) is used to secure the communication between the SPOCs. A third PKI is necessary for using the HTTPS mechanism.

Below, we have made an inventory of the recommendations from ICAO document 9303 entitled “Machine Readable Travel Documents” [3] and “EU – Passport Specification of 28/06/2006” [2] on the maximum usage period and validity period of certificates:

	Usage period CSCA (PA)	Usage period Document Signer keys (PA)	CVCA (EAC)	Validity period DVCA (EAC)	Validity period Inspection systems (EAC)
Period	5 years	3 months	3 years	3 months	1 month

Below, we have made an inventory of the recommendations from ICAO document 9303 entitled "Machine Readable Travel Documents" [3] on the minimal cryptographic key lengths by algorithm in bits:

	CSCA (PA)	Document Signer keys (PA)	Active Authentication keys (chip)
Key length	RSA 3072 DSA 3072/256 ECDSA 256	RSA 2048 DSA 2048/224 ECDSA 224	RSA 1024 DSA 1024/160 ECDSA 160

2.2.2.6. Exchange of certificates for document and terminal authentication

ICAO Public Key Directory for Passive Authentication

Authentication of e-passport data with the Passive Authentication mechanism requires the use of Country Signing Certification Authority (CSCA) certificates and Document Signing (DS) certificates. Exchange of CSCA root certificates [3, 4], requires the use of diplomatic channels. DS certificates are usually contained in the e-passport itself. ICAO has set up the ICAO Public Key Directory (ICAO PKD) to facilitate the exchange of DS certificates, CSCA Link Certificates, Certificate Revocation Lists (CRLs) and CSCA Master Lists.

At the time of finalising this report (April 2011) the most recent information about ICAO Member States participating in the ICAO PKD is from 31 January 2011. At this date the ICAO PKD website lists the following ICAO Member States as participating in the ICAO PKD: Australia, Canada, Switzerland, China, France, Germany, India, Japan, Kazakhstan, New Zealand, Singapore, Nigeria, Republic of Korea, United Kingdom, United States of America, Ukraine, Latvia, Czech Republic, Macao (China), United Arab Emirates, Hong Kong (China), Slovakia, Netherlands, Morocco, and Austria. These Member States are represented on the map below which comes from the ICAO website[1] and dates from 15 February 2011:

[1] http://www2.icao.int/en/MRTD/Downloads/PKD%20Documents/PKD%20World%20Map.bmp

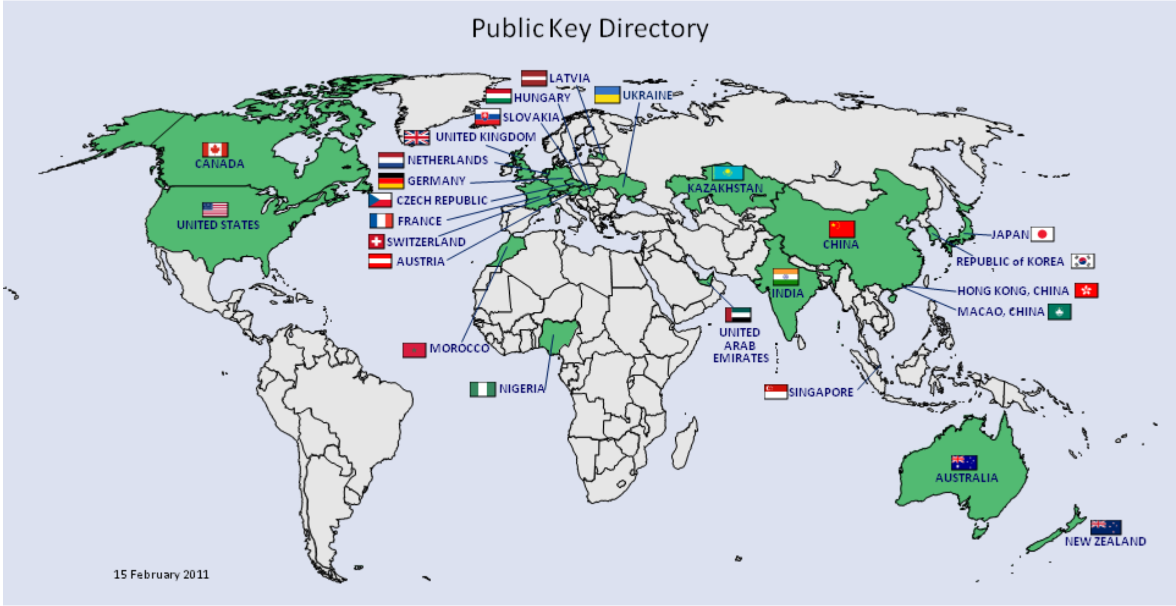


Figure 4 - ICAO PKD member states per April 2011

At the time of writing the final version of this report (26 April 2011), only 12 of these 25 states, namely New Zealand, Australia, the United States, Germany, France, Japan, the United Kingdom, Canada, Republic of Korea, Singapore, Switzerland, and the Czech Republic actually entered information in the PKD. A country has to be a paying member of the ICAO PKD to be able to place certificates in the directory. Reading information from the ICAO PKD is also possible for non-Member States.

The basis for the ICAO PKD lies in the PKD Memorandum of Understanding (MoU) [33]. The ICAO PKD is governed by the PKD Board, which determines a range of operational procedures [33].

Single Point of Contact (SPOC) for Terminal Authentication

Authentication of reader terminals before access is granted to additionally protected biometrics (fingerprint/ iris) requires regular exchange of certificate requests and certificates between Member States. Certificate requests and certificates conforming to [5] can be exchanged through a Single Point of Contact (SPOC), using the SPOC Web Service interface specified in the CVCA key management protocol for SPOC [6].

In the infrastructure outlined below, a Member State can send a certificate request from its Document Verifier (DV) via its domestic SPOC and a foreign SPOC to the CVCA of another Member State. If this request is accepted, the foreign CVCA can create a DV certificate, and send it via its SPOC and the SPOC of the requesting state to the DV that originated the request (see Figure 5).

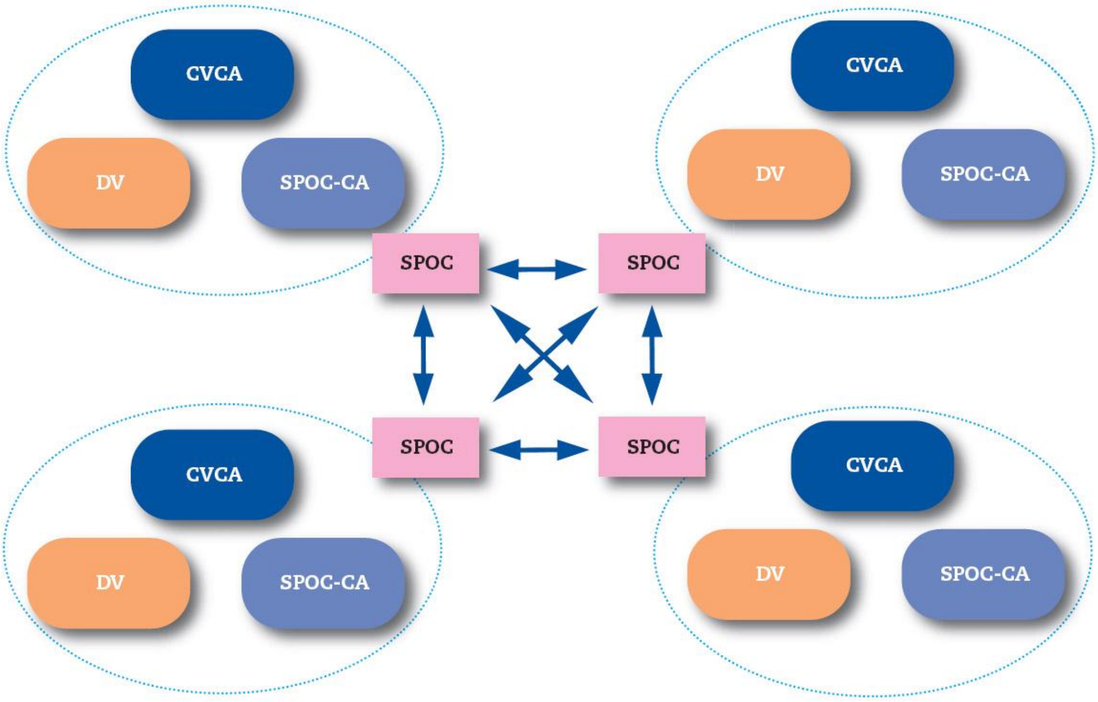


Figure 5 - SPOC representation

2.3. *Technical security of e-passports*

In this chapter we will explore the technical security issues of e-passports in the context of border security. First, the available literature will be discussed, followed by an analysis of relevant security objectives and issues for e-passports in the context of border security. Finally, some conclusions are presented.

2.3.1. Documentation

This section contains references to documentation, focusing on documentation relevant to the technical security issues. To consider the technical security issues with e-passports we found it useful to introduce an ad hoc classification in the following categories:

1. Security issues with the passport chip itself, i.e. the hardware and software implementing the ICAO and additional EU standards;

2. Security issues with the ICAO and additional EU standards;

3. Security issues with the passport inspection procedure, as implemented in inspection systems (ISs), and the management of the associated PKI infrastructure.

The first category is the focus of protection profiles for e-passports. Especially the second category has received broad attention in the wider security research community. (As noted above, the considerable body of research that does exist focuses mainly on questions regarding the privacy of user data. The amount of literature dealing with the authenticity and availability of passport data is severely limited.) The last category mainly concerns usage and operational issues.

2.3.1.1. Official specifications

The primary sources of documentation are the passport specifications themselves:

- Doc 9303 [7] and its supplement [8] define the basic behaviour of the passport and associated security protocols: Passive Authentication, Basic Access Control, Active Authentication.

- EAC documentation [9] defines the behaviour with respect to Extended Access Control, an advanced security mechanism to protect highly sensitive data on the passports (i.e. fingerprints and iris scans).

- The new Supplemental Access Control (SAC) specifications, designed to replace BAC in the longer run.

There is no official standard which specifies SAC yet, only preliminary technical reports by the Technical Advisory Group on Machine Readable Travel Document (TAG-MRTD). The mechanism is presented in [10, 11].

Additional information from ICAO, including reports of the Technical Advisory Group on Machine Readable Travel Document (TAG-MRTD), is available online at http://www2.icao.int/en/mrtd/

2.3.1.2. Protection profiles

Common Criteria protection profiles provide comprehensive accounts of the security requirements and the assurance requirements for e-passports, including their rationale:

- Common Criteria Protection Profile, Machine Readable Travel Document with ICAO Application, Basic Access Control, BSI-CC-PP-0055, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.10, 25th March 2009, available from http://www.commoncriteriaportal.org/files/ppfiles/pp0055b.pdf

- Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application", Extended Access Control BSI-PP-0026, Version 1.2, 19th November 2007, Bundesamt für Sicherheit in der Informationstechnik (BSI), available from http://www.commoncriteriaportal.org/files/ppfiles/pp0056b.pdf

- Protection Profile for Machine Readable Travel Document SAC (PACE) Supplemental Access Control, Reference PP-MRTD-SAC/PACE, Version 0.83, Agence Nationale de la sécurité des systémes d'information (ANSSI), available from http://www.gixel.fr/includes/cms/contenus/bibliotheque/file/CAP%20/PP MRTD-PACE 083.pdf

2.3.1.3. Scientific literature and other studies in open domain

As a high-profile application, the e-passport has attracted a lot of interest among scientific researchers, security enthusiasts, and privacy advocates. This led to a considerable amount of security public review, aided/enabled by the openness of the standards and easy access to actual e-passports. This information is in the public domain as research papers [12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26] and websites[2][3][4]. Some of these papers provide a general security analysis

[2] http://www.dexlab.nl/epassports.html

of the e-passport specification, some highlight more specific weaknesses. It is important to note that nearly all of the work above focuses on privacy issues: while this is a prime concern for the passport holder, it has little impact on border security.

Most of this material is related to (aspects of) e-passport specifications, though there is some work considering actual passports and passport inspections systems. One specific outcome of this public scrutiny seems to have been the introduction of SAC as an improved replacement for BAC. Also, it has highlighted the need for randomised numbering of passports, as handing out sequential numbers substantially reduces the MRZ key space which is in use for BAC[5].

E-passport specifications

- [19, 20] specifically look at the downside of using digitally signed data, namely the transferability of such evidence.

- [37] discusses how the weak certificate management combined with relatively long validity periods of passports enables forging passports when e.g. old certificates and their signing keys are not properly discarded and are leaked. In this scenario, even though such certificates are revoked it is still possible to produce and sign passports with a retrospective issue date. The same paper also briefly discusses other weaknesses in passport protocols related to holder privacy.

- [21, 22] aim to clarify the passport security protocols, which should help in understanding proper inspection procedures for e-passports. [23] provides a brief but good overview of passport inspection procedures, also mentioning EAC-related PKD issues.

- http://www.mrtdanalysis.org considers possible weaknesses and attack scenarios on e-passports. [38] gives an analysis of the strength of BAC, in the light of the entropy in the MRZ and the evolving computer power to crack it.

E-passport implementations

There has been some research into actual e-passport implementations:

- Several researchers have observed that the total possible number of distinctive BAC keys (part of the MRZ) is so low that brute force attacks are feasible, e.g. [6]. In particular, this is the case when passport numbers are handed out in sequence, a policy which some countries (e.g. the Netherlands) have since abandoned. In particular [17] discussed how hardware devices can be used to speed up the process of brute force attacks on BAC keys.

- [24] analyses security of the first generation Belgian e-passports. The authors consider attacks on BAC given the low entropy in the BAC keys (as mentioned above), but also discovered that the first generation of Belgian e-passports do not implement BAC at all and allow easy access to all the data without BAC.

[3] http://rowlandwatkins.com/past/2008/8/8/ - “On exploiting e-passport vulnerabilities”

[4] http://www.wired.com/politics/security/news/2007/08/epassport

[5] When sequential numbers are handed out, the key space which is in use is the total number of handed out e-passports for a

- [25] discusses a minor privacy problem caused by implementation-specific error codes leaking information prior to BAC.

- [26] presents a new timing attack on some implementations of BAC that enables tracking of a passport after once performing a BAC session with it (or eavesdropping one session and brute forcing the BAC protection).

Inspection procedure, including Public Key Directory management

From the border control point of view, a large part of e-passport security lies in the proper inspection of the electronic passport data. The passport specifications [3] provide means to perform such checks, but no clear recipe on which exact checks should be mandatory to ensure that full security is provided. For example, since Active Authentication is not mandatory, some inspection systems may choose not to perform Active Authentication inspection at all, effectively leaving passport chip cloning undetectable.

Yet another issue during passport inspection is access to trusted certificates [27] to check digital signatures of the passport data. Here again, the specifications provide protocols to perform such checks, but it is not very clear what exactly should happen if the required country signing certificates cannot be found in the Public Key Directory (PKD). Here again, an inspection terminal that chooses to leave a document signature unverified is open to accept forged passports.

There has been some research into the inspection procedure for e-passports:

- http://www.dexlab.nl/epassports.html highlighted that the inspection of digital signatures on e-passports is a non-trivial procedure.

- http://rowlandwatkins.com/past/2008/8/8/, an article entitled “on exploiting e-passport vulnerabilities”, considers hypothetical attacks on the PKD infrastructure, such as social engineering attacks to included forged certificates. One researcher reported finding buffer overflow weaknesses in two commercial e-passport reading applications (presented at DEFCON 15, August 2007).
  http://www.wired.com/politics/security/news/2007/08/epassport

We would like to note that we consider some of the above media coverage overrating the importance of the presented findings. For one, failure of one particular inspection system to properly check the chain of signatures and accept a forged passport should not be generalised to all inspection systems and procedures. It does, however, underline the importance of a proper inspection procedure (and, hence, the system) to be in place to avoid such problems.

Secondly, many articles stating the possibility to clone passports [39] do not try to describe the practical consequences of cloning. In our opinion it is relatively limited:

- Any change in the data on a cloned passport is easy to detect, as Passive Authentication will immediately reveal data has been altered.

- Clones of passports that were originally issued with Active Authentication or Chip Authentication are also very easy to detect as clones, given that any such clones will fail AA or CA checks.

- An exact clone of a passport that does not support AA or CA is indeed undetectable by means of purely electronic checks. But it still contains valid data properly signed by the issuing country. In such case the emphasis should be on (a) verifying that the chip belongs to the passport booklet and (b) the biometric data stored on the passport indeed belongs to the passport holder.

From the point of view of border security, only the last point deserves special attention. Here, lookalike fraud might be possible, especially for automatic border control systems. In particular, checks whether the booklet matches the chip are not sufficiently strong (e.g. the picture printed in booklet is not checked against the picture stored in the chip) a passport with a non-matching chip cloned from another passport may be accepted.

Biometrics

[28] provides some insights in the passport issuance process, more specifically results of experiments with taking and checking biometrics (face and finger) in larger e-passport trial in the Netherlands.

2.3.2. *Security objectives*

Given the objectives of the Frontex study, as discussed with Frontex, the issues of interest are primarily

(**Auth**) authenticity/integrity of the e-passport

(**Avail**) availability of the e-passport

as these aspects are vital to secure border controls. Regarding integrity, a distinction can be made between

(**Auth-data**) authenticity/integrity of the e-passport data

(**Auth-book**) authenticity/integrity of the e-passport itself

E.g. cloning a passport would violate (**Auth-book**), but not (**Auth-data**). For (**Auth-book**) one can further distinguish:

i. authenticity of e-passport chip,

ii. authenticity of the passport booklet, and

iii. that the two belong together.

Other security objectives are

(**Priv**) confidentiality/privacy, where one can further distinguish

(**Priv-Conf**) confidentiality of the passport data,

(**Priv-Track**) (un)traceability of individual passports, also known as tracking.

These objectives can be considered as secondary for the purpose of this report, since these do not directly impact the security of border controls. However, it should be noted that

- these issues are very important for the wider (public) acceptance of using electronic passports;

- a lack of confidentiality of passport data may provide information that can be used to harm border control security, for example by increasing possibilities for spoofing or faking passports;

- measures for improving confidentiality often introduce additional operational processes and procedures, and can therefore be detrimental to availability (e.g. due to the BAC protection mechanism, OCR errors when reading the MRZ could result in the border guard not being able to access the e-passport data).

Much of the public attention surrounding e-passports, and indeed (scientific) research into e-passport security, has focused on the issues of confidentiality and privacy. Derived security objectives, given the security mechanisms of the e-passport (discussed below), include:

- the confidentiality of the e-passport private key for AA;

- the confidentiality and integrity of the MRZ data needed to access the chip via the BAC mechanism;

- the confidentiality of private keys underlying the PKI infrastructures;

- the integrity of the associated public keys in the PKI infrastructures.

2.3.3. Conclusions

When it comes to border security, i.e. correctly establishing the passport bearer's identity at border control, as opposed to privacy, we have identified the following:

- Nearly all of the available literature on e-passport concerns privacy, rather than the border security.

- Passive Authentication is by far the most important mechanism to prevent changing the information in the e-passport.

- Weaknesses in the e-passport itself (the smartcard hardware or the software) can hardly impact border security, given that they do not impact the Passive Authentication mechanism unless lookalike fraud with cloned passport chips is considered a threat.

- Active Authentication only makes a very small contribution to border security, proving authenticity of the chip that carries the (digitally signed) information. The Chip Authentication part of Extended Access Control does the same.

- Except for Basic Access Control tying the chip to the physical passport booklet, BAC seems irrelevant for ensuring the availability and authenticity of the passport (data). Given that quality and interoperability issues with BAC might result in border guards being unable to access the e-passport data, BAC provides little benefit for border security[6]. The same applies to the Terminal Authentication part of EAC.

- Except for AA, the e-passport does not contain any security critical private keys. As a result, the Common Criteria certification of the security mechanisms in e-passport chips is not essential in the context of border security. It is, however, relevant to safeguard the privacy of e-passport holders.

- Stealing of passports is much more of an issue than stealing of card inspection systems or the Extended Access Control terminal keys these contain.

Overall, the most important issue for securing border control with respect to e-passports appears to be a solid verification procedure for e-passports. As the literature shows, weak verification procedures may accept forged or cloned passports. We believe that existence of weak verification systems is caused by the lack of a thorough specification tying all components of the verification process: physical checks, electronic checks, and biometric checks. Perhaps the Frontex report on guidelines and best practices for Automated Border Control systems [40] should be generalised to all e-passport verification procedures and systems.

[6] BAC and TA provide privacy benefits for e-passport holders and thus also facilitate the actual existence of e-passports, as without it e-passports might have been banned for privacy reasons.

2.4. *Issuance security of e-passports*

Because of higher technical security of e-passports, the importance of secure issuance procedures is increasing in the combat against identity fraud. In this section, we will investigate existing European Commission decisions and regulations, as well as relevant security issues and best practices on the issuance process.

2.4.1. *European regulation of the issuance process*

The issuance of e-passports is performed under coordination and control of a national government. Although travel documents can be issued to non-nationals of a country, the e-passport is usually only issued to country nationals. Although the technical specification of the e-passport is harmonised for the EU Member States via the ICAO Doc 9303, parts 1 and 3 [3 and 4] and Technical Guideline TR-03110 [5], the issuance procedure and entitlement criteria for an e-passport is regulated at a national level only and not in the remit of European Council decision C(2006) 2909 [2], regulating the technical security of e-passports within Europe.

So far, European harmonisation and regulation of issuance procedures (and especially entitlement criteria) has found little political support. Harmonisation is deemed to have a too strong impact on the sovereignty of a Member State. This is true especially for harmonisation of entitlement criteria, as they are usually linked to the criteria for citizenship of a country. In contrast to this, in the area of issuance procedures for Qualified Certificates there is active European regulation, via the European Parliament Directive 1999/93/EC [29] This difference might be explained by the fact that in the case of electronic signatures, the citizenship of an applicant is not relevant for the entitlement decision.

Harmonisation and regulation can promote the ability for border guards to effectively monitor the external Schengen border, as it can improve the border check effectiveness. A first step in this process is taken by the publication of *"Guide for Assessing Security of Handling and Issuance of Travel Documents"*. The latest version (3.4) of this Guide was released by ICAO in January 2010. It provides guidance and best practices on controls within the issuance procedure, as well as a self-assessment methodology. However, (as with any of the other recommendations) it has not been adopted as formal regulation and remains a set of good practices to date.

2.4.2. *Security issues identified in literature*

An e-passport for a false identity is a valuable tool for fraudsters. Therefore, there are constant attacks on the issuance process. In this section, we discuss a number of threat scenarios that are identified in literature, as well as currently available controls and best practices.

2.4.2.1. Threat scenarios

In [30] a number of threat scenarios are listed which are relevant for the issuance of travel documents. The scenarios relevant for the issuance of e-passports are listed below:

a. Applying for an e-passport under a false identity with genuine evidence, improperly obtained from another individual.

b. Applying for an e-passport under a false identity, using manufactured evidence.

c. Using a (falsely declared) lost/stolen e-passport of someone who resembles the bearer (lookalike fraud).

d. Apply for an e-passport with the intention of selling it to someone who resembles the bearer (lookalike fraud support).

e. Rely on TDIA staff to issue an e-passport outside the regular procedure.

Furthermore, an important aspect of the issuance process, although not strictly focused on security, is that it should be (and in practice is) a high-quality process, consistently producing e-passports compliant to international standards.

2.4.2.2.Controls/best practices

In order to be able to combat the threats for e-passport issuance, the issuing authority should implement a comprehensive set of internal controls, aimed at securing the issuance process. A set of controls have been defined for this by several organisations, which we will discuss here.

ICAO Guide for Assessing Security of Handling and Issuance of Travel Documents

The ICAO Guide identifies a large number of best practices in order to improve the security of the issuance process and is the most comprehensive single list of best practices we have identified. For a full overview of best practices we would like to refer to the Guide itself. Here, we will give an overview of the focus areas of these best practices:

1. Security organisation of the issuance function.
2. Reliance on partners in various stages of the issuance function.
3. First application versus renewal.
4. Lost and/or stolen travel documents.
5. Usage of relevant trusted registers and database in the entitlement decision.
6. Capturing biometrics (photo + fingerprint).
7. Documentary evidence of application (which “breeder” documents and inspection procedure).
8. Audit trail of (generic/personalised) components.
9. Quality of personalisation.
10. Delivery to passport holder.
11. Usage of approved chips and booklets.
12. Physical security of facilities.
13. IT security.

14. Personnel security.

15. Issuance abroad.

16. Quality control on the issuance process as a whole.

ETSI TS 101 456

A standard that can also provide some guidance is ETSI TS 101 456 [42], which is the standard produced by the European Telecommunications Standards Institute (ETSI) specifying the requirements with which Certificate Authorities have to comply in order to issue Qualified Certificates. Qualified Certificates can be used by natural persons for legally binding digital signatures in line with the European Parliament Directive 1999/93/EC [29]. In practice, this is achieved by issuing a smartcard to a person, which allows the person to digitally sign documents (such as e-mails, contracts, invoices, etc). Although providing requirements on similar subjects as the ICAO Guide, ETSI TS 101 456 [42] puts emphasis on building an audit trail and archive of registration (i.e. entitlement) decisions. It might be considered to adopt this standard also for the entitlement decision for electronic passports, as it will allow better auditing of the entitlement decisions and investigation of any prevalent incidents. The construction of an audit trail is also in line with the recommendations of the 2007 US GAO report “BORDER SECURITY; Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use” [31].

ISO/IEC 27001 & 27002

Part of the internationally widely used 27000 series of information security standards, ISO/IEC 27002 [43] provides a large number of controls which can be implemented in order to increase the security of an organisation. As it targets any organisation, it is not specific for the issues and threats related to the issuance of e-passports, but can be used to complement the controls defined in the ICAO guide. Especially, controls which are not directly related to the issuance process (like personnel security, IT security, etc) can be adopted.

The ISO 27000 series also include ISO 27001 [47] which describes a management system for information security, based on risk assessment and treatment. This effectively describes a method to select controls from ISO 27002, to implement them, to check on them and to act on the results.

2.4.3. Conclusions

Fraudsters of passports will typically exploit the weakest link in the issuance and usage processes or in the technical security of the passport. The technical security of the (electronic) passport is considered to be the highest ever in history, implying that the weakest link is shifting from document fraud to fraud in the issuance process and lookalike fraud. This shift is illustrated by the figures in [32]. Furthermore, it is expected that biometrics in e-passports will help to reduce lookalike fraud, implying that the focus of fraudsters will be the issuance process. Exploited vulnerabilities in this process could be TDIA staff errors, TDIA staff fraud and flaws in operational security.

Unlike for the issuance of qualified certificates, used for creating electronic signatures, there is no European information security regulation in place for the issuance of e-passports, as this is tightly linked to national citizenship. However, there are a number of best practices.

Of these, the ICAO guide is the most comprehensive and best suited as is was targeted specifically at the issuance procedure. Other such practices are described in the ETSI TS 101 456 standard and the ISO 27001 and 27002 standards. By looking at best practices for similar issuance processes, as in the issuance of Qualified Certificates, further improvements can be made. This has been subject to further study in the interviews and the questionnaire part of the study.

2.5. *Usage security and interoperability of e-passports*

2.5.1. E-passport usage

2.5.1.1. Usage at border control

The Schengen Borders Code EC 562/2006 [41] "establishes rules governing border control of persons crossing the external borders of the Member States of the European Union". Chapter II, Article 7, paragraph 2 states

"All persons shall undergo a minimum check in order to establish their identities on the basis of the production or presentation of their travel documents. Such a minimum check shall consist of a rapid and straightforward verification, where appropriate by using technical devices and by consulting, in the relevant databases, information exclusively on stolen, misappropriated, lost and invalidated documents, of the validity of the document authorising the legitimate holder to cross the border and of the presence of signs of falsification or counterfeiting.

The minimum check referred to in the first subparagraph shall be the rule for persons enjoying the Community right of free movement."

On third country nationals thorough checks shall be performed on entry and exit which are described in Chapter 2, Article 7, paragraph 3 of the Schengen Borders Code [41]. In this paragraph a "second line check" is mentioned which is defined in [41] as ""Second line check" means a further check which may be carried out in a special location away from the location at which all persons are checked (first line)."

Although the Schengen Borders Code [41] does not mention a "second line" check for persons enjoying the Community right of free movement, second line checks are not limited to third-country nationals. Border control processes outlined in the Frontex ABC best practice guidelines [40] demonstrate that Member States may also perform a second line check on passengers enjoying the Community right of free movement. Similarly, the Schengen Handbook [49] does not differentiate in its best practice recommendation that thorough checks "should be performed in the second line of control" "when there is a suspicion that a travel document (...) has been forged". Member States take into account the possibility that someone, either a third country national or a person enjoying the Community right of free movement, tries to use a falsified or counterfeited travel document.

At border control, inspection systems may be used as the "technical devices" mentioned in [41] to support the border guard. The Frontex ABC best practice guidelines [40] emphasises the facilitation function of automated border control/inspection systems (for persons enjoying the Community right of free movement) for the "minimum check [which] shall consist of a rapid and straightforward verification, where appropriate by using technical devices" [41]. Some Member States are working on, implementing or have already implemented at certain locations automated border control to that effect.

This means that border control at the external borders for persons enjoying the Community right of free movement in practice takes place in one of the following ways (which was confirmed in the interviews, questionnaire results and workshop):

- First line visual inspection (booklet) only by border guard
- First line inspection of booklet and chip by border guard in combination with an inspection system. Regarding biometric verification one or more of the following options can be performed. At least one of the facial verifications is performed:
    - Visual biometric comparison by border control guard of facial image from chip and/or data page with passport holder

      and/or
    - Automated biometric comparison of facial image

      and optionally
    - Automated biometric comparison of secondary biometric
- Second line visual inspection (booklet) only by border guard
- Second line inspection of booklet and chip by border guard in combination with an inspection system
- Automated border control (first line)
    - Only facial image
    - Facial image and secondary biometric.

2.5.1.2. Other uses of e-passports

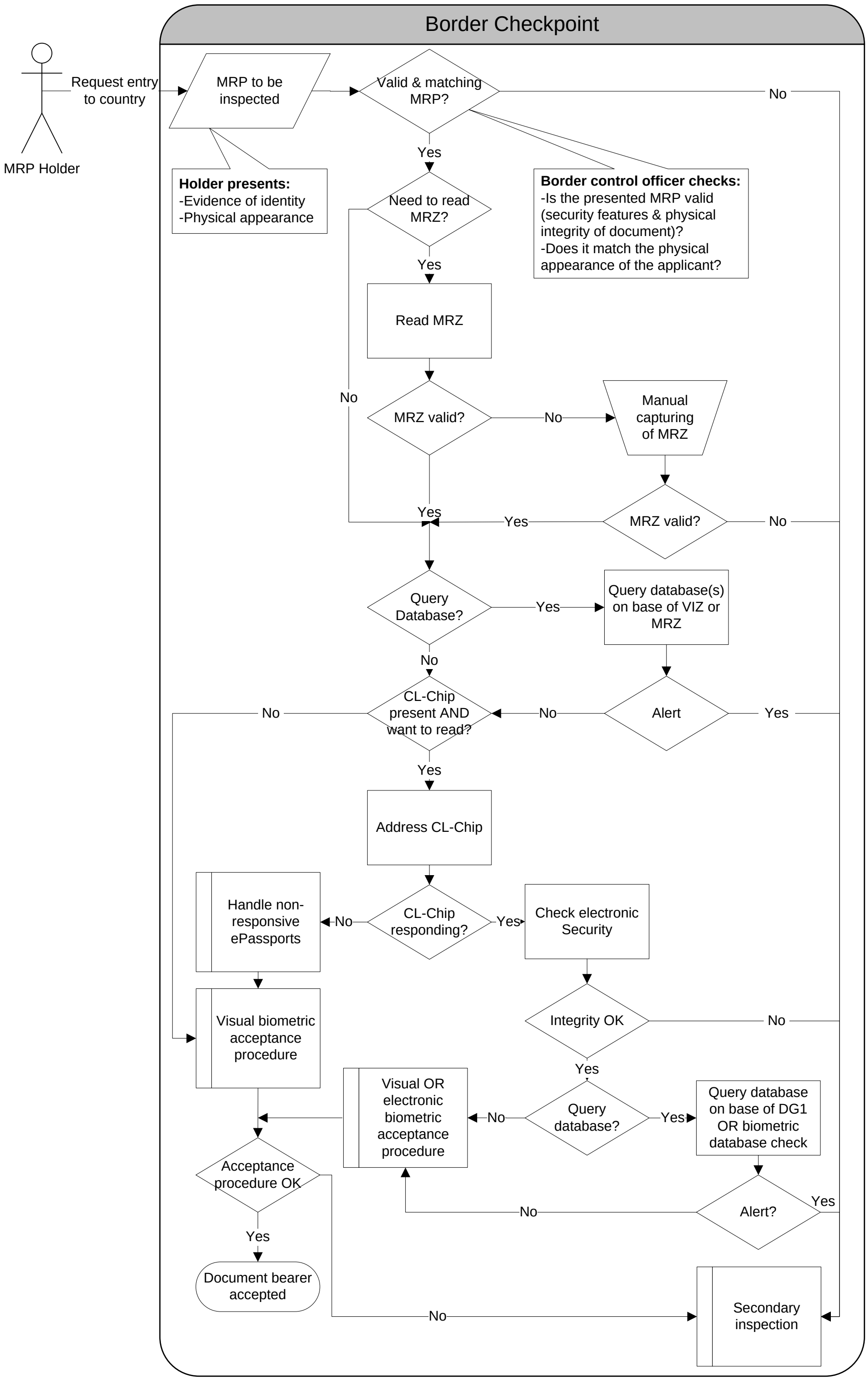
In addition to border passage, the passport is also used at other occasions. It serves as identification document and may be checked by regular police or in the criminal justice chain. Since establishing the identity of the holder is very important in these cases as well, verifying organisations may want to read and verify the chip. Therefore, they will also need inspection systems with underlying infrastructure. They will need their own access to signer certificates to verify the chip data. If these parties want to read the fingerprints from the chips, they need their own verifying certificate chain.

A passport or other official identification document may also be required when opening a new bank account or starting in a new job. Although it may not happen in the near future, it can be anticipated that in time these parties will also want to use the e-passport chip.

At airports, the passport is already used for check-in, boarding, and/or luggage collection. Optical reading of the MRZ is done at some places. In the future it may be the chip which is read. In that case the airline will also need access to signer certificates and probably their own verifying certificate chain.

2.5.2. Inspection procedure

ICAO Doc 9303 Part 1 Volume 2, section II-16 [3] gives the flow chart for reading eMRPs (see Diagram 1). The first process is the manual inspection of the passport by the border guard. The border guard performs a preliminary verification of the document holder and checks the physical security features and integrity of the document. Reading of the MRZ, checking against databases and reading the chip are all optional. If the chip is not read, a visual biometric acceptance procedure is performed. If the chip is read, checking the electronic security is described in ICAO Doc 9303 Part 1 Volume 2, section IV [3].



Border Checkpoint
Request entry to country
MRP Holder
MRP to be inspected
Holder presents:
-Evidence of identity
-Physical appearance
Valid & matching MRP?
No
Yes
Border control officer checks:
-Is the presented MRP valid (security features & physical integrity of document)?
-Does it match the physical appearance of the applicant?
Need to read MRZ?
Yes
Read MRZ
No
MRZ valid?
No
Manual capturing of MRZ
MRZ valid?
Yes
Yes
No
Query Database?
Yes
Query database(s) on base of VIZ or MRZ
No
CL-Chip present AND want to read?
No
No
Alert
Yes
Yes
Address CL-Chip
Handle non-responsive ePassports
No
CL-Chip responding?
Yes
Check electronic Security
Visual biometric acceptance procedure
Integrity OK
No
Yes
Visual OR electronic biometric acceptance procedure
No
Query database?
Yes
Query database on base of DG1 OR biometric database check
Acceptance procedure OK
No
Alert?
Yes
Yes
Document bearer accepted
No
Secondary inspection

Diagram 1 - ICAO inspection procedure

ICAO touches on inspection of e-MRPs in ICAO Doc 9303 Part 1 Volume 2, section IV-6 and IV-7.2 [3]. ICAO only requires Passive Authentication to be performed. For PA, both the C_{CSCA} and C_{DS} of each participating issuing state shall be stored in the inspection system. If the inspection system supports BAC or AA, it shall comply with the ICAO Doc 9303 specifications of these mechanisms.

The flow of the inspection process steps (both required and optional) in order of occurrence is described in ICAO as:

1. BAC (optional)

2. PA (completely, including calculating hashes over DGs) (required)

3. AA (optional)

    a. Comparison of MRZs

    b. Use of e-MRP key pair for AA

4. EAC (optional) mechanism not described

5. Decryption (optional) mechanism not described.

Verification of all other security features, like comparing the conventional MRC (OCR-B) and chip-based MRZ (LDS), Active Authentication, Basic Access Control, Extended Access Control and Data Encryption, are optional.

BSI describes in Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11 [9] two slightly different inspection procedures. The standard inspection procedure is for ICAO compliant documents which do not support EAC and/or for terminals which do not support EAC. The advanced inspection procedure can be used by terminals which support EAC on documents which also support EAC.

The standard inspection procedure consists of the following steps, provided the e-MRP supports the security mechanisms:

1. Select e-passport application

2. Basic Access Control
   Required if BAC is enforced by the MRTD chip
   Starts Secure Messaging
   Grants access to less sensitive data (DG1, DG2, DG14 and DG15 and SOd)

3. Passive Authentication (started): signature of SOd is verified, including certificate validation

4. Active Authentication

5. Read and authenticate data
   Finish PA: Hash values of data groups are compared to those in SOd.

The advanced inspection procedure consists of the following steps:

1. Select e-passport application

2. Basic Access Control
   Starts Secure Messaging
   Grants access to less sensitive data (DG1, DG2, DG14, DG15 and SOd)

3. Chip Authentication
   Restarts Secure Messaging

4. Passive Authentication (started): signature of SOd is verified, including certificate validation

5. Active Authentication (optional)

6. Terminal Authentication
   Grants access to more sensitive data (DG3, DG4)

7. Read and authenticate
   Finish PA: Hash values of data groups are compared to those in SOd.

In the advanced inspection procedure, Active Authentication is optional since Chip Authentication is performed, which also guarantees the authenticity of the chip.

2.5.3. Inspection systems

The inspection system fulfils an important role in the inspection process. However, we have not been able to identify official requirements or standards for inspection systems. The inspection processes as discussed in the previous paragraph do not put requirements on the inspection system itself. Similar as for e-passports, there should be functional specifications and protection profiles for inspection systems. This can be considered a serious lacuna and forms a threat to security and interoperability.

2.5.4. Security issues

In the past, the main focus has been on the documents. The use and inspection of the documents has not yet obtained a lot of attention so we have not been able to identify documentation regarding this subject. Vulnerabilities, threats and risks are derived on basis of the e-passport life cycle description in Chapter 4. Here, we already mention a number of risks as we have derived from the inspection procedure described in Section 2.5.2 based on ICAO Doc 9303 Part 1 Volume 2, section II-16 [3] and the BSI Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11 [9].

Inspection system

- Since e-passports with a non-functioning chip are still valid according to ICAO Doc 9303 part 1 volume 2 section IV paragraph 2.6 [3], disabling the chip may be a way to make falsification easier, not placing a chip makes counterfeit easier. This may be useful if the attacker was only able to forge the booklet or to alter the data page. If the non-functioning of the chip is accepted at border control and will result only in first line visual inspection of the e-passport, this may help the attacker.

  Countermeasure: If the cover of the passport indicates a chip should be present or the combination of issuing date and issuing country indicates a chip should be present, the inability to read the chip at first line border control should lead to thorough inspection at second line border control in which it is also checked that a chip is present at the correct place. When the chip is checked at first line border control and turns out to be broken, the passport should go to second line inspection. Only relying on the first line inspection of the booklet in case of a non-functioning chip could advance fraud.

- The chips in a large number of passports have been deliberately disabled.
  Because of the extra workload, this will provide at border control, especially when normally ABC systems are used, the checking will be less thorough.

  Countermeasure: Extra personnel.

- The inspection systems are disabled e.g. via a power shutdown or by disturbing the communication between inspection systems and passports. This may be useful if the attacker was only able to forge the booklet or to alter the data page. Because of the extra workload this will provide at border control, especially when normally ABC systems are used, the checking will be less thorough.

  Countermeasure: Power supply backup, extra personnel.

- An Automated Border Control system may be easier to trick since there is no visual inspection of the booklet (only the chip needs to be copied/counterfeited) and limited control on offering falsified biometric characteristics.

  Countermeasure: Good supervision on ABC systems or inspection by border guard.

- The original chip in the passport has been disabled and replaced by another chip. This may be a chip from another passport or a counterfeit. This will only work if the chip will pass the checks performed by the inspection system.

  Countermeasures: Good implementation of the inspection system with all security mechanisms implemented.

- The inspection system has been tampered with in such a way (e.g. by loading new software) that a positive result is returned for all passports.

  Countermeasure: Make inspection system tamper resistant and tamper evident. If software updating is possible, secure it with good procedural and technical measures.

- The attacker has knowledge of the defect list which indicates defects or flaws in certain groups of passports. If a specific defect means that the inspection system ignores for this group of passports the outcome of a certain check, this is valuable information for fraudsters. A passport which passes in this way may be easier to counterfeit/alter.

Countermeasure: Refer all passports with a defect that diminishes the security to second line inspection.

Basic Access Control

- According to ICAO Doc 9303, [3] BAC is not mandatory. In Europe it is mandatory according to Commission Decision C(2006) 2909 [2], but there still will be valid European passports in circulation without BAC till 2016. Inspection systems may be programmed in such a way that they accept e-passports without BAC. An attacker who has forged a chip may make an implementation without BAC.

  Countermeasure: The inspection system should know which combinations of issuing countries and issuing dates should support BAC and check on its presence.

Passive Authentication

- An invalid CSCA key certificate is inserted in an inspection system which will allow an e-passport with a fake chip with a self-produced DS certificate under the CSCA and self-signed DS data to pass the Passive Authentication procedure at the inspection system. Since PA is the only mandatory security mechanism, the inspection system may be programmed in such a way that it accepts the absence of other security mechanisms. In that case, this will be enough to pass the electronic inspection.

  Countermeasure: Implement technical and procedural measures to prevent unauthorised certificate insertion.

- An invalid CSCA key certificate inserted in the central repository will allow passports with a fake chip with self-produced DS certificates under the CSCA and self-signed DS data to pass the Passive Authentication procedure at all inspection systems in the country which make use of the central repository. Since PA is the only mandatory security mechanism, the inspection systems may be programmed in such a way that they accept the absence of other security mechanisms. In this case this will suffice.

  Countermeasure: Good procedures and technical measures to protect the CSCA keys which are loaded in the central repository.

- An insider in the issuance process which manages to get hold of an genuine DS or CSCA private key with which fake passport data can be signed.

  Countermeasure: Employee screening, procedural and technical measures.

- An insider in the issuance process which manages to use the equipment used for passport data signing to sign fake passport data.

  Countermeasure: Employee screening, procedural and technical measures.

Biometrics verification

- Poor quality of biometrics stored in e-passport making verification difficult, resulting in either a low threshold and many false acceptances or a normal threshold and many false rejections.

  Countermeasure: Check of biometric quality in issuance process.

- Poor quality of offered biometrics characteristics, resulting in either a low threshold and many false acceptances or a normal threshold and many false rejections.

  Countermeasure: Improve biometrics by good recording conditions.

- Low threshold for biometric matching resulting in many false acceptances.

  Countermeasure: Careful determination of threshold.

2.5.5. *Interoperability*

This part of the document study was performed using actual e-passports, which have been analysed with the Collis e-MRTD Explorer Tool [35].

2.5.5.1. Supported security mechanisms

The analysed e-MRTDs support the following security mechanisms:

State	Type	BAC	PA	AA	EAC
D	P (specimen)	Yes	Yes	—	Yes
GBR	P	Yes	Yes	—	—
FIN	P (specimen)	Yes	Yes	Yes	Yes
SWE	I	Yes	Yes	Yes	—
ESP	P	Yes	Yes	—	—
NLD	P(diplomatic)	Yes	Yes	Yes	Yes
POL	P	Yes	Yes	—	—
RUS	P	Yes	Yes	—	—

Table 1 - Small inventory of supported security mechanism

2.5.6. Configuration of security mechanisms

The security mechanisms in the analysed e-MRTDs are configured as follows:

State	Type	PA – signature algorithm	PA – DS cert in Sod	AA algorithm	EAC – CA algorithm
D	P (specimen)	ecdsa_with_sha1	Yes	—	ECDH
GBR	P	sha_256WithRSAEncryption	Yes	—	—
FIN	P (specimen)	sha_256WithRSAEncryption	Yes	rsaEncryption	ECDH
SWE	I	id_RSASSA_PSS and sha256	Yes	rsaEncryption	—
ESP	P	sha_1WithRSAEncryption	Yes	—	—
NLD	P(diplomatic)	sha_256WithRSAEncryption	Yes	rsaEncryption	ECDH
POL	P	sha_256WithRSAEncryption	Yes	—	—
RUS	P	ecdsa_with_sha1	Yes	—	—

Table 2 - Small inventory of configuration of security mechanisms

2.5.6.1. Identified issues

The results show interoperability issues in two e-MRTDs officially issued by EU Member States. Some of these issues could result in false rejection of legitimate e-passports, implying that they could hamper border control. Below, we give detailed descriptions of the issues found during our analysis of e-passports chip contents. The descriptions are targeted on readers that are familiar with e-passport technology.

Inconsistency between visual and electronic Machine Readable Zone (MRZ)

In one e-MRTD, the electronically personalised MRZ (Data Group 1) was inconsistent with the visually personalised MRZ.

This inconsistency may lead to rejection of this e-MRTD in border control, as ICAO requires a comparison between the visual MRZ and the electronic MRZ as the first step of Active Authentication.

Use of incorrect Object Identifier for the ldsSecurityObject

In another e-MRTD, an incorrect object identifier (OID) is used in the ASN.1 structure of the document Security Object (SOd).

The SOd contains a structure with hash values required for Passive Authentication to authenticate e-passport data. This structure should be identified with the OID 2.23.136.1.1.1 {joint-iso-itu-t(2) international-organizations(23) icao(136) mrtd(1) security(1) ldsSecurityObject(1)}. In the analysed e-MRTD, it is identified with OID 1.2.528.1.1006.1.20.1 {iso(1) member-body(2) nl(528) nederlandse-organisatie(1) enschede-sdu(1006) ???(1) ???(20) ???(1)}.

It is likely that this error is caused by the use of this OID in a worked example of the SOd in Appendix A of the Supplement to ICAO Doc 9303 [36].

The use of an incorrect OID for the lds security object may lead to a Passive Authentication failure at border control, as inspection systems may not be able to interpret the structure.

2.5.7. Mitigating the impact of known issues in genuine e-passports

A mitigation measure for the observed issues could be the usage of a 'defect list" in inspection systems, enabling these systems to recognise e-passports with known issues and interpret (technically wrong) information. Based on these preliminary results, the (central) maintenance and distribution of a "defect list" seems an important direction of further research. Keeping the list up-to-date and transferring it to all inspection systems might turn out to form a considerable challenge. However, if the defect decreases the security, extra thorough inspection of the document should be performed.

2.5.8. Conclusions

The passport's primary use is for border passage. The e-passport will be presented at border control where checks are performed to determine whether it is genuine, valid and belongs to the passport holder. Additional checks may be performed on whether the person is allowed to enter the country based on e.g. visa or watch lists, but these are not related to the passport itself. The passport verification can be done by a border guard via visual inspection, by a border guard aided by an inspection system or by an automated border control system which is supervised by a border guard but where the border guard is not involved in the actual inspection. If the border guard uses an inspection system this reads and verifies the chip and the chip data and potentially compares the biometric data stored in the e-passport to the holder. Biometric comparison of the facial image can also be done by the border guard. When first line border control fails the passport and its holder will normally proceed to second line border control where more thorough and extensive checks on the e-passport will be performed.

For the Schengen area common rules and procedures are described at high level in the Schengen Border Code. The inspection process is described in ICAO Doc 9303 at a high level. The chip inspection procedure is described in ICAO Doc 9303 and in BSI TR-03110.

There are no functional specifications or standards for inspection systems which is considered a serious lacuna for the security and interoperability of inspection.

Besides for border passage the passport may also be required at other occasions. It serves as identification document and may be checked by regular police or in the criminal justice chain. It may be required to open a bank account or start in a new job. At airports it may be used for check-in, boarding, and/or luggage collection.

In our document study we did not encounter any security requirements on e-passports readers. We note that such requirements do exist for the e-passport chips in the form of Common Criteria protection profiles. As these readers are a vital chain in border control we believe this might hamper border control. This will be subject to further study in the interviews and the questionnaire part of the study.

3. Interview results

The interviews were conducted in August-October 2010. We would like to once again thank all interviewees for providing their time and sharing their thoughts. A list of people who have been interviewed is included in Appendix A.1.

3.1. Interview results on issuance

Interviews on issuance were conducted in The Netherlands, Luxembourg and France, with issuing authority officials.

The interviews confirmed the conclusion from the document study that the focus of fraudsters might shift to the issuance process. However, this is not in practice yet as the full capability of the e-passport is only seldom deployed for border controls.

The interviewees described the issuance process within their own country. From the descriptions we can conclude that the issuance processes in these three countries show significant differences. For example: in some of the countries a citizen can apply for a new e-passport from anywhere in the country while in the other, one could only apply for a new e-passport only in the municipality where the applicant is a resident. Moreover, in one country fingerprint verification during delivery was mandatory, in another country it was not commonly used but technically possible and in yet another country it was not technically possible at all.

Another difference is what evidence of identity is used and specifically how it is obtained. In one country the application officer relies on paper documents, presented by the applicant. This enables a large risk for identity fraud. To mitigate this risk, the respective country is currently in the process to set up a secure channel for obtaining birth certificate information. This risk was less present in the other two countries, as they have deployed a national persons registry.

A common problem discussed during the interviews was the extraction of fingerprints of older people. As the fingerprint quality degrades with age, it can be impossible to extract fingerprints with sufficient quality of older people. There is some guidance of ICAO on this subject (better to have poor quality fingerprints than no fingerprints), however not all three countries have adopted this recommendation.

The interviewees indicated that segregation of duties (ensuring that passports are not issued under single control) was sometimes difficult to achieve especially in small municipalities and that the ICAO Guidelines seem to be written for large countries, not so much for very small countries (on this point at least). Related to this is that sometimes civil servants need to perform so many (other) tasks, their knowledge/experience on the issuance process might become too low. This is a hard problem to solve in small municipalities. One of the interviewees suggested that formal certification of staff involved in issuance might be an interesting practice.

Besides providing additional security benefits some downsides of e-passports were also discussed. An interviewee remarked that since the introduction of the e-passport a lot of publicity and management effort has been given to “hackers” who have tried to compromise the e-passport security. Even if they are only partially successful, this can lead to a lot of media attention and political debate, taking up a lot of time and resources of the passport office. Also the increased reliance on machines to verify the e-passport can introduce vulnerabilities in the border control, such as cloning of e-passports and a loss of the human experience of the border guard in assessing the traveller (e.g. in ABC scenario’s).

Finally, the importance of regular audits at parties involved, including the passport offices themselves, was commonly agreed by the interviewees. One of the interviewees indicated good improvements achieved by performing such audits at passport offices within his country.

3.2. *Interview results on technical security and usage*

Interviews on inspection and technical security were conducted in Germany, the Netherlands, the UK and Poland, primarily with people involved in inspection.

One of the interviewees warned that there may be a tendency to think of the airport as the typical setting for border control, but he brought forward that in some Member States most of the border traffic is land-based (e.g. over the road and train lines) where the operational setting is very different.

The interviews with experts confirmed a gap identified in our document study. We did not identify many rules, regulations, standards or guidelines regarding e-passport ***inspection***. Requirements for e-passports adopted by the EU in Commission Decision C(2006) 2909, the EU Biometric Passport specification (ICAO Doc 9303 Volume 1 [3] and BSI TTR-03110, v1.11 [5]) only describe ***procedures*** for e-passport inspection, indicating the sequence in which (electronic) verifications should be performed. However, generally accepted requirements, functional specifications and protection profiles for inspection systems, mobile readers and automated border control systems do not exist.

The interviewees also confirmed that there are no European rules, regulations and guidelines regarding e-passport inspection which e.g. indicate when the passport and its holder should be sent to second line inspection and that additional verifications should be performed at second line inspection. Considering the common external borders of the Schengen area, we would expect these kinds of rules and regulations.

It was remarked by one interviewee that for automated border control, the possibilities for profiling, based on the travel document, are limited. It is considered a risk that it is (currently) not possible to skim through a travel document to have a look at visa, visa stamps etc. to get an impression of the travel history. To date, there is no operational guidance to mitigate this risk.

Not only constitutes this lack of operational guidance to a risk, but it can have other effects as well. One of the interviewees indicated that the public credibility of the e-passport system is at stake, as governments lack to require inspection of the chip: “Not utilizing the huge investments that issuing authorities have made with tax payers’ money cannot be explained to the public”. It became clear that there is only little use of the e-passport chip in practice, as confirmed later by the questionnaire results.

An interviewee expressed concerns regarding the usability of biometric data for automated identity verification. This person was worried about the quality of biometrics stored in the e-passport chips. It seems that there is no requirement for issuing authorities to comply with a biometrics quality standard. In a pilot project with automated border control, a huge difference in biometrics quality was identified between passports from different Member States. One passport can have a digitally captured face image, a limited loss of quality due to compression, and a background with a percentage grey within the limits of the requirements specifications; another passport can have a face image with a blue or pinkish background, which has been printed, sometimes even damaged, scanned and highly compressed. These non- or hardly ICAO-compliant facial biometric images form a threat to the development of consistently reliable automated verification.

The PKI complexity also came forward in the interviews as an important issue, both of the signing and verifying PKI. One of the interviewees shared his concerns regarding Passive Authentication, the mechanism to verify the authenticity of data in the chip. There is a risk of unauthorised border control due to the unavailability of certificates for Passive Authentication. Combined with limited awareness and knowledge about the way this mechanism functions, altered passports may pass undetected.

Another issue that came forward in the interviews was the handling of e-passports that fail to meet the ICAO standards due to “defects”. Examples of defects are wrongly computed hashes (in the so-called SOD file) and problems with certificate encoding. This was perceived as an important issue for which “defect lists” are being considered that describe these defects in terms of exceptions. The inspection system software currently cannot easily be adapted to cope with defects implying that such exceptions are now dealt with manually.

4. Generic threat and vulnerability assessment in the e- passport life cycle

4.1. Introduction

This chapter is part of the Frontex study towards the technical and operational security of e-passports. As such, it serves two purposes:

1. Presenting to the e-passport community an overview of vulnerabilities and possible countermeasures related to the e-passport life cycle steps.

2. Preparing for the risk analysis and expert workshop which concludes this study.

In this document, a generic lifecycle description is given for e-passports. For each lifecycle step, a number of vulnerabilities are presented with their possible countermeasures. The information in this document is based on publicly available international standards, literature and interviews with a number of e-passport experts throughout Europe.

The risk assessment on the e-passport life cycle is performed according to the international standard ISO/IEC 27005-2008 “Information Security Risk Management” [47], supplemented with the NIST special publication 800-30 entitled “Risk Management Guide for Information Technology Systems”. [45] In the ISO 27005 standard [44] the risk assessment process is divided in three distinct phases: risk identification, risk estimation and evaluation, and risk treatment, which are depicted below:

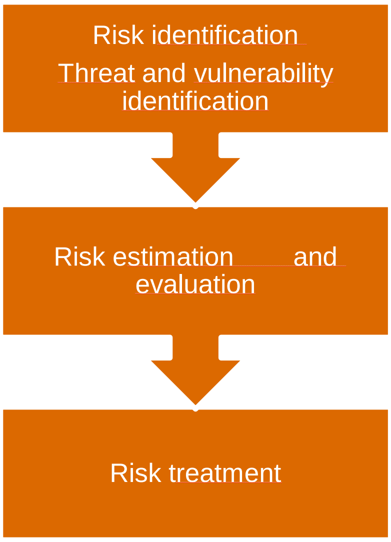

Risk identification
Threat and vulnerability identification
Risk estimation and evaluation
Risk treatment

Figure 6 - Risk assessment process

After this introductory section, we outline the risk identification process in Section 4.2. Section 4.3 addresses the e-passport life cycle and in each of the steps of the life cycle we document the identified vulnerabilities. These are complemented by the countermeasures. In Section 4.4, the vulnerabilities are summarised in a table.

4.2. *Risk identification*

In this chapter, the methodology described in the ISO 27005:2008 standard entitled “Information technology - Security techniques - Information security risk management” [44] and NIST special publication 800-30 entitled “Risk Management Guide for Information Technology Systems” [45] is followed. We introduce and use the following terms in line with these standards:

- **Vulnerability**

  A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.

- **Threat**

  The potential to accidentally trigger or intentionally exploit a specific vulnerability. Threats can be natural/environmental or human.

A fundamental difference between a threat and vulnerability is that the latter can be mitigated or even completely removed, while in principle a threat cannot be influenced.

A manifestation of a threat (explaining the intent, methods etc.) is called an **attacker.** A (potential) **incident** is based on a combination of a threat (“who” or “what”) and a vulnerability (“exploit”).

A (potential) incident has an **impact** and a **likelihood of occurrence**. The **risk** related to an incident is based on its **impact** and **likelihood of occurrence**. In the model we use (based on ISO 27005 [44]), an incident impact can vary from very low (1) to very high (5). Moreover the likelihood can vary from very unlikely (1) to very likely (5). The risk is the product of the two, as indicated in the table below. In this study we have not tried to quantify either the impact or probability.

		Incident likelihood of occurrence				
		Very unlikely(1)	Unlikely (2)	Possible (3)	Likely (4)	Very likely (5)
Incident impact	Very low (1)	**1**	**2**	**3**	**4**	**5**
	Low (2)	**2**	**4**	**6**	**8**	**10**
	Medium (3)	**3**	**6**	**9**	**12**	**15**
	High (4)	**4**	**8**	**12**	**16**	**20**
	Very high (5)	**5**	**10**	**15**	**20**	**25**

Table 3 - Risk-rating methodology

In the remainder of this chapter, the (ultimate) incident outcomes are defined and the attackers are introduced. In the next chapter, the e-passport lifecycle and related threat-vulnerability combinations which lead to the incident outcomes are identified for each of the life cycle steps.

4.2.1. Ultimate incident outcome

During the life cycle of the e-passport, a number of incidents can become manifest. As the study focuses on technical and operational security of the e-passport in border control scenarios, the ultimate incident outcome is:

Unauthorised border passage while having presented a travel document at border control.

We have added “while presenting a travel document at border control” in order to exclude all possible generic incident outcomes (such as crossing the border outside border check points, trafficking, etc). In the next section, possible incident outcomes are discussed. These incident outcomes will form the basis to relate the vulnerabilities in each of the e-passport life cycle steps.

4.2.2. Incident outcomes

Using a decomposition of the ultimate incident outcome (focusing on e-passports as stated before) we find the following incident outcomes:

O.1. Fraudulently obtaining a genuine e-passport through manipulation of the issuance procedure

O.2. Fraudulently obtaining a genuine e-passport through manipulation of the issuance systems

O.3. Lookalike fraud with a genuine e-passport

O.4. Forging or manipulating an e-passport

O.5. Exploiting weaknesses in the e-passport inspection procedure

O.6. Manipulating (part of) the e-passport inspection system

These incident outcomes are detailed below.

O.1 Fraudulently obtaining a genuine e-passport through manipulation of the issuance procedure

The attacker has obtained a genuine e-passport by manipulating the issuance procedure. This can be achieved by trying to circumvent/subvert controls in the issuance procedure (e.g. by falsifying evidence of identity) or by circumventing the issuance procedure altogether (e.g. stealing e-passports or bribing civil servants).

O.2 Fraudulently obtaining a genuine e-passport through manipulation of the issuance systems

The attacker has obtained a genuine e-passport by manipulating the issuance systems. This can for instance be achieved by inserting malicious applications in the e-passport production system which allows the attacker to change the name in the issued e-passport.

O.3 Lookalike fraud with a genuine e-passport

The attacker successfully crosses the border on an e-passport that was issued for a different person. This can be caused by a manual mismatch of a border guard or a matching error by exploiting the inherent fuzziness of the (different) matching algorithms for biometrics (e.g. thresholding the False Acceptance Rate versus the False Rejection Rate. This incident outcome has the highest probability of success if the attacker can select an e-passport of which the biometrics is (very) similar to the attacker’s biometrics.

O.4 Forging or manipulating an e-passport

The attacker successfully crosses the border with a forged e-passport. To forge an e-passport he has a number of options such as using blank (i.e. non-personalised) e-passports, data groups from a genuine e-passport, data signing keys and customisable e-passport platforms (chip and software).

As the combination of security mechanisms in the 2nd generation e-passports is very robust, usually only part of these mechanisms can be forged. In practice the attacker would need to simultaneously exploit (known) weaknesses in the inspection procedure (attack scenario O.5).

O.5 Exploiting weaknesses in the e-passport inspection procedure

The attacker successfully crosses the border by exploiting (known) weaknesses in the e-passport inspection procedure. As the security mechanisms in current e-passports (BAC, PA, AA, EAC) and biometrics are quite complex, they are not all implemented everywhere along the EU/Schengen border. Also, the different biometrics matching algorithms in use, could result in false rejections/acceptance issues. This can be caused by performing quality control procedures with the issuing country matching algorithm only.

O.6 Manipulating (part of) the e-passport inspection system

In this attack scenario, the attacker manipulates the inspection system, for instance by inserting a rogue DS certificate into the inspection system. This would allow the attacker to pass the PA security mechanism with self-generated data groups.

4.2.3. Attack model

Attackers can have different levels of expertise, knowledge and technical abilities. They can have very different levels of funding and organisation. Finally, they may be willing to accept different levels of risk of detection, and may have different attack goals.

4.2.3.1. Attacker goals

The attacker's goal is to achieve the ultimate incident outcome:

> *Unauthorised border passage while having presented a travel document at border control.*

The attacker can be motivated to achieve this goal for different reasons (economic, publicity, political).

4.2.3.2.Attacker capabilities

Below we list expertise, knowledge and capabilities that an attacker might have, and which provide ingredients of attacker profiles. Independent of these, attackers may have access to varying amounts of:

- Time
- Money
- Willingness to accept detection of the attempt (i.e. probability of detection of the attack at border control).

Low-cost capabilities

- Passport data, copied from genuine e-passports, excluding fingerprint information.
- Ability to insert a fake chip in a passport booklet, e.g.:
  - behind a visa sticker;
  - in the cover;

    - in a fake replacement cover only detectable on very close inspection.

- Programmable contactless smartcards and the ability to program these.

- A couple of stolen or bought genuine passports.

Medium-cost capabilities

- Detailed knowledge about defect lists.

- Ability to destroy chips in other people's e-passports remotely. This would allow an attacker to disable his e-passport and blend in with the other people, which do not function as well.

- The ability to perform a Denial of Service attack on an inspection system. This could be done physically or programmatically (e.g. by triggering buffer overflows in the inspection system software).

- Ability to do brute force attacks on BAC.

- Knowledge about native OS and proprietary initialisation and personalisation procedures (possibly needed to use chips in stolen blanks).

High-cost capabilities

- Large numbers of stolen or bought genuine passports.

- Ability to insert a fake chip in a passport booklet,

    - in the existing genuine cover;

    - in the laminated passport page which is essentially undetectable, even on close inspection.

- Passport data, copied from genuine e-passports, including fingerprint information.

- (Stolen or bought) blank passports. The chip can be at different stages of initialisation.

- The capability to produce high quality forged passport booklets.

- Ability to retrieve private Active Authentication or Chip Authentication keys from the passport chip by side-channel analysis (e.g. Differential Power Analysis).

- An insider in the issuance process.

- Access to country signing keys.

- An insider at border control.

- Access to inspection system keys.

- The ability to insert fake keys in inspection systems.

- The ability to tamper with the operation of inspection systems (e.g. by changing the inspection system software).

- Detailed technical knowledge about the inspection systems.

4.2.3.3. Attacker profiles

The different attackers may be willing to accept a different risk level. For instance, an economic refugee might be willing to accept a 50% detection probability (e.g. by trying to pass by an ABC gate with a life-size photograph before his face), while a criminal organisation will accept a much lower detection probability and resort to carefully implemented lookalike fraud (e.g. use the official image matching algorithm to locate a matching person then buying/stealing the person's e-passport). Defending against attackers who are willing to accept a high detection probability becomes progressively expensive. The following attacker's profiles have been identified:

(Unorganised) private individuals

Goal: Crossing a border checkpoint without being correctly identified (e.g. with a false identity)

Capabilities: Low

Internal malfeasant

Goal: Actively exploiting insider access to the issuance process for personal monetary gain (e.g. by an application officer)

Capabilities: High

Organised criminal and terrorist organisations

Goal: Crossing a border checkpoint without being correctly identified (e.g. with a false identity). This could result in human trafficking or criminals illegally going abroad or entering to escape detention.

Capabilities: High

(Foreign) Governments

Goal: Crossing a border checkpoint, belonging to a foreign country, without being correctly identified. (e.g. with a false identity)

Capabilities: High

Hacker

Goal: Generating publicity about security issues related to e-passports

Capabilities: Medium

4.3. *E-passport life cycle*

The following life cycle is presented:

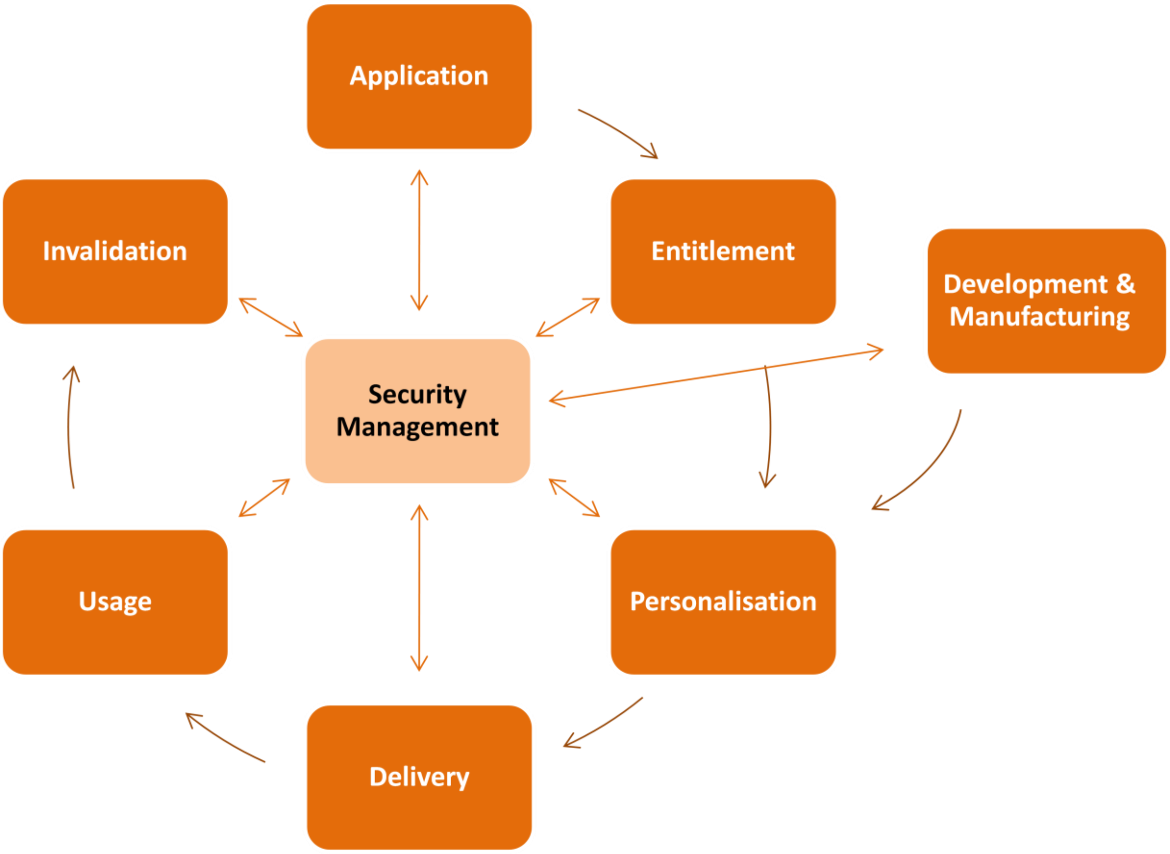


Figure 7 - Life cycle e-passport

This life cycle is based on the ICAO Guidelines for Assessing Security of Handling and Issuance of Travel Documents (v3.4) [ICAO] and is abstracted in the above figure. As a result, this is an approximation of a real-life life cycle (for instance in practice invalidation of an e-passport usually only takes place after a new e-passport has been issued).

Actor list

The following actors participate in the e-passport life cycle.

Actor	Activities
Developer/Designer	Designs the (blank) e-passport components, such as chip, booklet, antenna, chip operating system and e-passport application according to standards (e.g. ICAO Doc 9303).
Manufacturer	Manufactures and assembles the e-passport components into blank e-passports. There can be multiple manufacturers providing e-passports to a single government and manufacturers can utilise subcontractors for component assembly.
Tester/QA	Ensures quality of produced products and conformity to standards.
Certification laboratory	Certifies the design and manufacturing of the e-passport against technical standards.
Applicant	Person applying for a new e-passport.
E-passport holder	Person in possession of a genuine, valid e-passport.
Application officer/system	Government official and supporting systems in charge of processing applications for new e-passports.
Entitlement officer/system	Government official and supporting systems to make the entitlement decision.
Personalisation officer/system	Government official and supporting systems to personalise the blank e-passport with the identity of the applicant.
Delivery officer/system	Government official and supporting systems which deliver the personalised e-passport to the applicant.
Border guard	Government official who allows or denies entry into the country after verification of a traveller's identity (e.g. by using an e-passport).
Inspection system	System supporting the border guard in establishing the validity of an e-passport.
Automated border control (ABC) system	System without human intervention which verifies a traveller's identity and (dis)allows entry. It is usually monitored by a Border Guard.
Police officer/Other government official	Government official who receives and processes reports of stolen/lost e-passports.

In this chapter, each step is discussed in further detail. Also, the vulnerabilities are presented per (sub)step. Please see Section 4.4 for the full, concatenated list of vulnerabilities in the e-passport life cycle.

4.3.1. Security management

This is not a step in the e-passport lifecycle but a governance process performed by a (central) body within a country. As described in the ISO 27001 standard [47] security management takes the form of a Plan-Do-Check-Act process, also known as a Deming cycle[7].

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.1	Lack of centralised security standards	O.1, O.2, O.5, O.6	Central and common security standards	ICAO - 2
V.2	Lack of central oversight/coordination of the issuance or border control process	O.1, O.2, O.5, O.6	Central responsible organisation/department	ICAO – 1
V.3	Lack of audits/auditability	O.1, O.2, O.5, O.6	Regular audits and threat assessments	ICAO - 1.4
V.4	Lack of oversight/traceability on e-passports throughout its lifecycle	O.[1-6]	Central registration of e-passport components in their respective lifecycle (asset management).	ISO2-7
V.5	Lack of communication on security incidents among parties on national, EU or global (UN) level.	O.[1-6]	Incident knowledge sharing on (inter)national level.	ISO2-13
V.6	Personnel security – insufficient training of employees	O.[1-6]		ICAO 3
V.7	Physical security during transportation and storage	O.1, O.3		ISO2 –9

4.3.2. Development and Manufacturing

In this first step of the e-passport life cycle, the technical and physical elements of the e-passport (i.e. the chip) are developed, manufactured and (if necessary) assembled. The technical standards for the e-passport are well defined. The mandatory standards and specifications of the European Union are derived from the EC Council Regulation [1] and the Commission Decision [2] and include [3], [4] and [5].

The process in which the e-passport (components) are developed, manufactured and tested for manufacturing defects (i.e. quality control during manufacturing) is less restrictive and provides more room for interpretation to Member States and manufacturers. The Development and Manufacturing step is depicted in Diagram 2 - Development and Manufacturing below:

[7] A Deming cycle is a model for a management system in which the four phases (Plan-Do-Check-Act) are continuously followed.

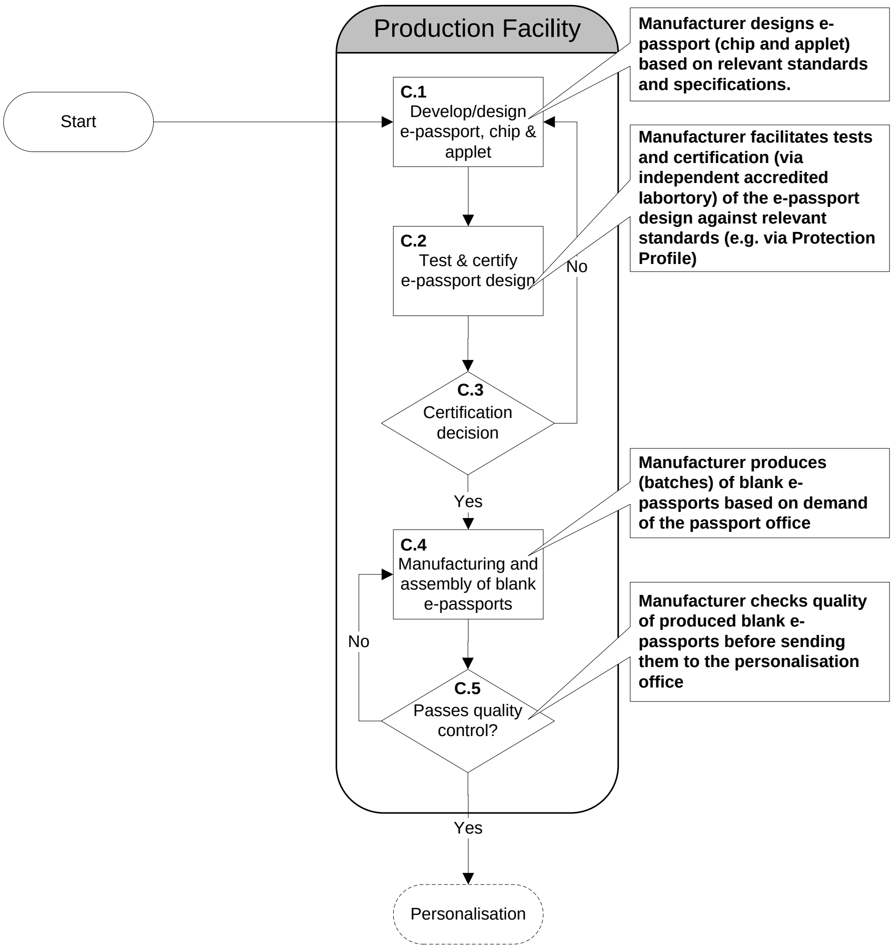

Production Facility
Start
C.1
Develop/design e-passport, chip & applet
C.2
Test & certify e-passport design
No
C.3
Certification decision
Yes
C.4
Manufacturing and assembly of blank e-passports
No
C.5
Passes quality control?
Yes
Personalisation
Manufacturer designs e-passport (chip and applet) based on relevant standards and specifications.
Manufacturer facilitates tests and certification (via independent accredited labortory) of the e-passport design against relevant standards (e.g. via Protection Profile)
Manufacturer produces (batches) of blank e-passports based on demand of the passport office
Manufacturer checks quality of produced blank e-passports before sending them to the personalisation office

Diagram 2 - Development and Manufacturing

As can be seen in the above Diagram, the step Development and Manufacturing is broken down into the following sub-steps:

C.1. Development and design of e-passport (including chip, operating system and e-passport applet)

In this step, the chip, antenna, operating system and e-passport applet are designed and developed. These items are specified by a number of mandatory standards and regulations. In this step, the manufacturer as subcontractor of the Travel Document Issuance Authority (TDIA) ensures that the result is compliant with the relevant standards [1, 2, 3, 4, 5].

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.10	Incompatibility with technical standards	O.4, O.5	Compliance with eMRTD standards	ICAO – Chapter 6 Commission Decision 2006/2909
V.11	Lower requirements for security features for certain passport types	O.1, O.3, O.4, O.5	Use the same security features for all types of passports	ICAO – Chapter 6.4 & 11
V.14	Insufficient security in Systems Development Life Cycle in the e-passport application	O.4	Follow Common Criteria protection profiles BSI-CC-PP-0055 and BSI-CC-PP-0056.	ISO2 – Chapter 12 NIST 800-64

C.2. Testing and certification of the (design of the) chip, e-passport application, booklet and blank e-passport.

After design and development, the chip, e-passport application, booklet and the assembled blank e-passport are tested for compliance with mandatory standards and provided documentation. The e-passport is evaluated against the following Common Criteria Protection Profiles by an independent and accredited laboratory:

- Common Criteria protection profile BSI-CC-PP-0055 (BAC)

- Common Criteria protection profile BSI-CC-PP-0056. (EAC)

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.14	Insufficient security in Systems Development Life Cycle in the e-passport application	O.4	Follow Common Criteria protection profiles BSI-CC-PP-0055 and BSI-CC-PP-0056.	ISO2 – Chapter 12 NIST 800-64

C.3. Certification decision of the e-passport design

The certification decision is based on a positive report by an independent, accredited laboratory as described in step C.2.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
-	-	-	-	-

C.4. Manufacturing and assembly of chip, antenna and booklet into the blank e-passport, including the software initialisation of the chip

In this sub-step, all (sub) components of the blank e-passport are manufactured and assembled into the pre-personalisation, i.e. blank, e-passport. This includes manufacturing and assembly of the chip, antenna and booklet and initialisation of the chip software (usually of the chip operating system and e-passport application). The following critical components are identified, necessary for the assembly of the e-passport:

- E-passport chip
- Private keys
- E-passport chip operating system and application.

Manufactures may depend on subcontractors to supply one or more of the components. In this case (but also when there is only a single manufacturer) the security of the manufacturer's supply chain and internal organisation becomes very relevant for the security of the e-passport.

Once the chip hardware is manufactured or received, the initialisation of the e-passport application is performed. Initialisation of the software can be broken down further in the following steps:

1. Installation (or completion) of the chip operating system
2. Installation of the e-passport application, i.e. the software that provides the e-functionality of the passport plus the functionality needed for personalisation
3. Disabling any installation of further applications.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.8	Personnel security – insufficient trustworthiness of employees	O.1	Screening, maintain employee morale, segregation of duties, traceability of blank e-passport (components)	ICAO – Chapter 3.1
V.12	Insufficient cryptographic key protection (e.g. production keys)	O.4	Usage of security modules, e.g. compliant to FIPS 140-2 level 2 or equivalent.	ICAO – Chapter 8.2

V.13	Insufficient physical security	O.1	-Deploy security zoning and controls. -Usage of transport keys for blank e-passports	ICAO – Chapter 7 ISO2 – Chapter 9
V.15	Insufficient security in Systems Development Life Cycle of chip production systems	O.2, O.4	Deploy SDLC controls.	ISO2 – Chapter 12 NIST 800-64
V.16	Insufficient logical/network access controls in chip production systems	O.2, O.4	Deploy Communications management controls.	ISO2 – Chapter 11

C.5. Quality control of manufacturing process

As the manufacturing process is high-volume, adequate quality control is essential to prevent defective e-passports to be issued.

Potential vulnerabilities

No.	**Vulnerability name**	**Related incident outcomes**	**Specific countermeasures**	**Ref.**
V.9	Insufficient testing and quality control	O.4, O.5	-Test each manufactured e-passport for defects. -Defects lists. -Recall issued e-passports by notifying the e-passport holder and invalidation after a grace period (may not be currently feasible in all countries).	-

Development and Manufacturing end result(s)

The result of the step Development and Manufacturing is a functioning blank e-passport (and any associated transport keys); conforming to the mandatory e-passport standards and specifications, ready to be personalised in the personalisation step of the e-passport life cycle.

4.3.3. *Application*

In this step, the (future) e-passport holder (applicant) applies for an e-passport and provides the issuing authority with relevant documentation to substantiate his identity claim (i.e. provide sufficient evidence of identity) and the necessary biometrics (i.e. photo and fingerprints). This step is commonly initiated by the applicant. The Application step is depicted in Diagram 3 - Application below:

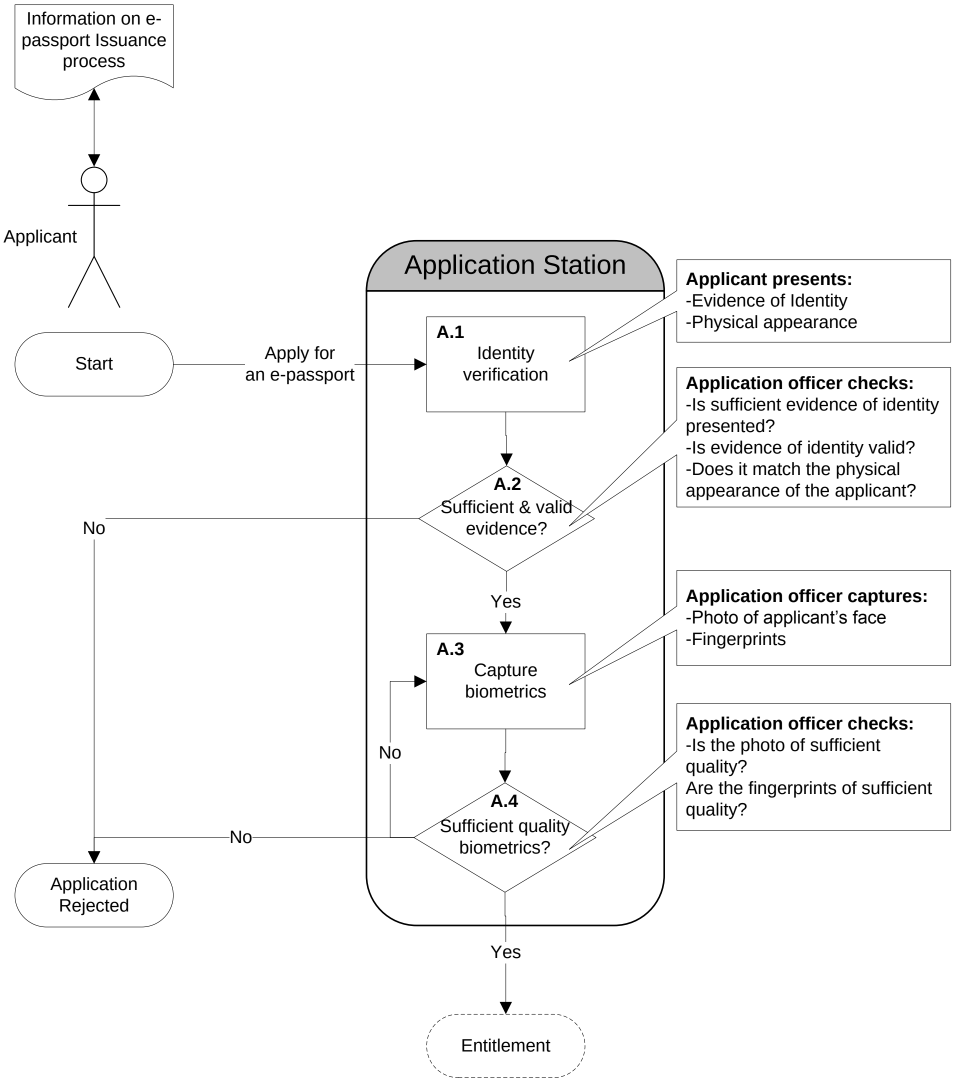

Information on e-passport Issuance process
Applicant
Start
Apply for an e-passport
Application Station
A.1 Identity verification
A.2 Sufficient & valid evidence?
No
Yes
A.3 Capture biometrics
No
A.4 Sufficient quality biometrics?
No
Yes
Application Rejected
Entitlement
Applicant presents:
-Evidence of Identity
-Physical appearance
Application officer checks:
-Is sufficient evidence of identity presented?
-Is evidence of identity valid?
-Does it match the physical appearance of the applicant?
Application officer captures:
-Photo of applicant's face
-Fingerprints
Application officer checks:
-Is the photo of sufficient quality?
Are the fingerprints of sufficient quality?

Diagram 3 - Application

As can be seen in the above Diagram, the step Application is broken down into the following sub-steps:

A.1. Identity verification of the applicant

In this step, the identity of the applicant is verified according to *Evidence of Identity* the applicant presents. For a renewal of the e-passport, this is usually a previously issued identity document. For first time applicants or for applicants whose travel document was stolen or lost, other *evidence of identity* documentation may be presented.

We would like to refer to [ICAO] for a list of possible primary and supporting documents to establish sufficient *evidence of identity*.

Also independent authoritative sources may be consulted (e.g. national persons registry) in order to establish the applicant's identity.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.19	Insufficient evidence of identity required	O.1	Properly designed identification procedures.	ICAO – Chapter 3.4
V.20	Presented evidence of identity ("breeder document") is not genuine or valid (e.g. home manufactured forgery of an electricity bill)	O.1	Provide the application officer with sufficient tools to check the validity of presented evidence of identity documents	ICAO – Chapter 3.4
V.24	Less security of alternative issuance processes (e.g. abroad, emergency)	O.1, O.2	Ensure similarly secure procedures for all issuance processes. Reduce validity period for less securely issued e-passports.	ICAO – Chapter 2

A.2. Decision whether sufficient and valid evidence of identity is presented

Based on the presented evidence of identity and the results of the validity checks, the application officer decides whether the evidence of identity is sufficient in order to positively establish the applicant's identity.

When the application officer decides that insufficient evidence of identity is available he must reject the application.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.1	Lack of centralised security standards	O.1	Central and common procedures and standards	ICAO – Chapter 2
V.3	Lack of audits/auditability	O.1	Document decisions of the application officer.	ICAO – Chapter 1.4

V.17	Personnel security - insufficient trustworthiness of employees	O.1	Use appropriately trained staff and only civil servants	ICAO – Chapter 3.1
V.18	Personnel security - insufficient segregation of duties	O.1	Use different employees for application and entitlement functions	ICAO – Chapter 9.3
V.23	First-time applications are not treated with additional scrutiny	O.1	Extra checks when e-passport expired more than two years ago, usage of database and reference checks	ICAO – Chapter 3.2

A.3. Capturing of the applicant's biometrics

When the identity of the applicant is sufficiently established the application officer will capture the biometrics of the applicant. These consist of an image of the applicant's face and his/her fingerprints. The image of the applicant's face can be captured live via a camera at the application station or via a photo that the applicant presents. Fingerprints are captured live at the application station.

Potential vulnerabilities

No.	**Vulnerability name**	**Related incident outcomes**	**Specific countermeasures**	**Ref.**
V.22	Insufficient trustworthy channel for biometrics (photo and fingerprint)	O.1	Verify captured biometrics with the applicant during application (or delivery).	ICAO – Chapter 2.3
V.26	Insufficient physical security	O.1		ICAO 7, ISO2.Ch9
V.27	Insufficient security in Systems Development Life Cycle of issuing systems	O.2, O.4		ISO2.Ch12
V.28	Insufficient logical/network access controls in issuing systems	O.2		ISO2.Ch11
V.25	False fingerprints during capturing ("gummy fingers")	O.1	Training and vigilance of application officers	-

A.4. Quality control of biometrics

Before the application is finalised the quality of the captured biometrics is verified. For this, a number of standards have been developed, such as the PhotoMatrix (for images of the applicant's face) and the NIST developed Fingerprint Image Quality (for fingerprint images). Without such a quality check the issuance procedure may result in biometrics of insufficient quality being used for the e-passport, reducing the e-passport's effectiveness.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.21	Insufficient quality biometrics were captured	O.3, O.5	Deploy quality control tests for biometrics.	ICAO – Chapter 2

Application end result(s)

The result of the step Application is a complete application file, containing personal information (name, date of birth, etc.) and high quality biometrics (i.e. image of applicant's face and fingerprints).

4.3.4. Entitlement

In this step, the application is judged, on which basis the decision is made whether to issue the e-passport. Judgement can include checks of completeness of the application file and the identity of the applicant — with independent and authoritative sources — to:

- establish the applicant's identity/existence and

- verify if the applicant is entitled to travel (e.g. if there are criminal restrictions).

The Entitlement step is depicted in Diagram 4 - Entitlement below:

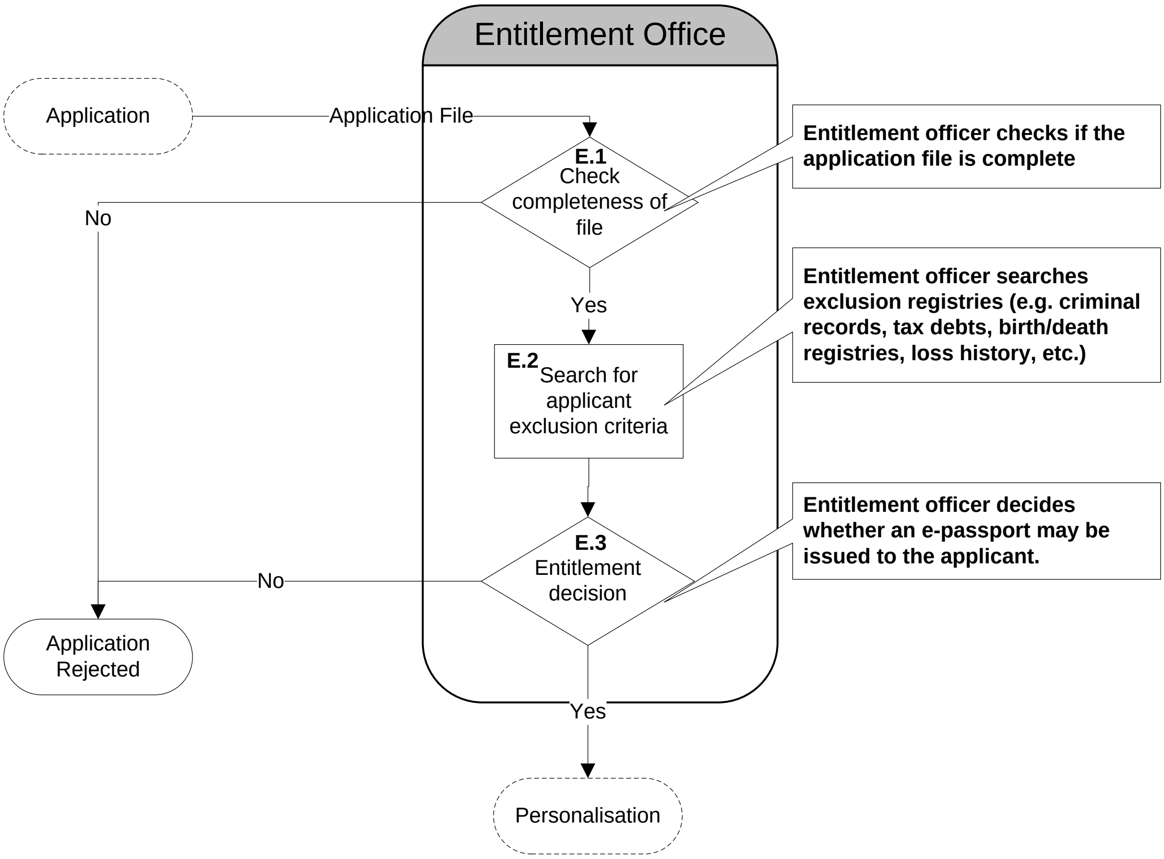

Entitlement Office
Application
Application File
E.1
Check completeness of file
No
Yes
E.2
Search for applicant exclusion criteria
E.3
Entitlement decision
No
Application Rejected
Yes
Personalisation
Entitlement officer checks if the application file is complete
Entitlement officer searches exclusion registries (e.g. criminal records, tax debts, birth/death registries, loss history, etc.)
Entitlement officer decides whether an e-passport may be issued to the applicant.

Diagram 4 - Entitlement

As can be seen in the above diagram, the step Entitlement is broken down into the following sub-steps:

E.1 Check completeness of application file

Before the application file is accepted by the entitlement officer the completeness of the application file is evaluated. When it is apparent that the application file is not complete, the application is rejected.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
-	-	-	-	-

E.2 Search for applicant exclusion criteria

The entitlement officer searches for exclusion criteria in authoritative sources, based on the applicant's identity established during application. Exclusion criteria may be: active criminal records or trial pending, renouncement of nationality, tax debt, excessive loss history, etc. Please note that as the entitlement officer only has the application file available he/she cannot further scrutinise the applicant's evidence of identity.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.32	Insufficient information is available to the entitlement officer to base his decision on (e.g. criminal records, passport loss history, etc.)	O.1	Provide up-to-date and accessible registries for criminal records, national citizens, loss history, etc.	ICAO 3.4, 3.5
V.33	Insufficient checks against loss history of the applicant	O.1, O.3, O.4	Provide up-to-date and accessible registries for criminal records, national citizens, loss history, etc.	ICAO 10
V.34	Insufficient follow-up of (apparent) fraudulent applicants.	O.1, O.3, O.4	Report potential fraudulent applicants to the police.	ICAO 3.7

E.3 Entitlement decision

Finally the entitlement officer decides whether the applicant is entitled to be issued an e-passport. This decision is based on the identity established during application and the search for exclusion criteria on the previous sub-step.

Potential vulnerabilities

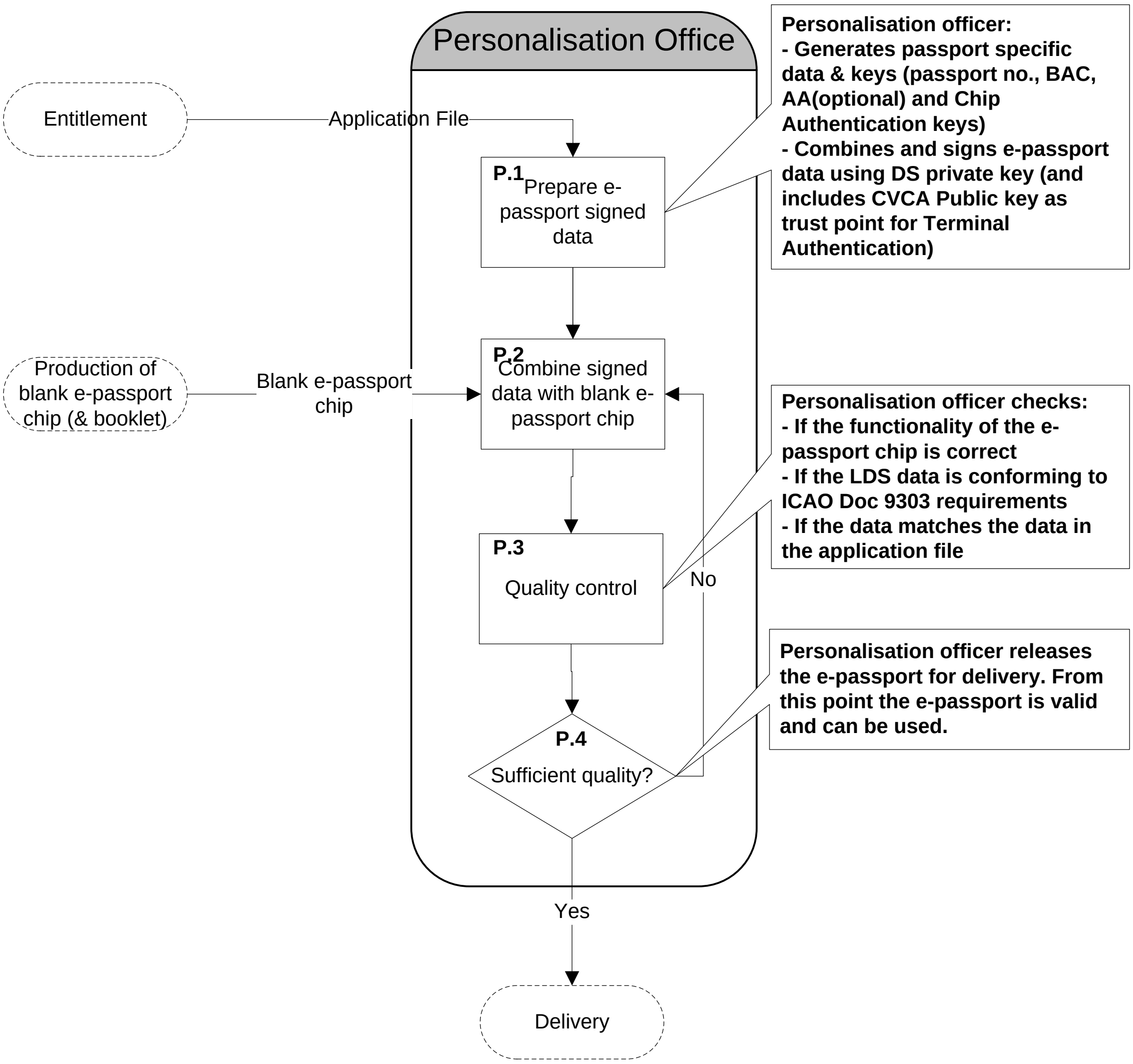
No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.29	Personnel security – insufficient trustworthiness of employees	O.1	Use appropriately trained staff and only civil servants	ICAO 3.1
V.30	Personnel security – insufficient segregation of duties	O.1	Use different employees for application, entitlement and delivery functions	ICAO - 9.3
V.31	Non-deterministic/Not traceable entitlement decision-making	O.1	Document the decision procedure and provide for an audit trail for all entitlement decisions	ICAO 3.1

Entitlement end result(s)

The result of this step is a verified and approved application information file, ready for personalisation.

4.3.5. Personalisation

In this step, the personal information of the applicant (e.g. biographical and biometric data) is inserted into the blank e-passport, thus personalising the e-passport. Also e-passport specific data and keys are generated and inserted into the blank e-passport. The Personalisation step, including sub-steps, could be fully automated, as no human intervention is necessary. The step Personalisation is depicted in Diagram 5 - Personalisation below:



Personalisation Office
Entitlement
Application File
P.1 Prepare e-passport signed data
Production of blank e-passport chip (& booklet)
Blank e-passport chip
P.2 Combine signed data with blank e-passport chip
P.3 Quality control
No
P.4 Sufficient quality?
Yes
Delivery
Personalisation officer:
- Generates passport specific data & keys (passport no., BAC, AA(optional) and Chip Authentication keys)
- Combines and signs e-passport data using DS private key (and includes CVCA Public key as trust point for Terminal Authentication)
Personalisation officer checks:
- If the functionality of the e-passport chip is correct
- If the LDS data is conforming to ICAO Doc 9303 requirements
- If the data matches the data in the application file
Personalisation officer releases the e-passport for delivery. From this point the e-passport is valid and can be used.

Diagram 5 - Personalisation

As can be seen in the above diagram, the step Personalisation is broken down into the following sub-steps:

P.1 Prepare e-passport signed data

In this sub-step, the e-passport data to be inserted into the blank e-passport is prepared. The personal information from the application file is structured in data groups (DGs) according to the requirements of ICAO Doc 9303 [3,4], together with passport-specific data (e.g. passport no., MRZ, BAC keys, AA key pair (optional) and Chip Authentication key pair are generated). AA and Chip Authentication public keys are stored in individual DGs. All DGs form a logical data structure (LDS) with a so-called document security object directory (SOd). This SOd contains hash-values calculated over individual DGs, as well as the DS public key certificate, and is signed with the DS private key. In addition, AA and/or Chip Authentication private keys are prepared for loading, as well as the CVCA public key (as a trust point for Terminal Authentication).

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.39	Insecure cryptographic protocols used in personalisation, e.g. generation of keys.	O.4, O.6	Conform to ICAO Doc 9303	ICAO - 6
V.40	Insufficient cryptographic key protection (e.g., production keys)	O.4	Usage of security modules, e.g. compliant to FIPS 140-2 level 2 or equivalent.	ICAO - 8.2

P.2 Insert signed data into blank e-passport

In this sub-step the prepared, signed e-passport data is inserted into the blank e-passport. In order for the personalisation equipment to access the blank e-passport application to insert the prepared data, the transport key is used. Once the e-passport is properly personalised, the e-passport application is closed for further updates to prevent possible fraud.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.35	Personnel security – insufficient trustworthiness of employees involved in personalisation	O.1		ICAO 3.1
V.37	Vulnerabilities related to de-centralised personalisation (e.g. in use for emergencies)	O.1, O.4	Similar (technical) controls as in regular issuance.	ICAO 11
V.38	Passport chip not closed (made read-only) after e-passport application is loaded.	O.4	Proper personalisation procedure. Sufficient documentation.	-
V.40	Insufficient cryptographic key protection (e.g., production keys)	O.4	Usage of security modules, e.g. compliant to FIPS 140-2 level 2 or equivalent.	ICAO - 8.2

V.41	Insufficient physical security	O.1		ICAO 7, ISO27002 Ch9
V.42	Insufficient logical/network access controls in personalisation systems	O.2, O.4	Usage of Common Criteria.	ISO27002 Ch11
V.43	Insufficient security in Systems Development Life Cycle of personalisation systems	O.2		ISO27002 Ch12

P.3 Quality control

After personalisation the personalisation officer checks whether the personalisation was successful. For this, the functionality could be tested and the data now present in the e-passport compared with the original application file.

Potential vulnerabilities

No.	**Vulnerability name**	**Related incident outcomes**	**Specific countermeasures**	**Ref.**
V.36	Insufficient quality controls after personalisation	O.1, O.3	Verify e-passport functionality and contents by: - reading the chip data and performing the security mechanisms; - validating the conformity of the LDS to the requirements of ICAO Doc 9303; - comparing all data groups against the application file.	ICAO 5.2

P.4 Quality decision

Based on step P.3, the personalised e-passport is accepted or rejected for usage. In case the personalisation was not perfect the e-passport is rejected. If non-compliant e-passports are accepted for use they may lead to more significant problems, such as defect lists.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
-	-	-	-	-

Personalisation end result(s)

The result of this step is a ready-to-use e-passport which has not yet been delivered to the applicant.

4.3.6. Delivery

In this step, the personalised e-passport is delivered to the applicant. The step Delivery is depicted in Diagram 6 - Delivery below:

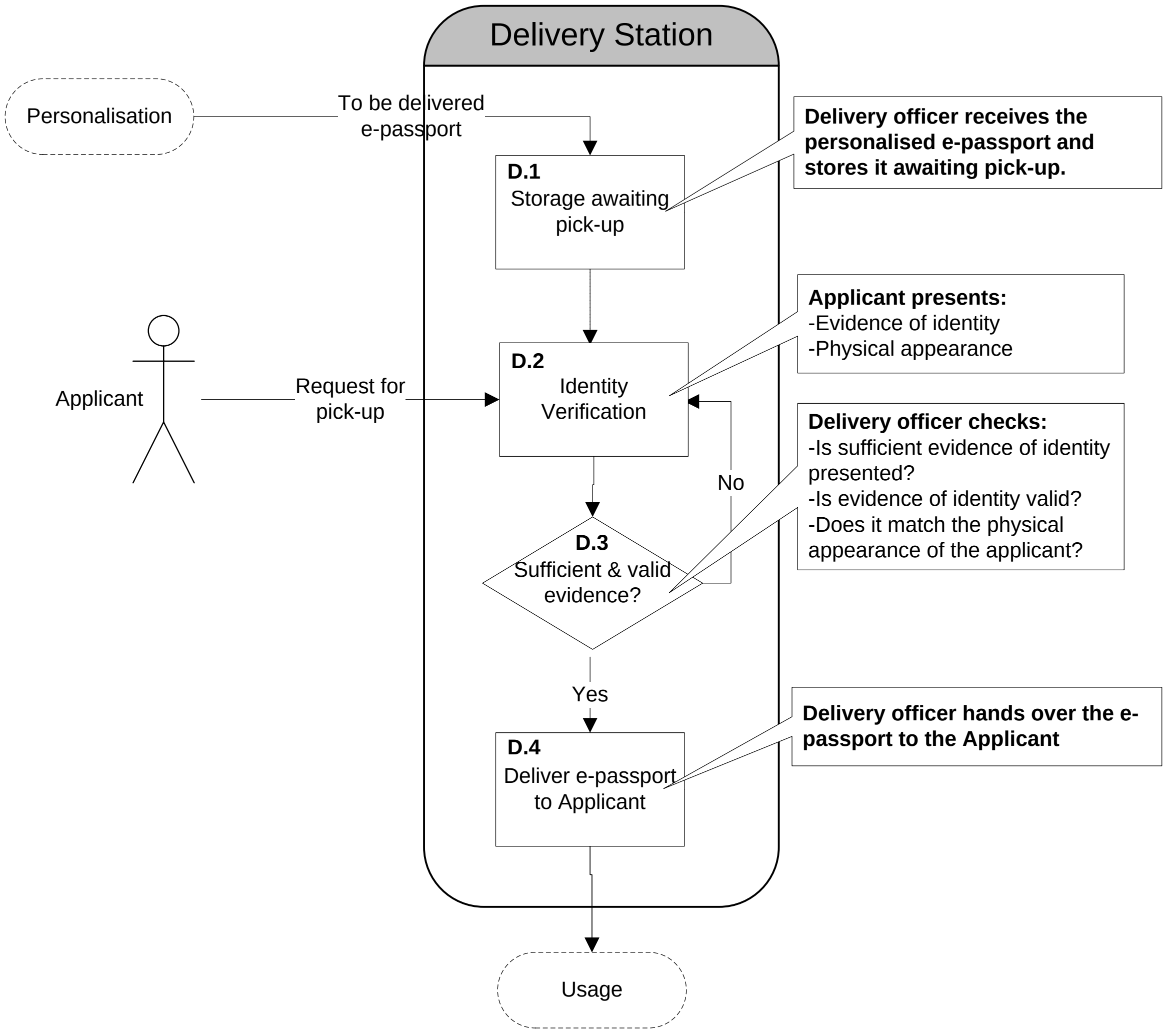

Delivery Station
Personalisation
To be delivered e-passport
D.1 Storage awaiting pick-up
Delivery officer receives the personalised e-passport and stores it awaiting pick-up.
Applicant
Request for pick-up
D.2 Identity Verification
Applicant presents:
-Evidence of identity
-Physical appearance
No
Delivery officer checks:
-Is sufficient evidence of identity presented?
-Is evidence of identity valid?
-Does it match the physical appearance of the applicant?
D.3 Sufficient & valid evidence?
Yes
D.4 Deliver e-passport to Applicant
Delivery officer hands over the e-passport to the Applicant
Usage

Diagram 6 - Delivery

As can be seen in the above diagram, the step Delivery is broken down into the following sub-steps:

D.1 Storage awaiting pick-up

As soon as the e-passport is personalised (and, thus, ready for use), it will need to be stored awaiting pick-up by the applicant. As there are, in all likelihood, multiple e-passports stored for short/medium term in the Delivery Stations they are kept in a sufficiently secure location and with a verifiable audit trail.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.46	Not collected e-passports are not inventoried and invalidated	O.1, O.4	Monitor and destroy passports that have not been picked up.	ICAO 5.3
V.47	Insufficient physical security	O.1, O.4	Store and transport already personalised e-passports securely.	ICAO 7, ISO2.Ch9

D.2 Identity verification

If the applicant comes to the delivery station to pick-up his e-passport, the identity of the applicant is verified. Ideally, the identity verification is as strong as during application.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.44	Identity of collecting person is insufficiently verified	O.1, O.3	Use all biometrics to verify the identity of the e-passport holder before delivery.	ICAO 5.3
V.45	E-passport delivered via mail or third person	O.1	Request for receipt of confirmation upon delivery.	ICAO 5.3

D.3 Delivery decision

Based on the identity verification of the previous sub-step, the delivery officer decides whether to hand over the e-passport. Fraudulent attempts to collect an e-passport are reported to the relevant authorities.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
-	-	-	-	-

D.4 Deliver e-passport to applicant

In this final sub-step, the e-passport is handed to the applicant. Allowing other persons than the applicant to pick-up the e-passport introduces vulnerability in the delivery process, as the receipt of the e-passport by the applicant cannot be verified. Upon delivery, any still valid old e-passport is usually invalidated (possibly both through physical destruction or registration).

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.45	E-passport delivered via mail or third person	O.1	Request for receipt of confirmation upon delivery	ICAO 5.3

Delivery end result(s)

The result of this step, is that the e-passport is in possession of the applicant, ready for usage.

4.3.7. Usage

In this step, the applicant (now e-passport holder) can use his/her e-passport. The usage period is limited by the e-passport validity period (usually between 5 and 10 years). At the end of the usage period, the validity of the e-passport automatically expires (but of course the border control officer can decide whether to accept the expired e-passport or not). Please note that the e-passport does not necessarily technically expire at the same time, so can remain technically valid. During its validity period, the e-passport can be lost or stolen, in which case the holder requests the relevant authorities to invalidate his e-passport. This is often a prerequisite to apply for a new e-passport.

This section provides an inventory of potential vulnerability related to the use of e-passports for border control. During the usage phase of the e-passport life cycle, the e-passport can be used for several purposes. Although the e-passport may be used for purposes other than border control (e.g. in banking, for online identification purposes), the risks associated with such use are not evaluated in the scope of this study.

In order for the border control officer to verify that the e-passport is valid, genuine and matching the holder, border control systems (e.g. an inspection system) are used. Such inspection systems have their own life cycle. In the usage phase these ***inspection systems obtain and exchange data, process data received from systems in other States and utilise that data in inspection operations***[8]. They do this at the front-end by *obtaining, exchanging, processing and utilising data* from the e-passport chip. But also in the back end by *obtaining, exchanging, processing and utilising data* regarding lost and stolen documents; for Passive Authentication: CSCA and DS certificates, CRLs and defect lists; for Terminal Authentication: CVCA/DV/IS certificates).

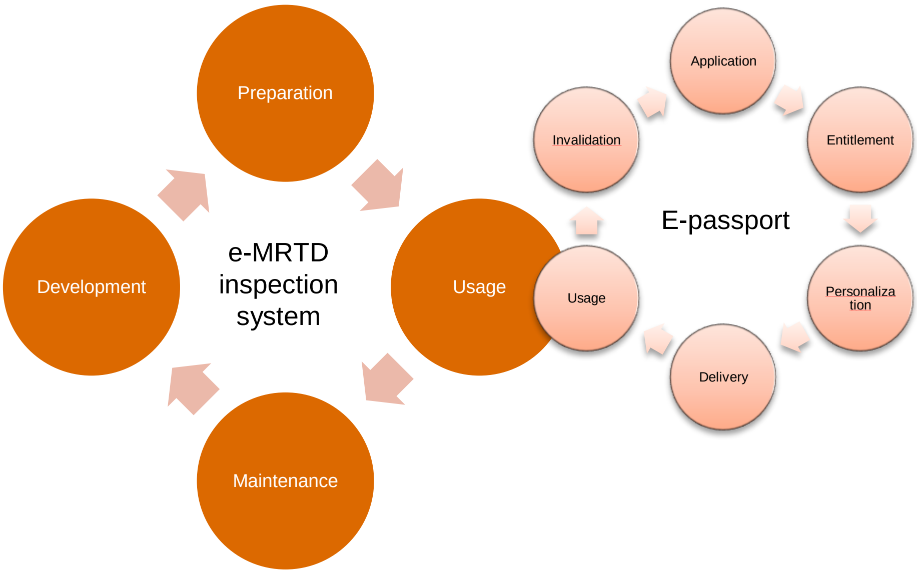


Figure 8 - inspection system lifecycle

The step Usage of the e-passport life cycle meets the usage step of the inspection system life cycle, and is depicted in Diagram 7 - Usage below:

[8] Paraphrasing ICAO's definition of "Global Interoperability"

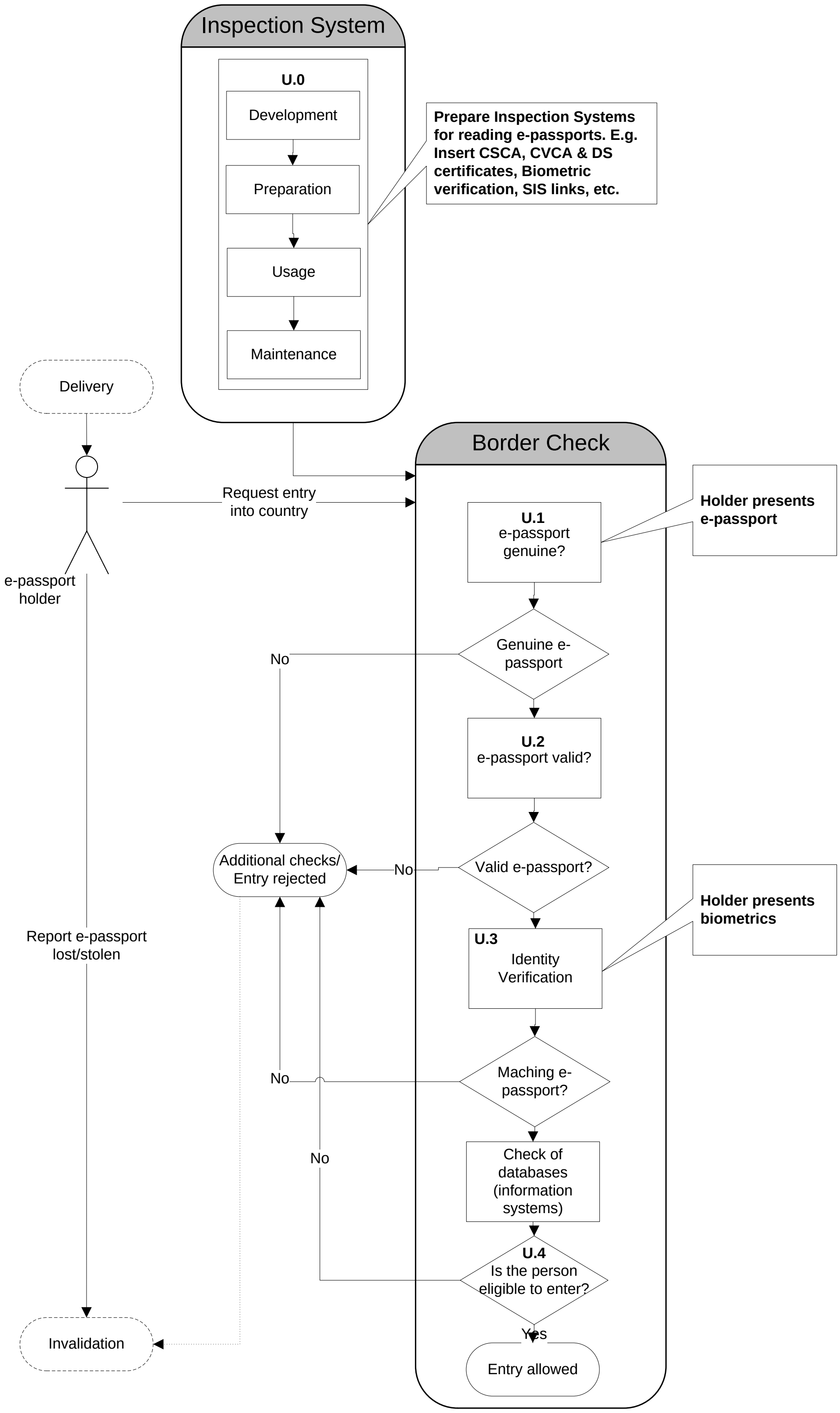

Inspection System
U.0
Development
Preparation
Usage
Maintenance
Prepare Inspection Systems for reading e-passports. E.g. Insert CSCA, CVCA & DS certificates, Biometric verification, SIS links, etc.
Delivery
e-passport holder
Request entry into country
Border Check
U.1
e-passport genuine?
Holder presents e-passport
Genuine e-passport
No
U.2
e-passport valid?
Valid e-passport?
No
Additional checks/ Entry rejected
U.3
Identity Verification
Holder presents biometrics
Report e-passport lost/stolen
Maching e-passport?
No
Check of databases (information systems)
No
U.4
Is the person eligible to enter?
Yes
Entry allowed
Invalidation

Diagram 7 - Usage

As can be seen in the above diagram, the step Usage is broken down into the following sub-steps:

U.0 Prepare and maintain border control systems (inspection system life cycle)

This sub-step considers a critical prerequisite for additional security through the usage of electronic passports: the inspection system[9]. In order for border control officers to properly use and verify the security features of the e-passport an inspection system is provided.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.1	Lack of centralised security standards	O.1	Central and common procedures and standards.	ICAO – Chapter 2
V.3	Lack of audits/auditability	O.1	Document decisions of the application officer.	ICAO – Chapter 1.4
V.51	Insufficient guidance provided by border system to border guard	O.5, O.6	Clear communication of different results of inspection procedure (e.g. failure of PA, AA, EAC or biometric matching)	-
V.54	Insufficient operational ability for border control to evaluate security mechanisms (BAC, PA, AA, EAC) of the e-passport.	O.4, O.5	Have all necessary systems (and related infrastructure, for example for EAC) and training available for border guards.	-
V.55	Insufficient reporting or registration of lost/stolen e-passports	O.4	Provide proper access of inspection system to registry of lost/stolen e-passports.	ICAO 10
V.60	Insufficient integrity protection of (storage of) public key certificates (DS certificates, CSCA)	O.6	- Use a trusted source for DS, CSCA certificates (bilateral or ICAO PKD). - Use an integrity checking mechanism to validate that certificates may be used in inspection operations.	-
V.61	Insufficient confidentiality protection of (EAC) private keys	O.4, O.6	Usage of security modules, e.g. compliant to FIPS 140-2 level 2 or equivalent.	-
V.62	Insufficient border guards available when border control systems are not available.	O.5	Draft a procedure when border control systems are not working.	ISO2.Ch14
V.64	Insufficient logical/network access controls in border control systems	O.4, o.6		ISO2.Ch11
V.65	Insufficient security in Systems Development Life Cycle of border	O.6	Develop inspection systems with high security	ISO2.Ch12

[9] As this is strictly not a sub step of the e-passport life cycle, it is coded as "U.0".

	control systems		requirements Common Criteria evaluation.	

The next sub-steps concern the usage step in the e-passport life cycle, where the border control officer/ABC system uses the e-passport in inspection operations. For this he has the e-passport, the traveller itself and the inspection system at his disposal. The inspection process can be broken down into four sub-steps:

1. Verification of authenticity of the e-passport
2. Verification of validity of the e-passport
3. Verification of the e-passport holder's identity
4. Verification of the e-passport holder's eligibility to enter the country/territory.

U.1 Document authentication

In this sub-step, the border control officer/ABC system attempts to verify the authenticity of the presented (e-passport) document.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.48	Chip can be disabled	O.3, O.4, O.5	Issue a procedure to follow when a (partially) non-functional e-passport chip is found during border control.	-
V.49	Chip communication can be jammed	O.3, O.6	Issue a procedure to follow when a (partially) non-functional e-passport chip is found during border control.	-
V.50	European National Identity Cards (or any other accepted travel documents, like residence permits) can be used if they are less secure than the e-passport	O.5	Ensure that all travel documents accepted for international travel have the same security level.	-
V.52	Insufficient quality of e-passports (e.g. defects)	O.4	Sufficient quality controls in issuance process.	ICAO – 5.2

U.2 Document validity verification

In this sub-step, the border control officer/ABC system attempts to verify the validity of the presented (e-passport) document. This can be done electronically, based on the combination of document expiry date and certificate end of validity or in a machine-readable manner, based on the document expiry date in the MRZ. In case of reading problems or system unavailability, the border control officer can fall back to manual inspection, based on the document expiry date in the MRZ or the VIZ.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.58	Multiple passports per person	O.3, O.4	Only provide one valid passport to one person. Invalidate old passports immediately.	ICAO 6.4

U.3 Verification of the document holder's identity

In this sub-step, the border control officer/ABC system attempts to verify the identity of the holder of the presented authentic, valid (e-passport) document.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.56	Inability to verify biometrics during border control	O.3, O.5	Proper procedures and equipment.	-
V.57	Too long validity time of e-passport	O.3, O.4	Recommended at five years.	ICAO 6.4
V.59	Insufficient biometric quality	O.3	Quality control during issuance	ICAO - 5.2
V.63	Automated border control eliminates human experience and expertise in border checks	O.5	Randomly select travellers to go through a manual border check after passing the ABC check. As second line requires additional expertise, we recommend to only use ABC for first line control.	-
V.53	False fingerprints during border control ("gummy fingers")	O.1	Training and vigilance of border guards or high quality inspection systems.	-

Based on the e-passport, the traveller’s physical appearance and the results of the validity checks, the border control officer decides whether the evidence is sufficient in order to positively establish the traveller’s identity.

When the border control officer decides that the evidence is insufficient, he rejects the request for entry immediately or refers the traveller to second line border control. In second line border control, additional checks may take place to establish the identity of the traveller. Possible checks in second/third line border control are: interview questions, searching the traveller’s luggage/possessions, querying registries and databases, further investigation of the travel document presented.

U.4 Verification of the holder’s eligibility to enter

This sub-step is out of scope for this study, but represented here to provide a complete set of sub-steps. This is, for instance, related to visa application or watch/black-lists.

Usage end result(s)

As Usage is a steady-state step during the validity period of the e-passport, there is no defined end result of the Usage step.

4.3.8. Invalidation

In this step, the e-passport is invalidated, so that it can no longer be used for identification. Multiple reasons can be identified to invalidate an e-passport:

- The e-passport was lost or stolen
- The e-passport is found to be no longer functioning correctly
- A new e-passport was issued to the same holder.

Note that in this step the regular expiration of e-passports is not covered. Although expired e-passports should not be accepted as a valid e-passport in the Usage step, it is therefore not strictly necessary to explicitly invalidate or destroy expired e-passports. The invalidated passport may be handed back to the holder, or may be kept by the police for destruction. The step Invalidation is depicted in Diagram 8 - Invalidation below:

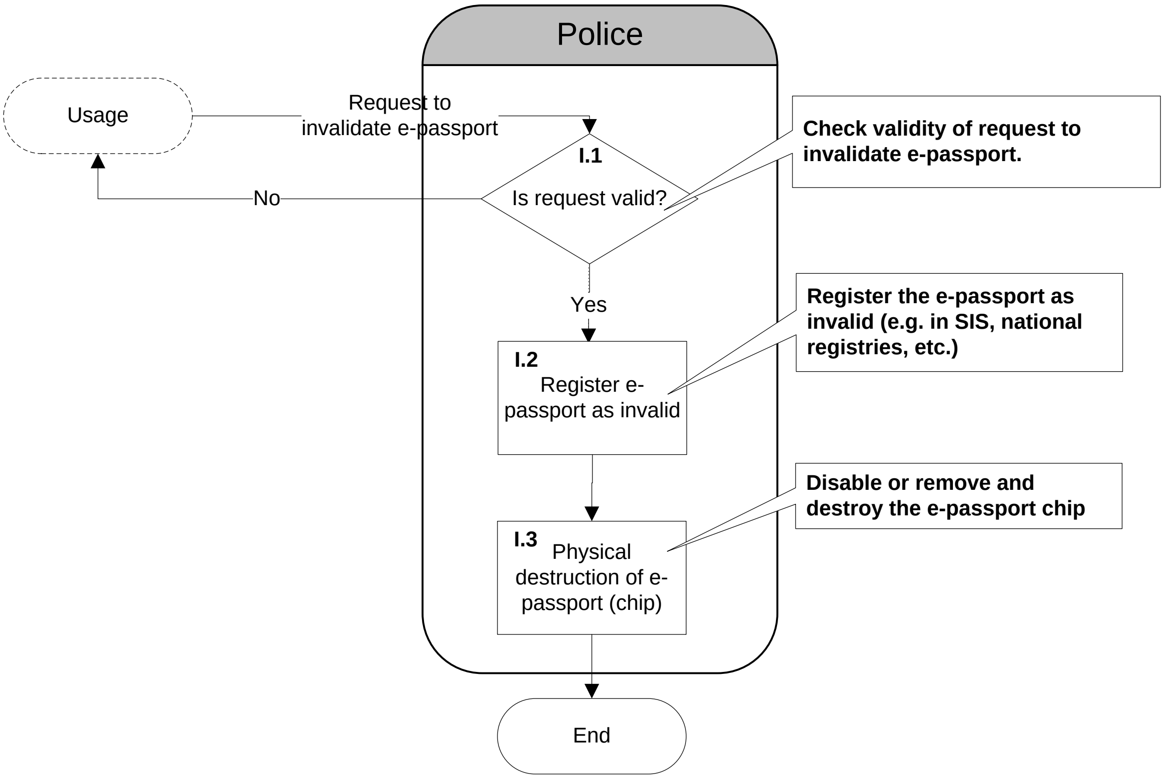

Police
Usage
Request to invalidate e-passport
I.1
Is request valid?
No
Yes
I.2
Register e-passport as invalid
I.3
Physical destruction of e-passport (chip)
End
Check validity of request to invalidate e-passport.
Register the e-passport as invalid (e.g. in SIS, national registries, etc.)
Disable or remove and destroy the e-passport chip

Diagram 8 - Invalidation

As can be seen in the above diagram, the step Invalidation is broken down into the following sub-steps:

I.1 Request validity check

The passport office performs validity checks on a request to invalidate an e-passport in order to prevent e-passports being invalidated by unauthorised persons. E-passport holders are made aware of the need to report stolen/lost e-passports. Expired e-passports do not necessarily need to be invalidated.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.67	Insufficient public awareness of the need to report stolen or lost e-passports	O.3		ICAO 10

I.2 Register e-passport as invalid

When the request is deemed to be valid, the e-passport is registered as invalid. This information is available to relying parties, such as border control officers, application officers and delivery officers, as well as any other stakeholders outside the formal e-passport issuance and usage lifecycle (such as notaries).

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.66	Insufficient registration of lost/stolen passports	O.3, O.4	Keep a central registry of invalidated e-passports (e.g. SIS, Interpol SLTD[10] database), accessible to all relevant relying parties.	ICAO 10
V.69	Insufficient physical security	O.1		ICAO 7, ISO2.Ch9

[10] Stolen and Lost Travel Document

I.3 Physically destroy e-passport (chip)

In order to prevent the now invalidated e-passport (components) or to prevent data to be used for forgery attempts, the e-passport (chip and booklet) are also physically invalidated/destroyed. In case the e-passport is not in possession of the relevant authorities (i.e. when the e-passport is lost or stolen) this sub-step cannot be performed.

Potential vulnerabilities

No.	Vulnerability name	Related incident outcomes	Specific countermeasures	Ref.
V.68	Inadequate e-passport destruction upon invalidation	O.3, O.4	Disable or remove and destroy the e-passport chip.	-

Invalidation end result(s)

The result of this step is the invalidated e-passport, which can no longer be used for identification/travel.

4.4. *Summary table of vulnerabilities per life cycle step*

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
Security management (overall)					
V.1	Lack of centralised security standards		O.1, O.2, O.5, O.6	Central and common security standards	ICAO – 2
V.2	Lack of central oversight/coordination of the issuance or border control process		O.1, O.2, O.5, O.6	Central responsible organisation/department	ICAO – 1
V.3	Lack of audits/auditability		O.1, O.2, O.5, O.6	Regular audits and threat assessments	ICAO - 1.4
V.4	Lack of oversight/traceability of e-passports throughout its life cycle		O.[1-6]	Central registration of e-passport components in their respective life cycle (asset management)	ISO2-7
V.5	Lack of communication on security incidents among parties at national, EU or global (UN) level		O.[1-6]	Incident knowledge sharing at (inter) national level	ISO2-13

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
V.6	Personnel security – Insufficient training of employees		O.[1-6]		ICAO 3
V.7	Physical security during transportation and storage		O.1, O.3		ISO2 – Ch 9
Development and Manufacturing					
V.8	Personnel security – Insufficient trustworthiness of employees involved in issuing, e.g. bribing or blackmailing employees		O.1	Screening, maintaining employee morale, segregation of duties, traceability of blank e-passport (components)	ICAO 3.1

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
V.9	Insufficient testing and quality control	Many defects in issued passports might lead to them being accepted by border guards, opening up vulnerabilities.	O.4, O.5	-Test each manufactured e-passport for defects -Defects lists -Recall issued e-passports by notifying the e-passport holder and invalidation after a grace period (may not be currently feasible in all countries)	-
V.10	Incompatibility with technical standards		O.4, o.5	Compliance with eMRTD standards – Common criteria certification	ICAO 6
V.11	Lower requirements for security features for certain passport types (when compared with regular passports) • Diplomatic • Emergency/Temporary • Offical/Special		O.1, O.3, O.4, O.5	Use the same security features for all types of passports	ICAO 6.4 ICAO 11

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
V.12	*Insufficient cryptographic key protection (e.g. production keys)*		*O.4*	*Usage of security modules, e.g. compliant to FIPS 140-2 level 2 or equivalent*	*ICAO - 8.2*
		Generic			
V.13	Insufficient physical security		O.1		ICAO 7, ISO2.Ch9
V.14	*Insufficient security in Systems Development Life Cycle in the e-passport application, e.g. e-passport application that allows for cryptographic key export*		*O.4*		*ISO2.Ch12*
V.15	*Insufficient security in Systems Development Life Cycle of chip production systems*		*O.2, O.4*		*ISO2.Ch12*
V.16	*Insufficient logical/network access controls in chip production systems*		*O.2, O.4*		*ISO2.Ch11*
Application					

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
V.17	Personnel security – Insufficient trustworthiness of employees involved in issuing, e.g. bribing or blackmailing employees		O.1	Use appropriately trained staff and only civil servants	ICAO 3.1
V.18	Personnel security – Insufficient segregation of duties (between application and entitlement)		O.1	Use different employees for application and entitlement functions (constrained by number of available personnel)	ICAO 9.3
V.19	Insufficient evidence of identity required	During application, the applicant is not required to provide sufficient evidence of identity	O.1	Properly designed identification procedures	ICAO - 3.4

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
V.20	Presented, invalid evidence of identity is not genuine or valid	During application, the evidence of identity cannot be properly checked because of missing biometrics, security features or independent authoritative source (e.g. stolen documents registry)	O.1	Provide the application station with sufficient tools to check the validity of presented evidence of identity documents	ICAO – 3.4
V.21	*Insufficient quality biometrics were captured*		*O.3, O.5*		*ICAO - 2*
V.22	*Insufficient trustworthy channel for biometrics (photo and fingerprint)*		*O.1*	*Verify biometrics with the applicant during application*	*ICAO - 2.3*
V.23	First applications are not treated with additional scrutiny		O.1	Extra checks when e-passport expired more than two years ago, usage of database and reference checks	ICAO - 3.2

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
V.24	Less security of alternative issuance processes - abroad (i.e. via embassies) - emergency issuance		O.1, O.2	Ensure similarly secure procedures for all issuance processes. Reduce validity period for less securely issued e-passports.	ICAO 2
V.25	*False fingerprints during capturing ("gummy fingers")*		*O.1*	*Training and vigilance of application officers*	-
		Generic			
V.26	Insufficient physical security		O.1		ICAO 7, ISO2.Ch9
V.27	Insufficient security in Systems Development Life Cycle of issuing systems		O.2, O.4		ISO2.Ch12
V.28	Insufficient logical/network access controls in issuing systems		O.2		ISO2.Ch11
Entitlement					
V.29	Personnel security – Insufficient trustworthiness of employees involved in issuing, e.g. bribing or blackmailing employees		O.1	Use appropriately trained staff and only civil servants	ICAO 3.1

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
V.30	Personnel security – Insufficient segregation of duties (between application and entitlement)		O.1	Use different employees for application and entitlement functions (constrained by number of available personnel)	ICAO - 9.3
V.31	Non-deterministic/not traceable entitlement decision-making		O.1	Document the decision procedure and provide for an audit trail for all entitlement decisions	ICAO 3.1
V.32	Insufficient information is available to the entitlement officer to base his decision on (e.g. criminal records, passport loss history, etc.)		O.1	Provide up-to-date and accessible registries for criminal records, national citizens, loss history, etc.	ICAO 3.4, 3.5
V.33	Insufficient checks against loss history of the applicant		O.1, O.3, O.4	Provide up-to-date and accessible registries for criminal records, national citizens, loss history, etc.	ICAO 10
V.34	Insufficient follow-up of (apparent) fraudulent applicants		O.1, O.3, O.4		ICAO 3.7

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
Personalisation					
V.35	Personnel security – Insufficient trustworthiness of employees involved in issuing, e.g. bribing or blackmailing employees		O.1		ICAO 3.1
V.36	Insufficient quality controls after personalisation		O.1, O.3	Verify e-passport functionality and contents by - reading the chip data and performing the security mechanisms - validating the conformity of the LDS to the requirements of ICAO Doc 9303 - comparing all data groups against the application file	ICAO 5.2
V.37	Vulnerabilities related to decentralised personalisation (e.g. in use for emergencies)		O.1, O.4	Similar (technical) controls as in regular issuance	ICAO 11

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
V.38	*Passport chip not closed (e.g. made read-only) after e-passport application is loaded.*		*O.4*	*Proper personalisation procedure. Sufficient documentation of e-passports.*	-
V.39	*Insecure cryptographic protocols used in personalisation, e.g. generation of keys*		*O.4, O.6*	*Conform to ICAO Doc 9303*	*ICAO - 6*
V.40	*Insufficient cryptographic key protection (e.g. production keys)*		*O.4*	*Usage of security modules, e.g. compliant to FIPS 140-2 level 2 or equivalent*	*ICAO - 8.2*
		Generic			
V.41	Insufficient physical security		O.1		ICAO 7, ISO2.Ch9
V.42	*Insufficient logical/network access controls in personalisation systems*		*O.2, O.4*	*Usage of Common Criteria*	*ISO2.Ch11*
V.43	*Insufficient security in Systems Development Life Cycle of personalisation systems*		*O.2*		*ISO2.Ch12*
Delivery					

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
V.44	Identity of collecting person is insufficiently verified		O.1, O.3	Use all biometrics to verify the identity of the e-passport holder before delivery	ICAO 5.3
V.45	e-passport delivered via mail or third person		O.1	Request for receipt of confirmation upon delivery	ICAO 5.3
V.46	E-passports not collected are not inventoried and invalidated		O.1, O.4	Monitor and destroy passports that have not been picked up	ICAO 5.3
		Generic			
V.47	Insufficient physical security		O.1, O.4	Store and transport already personalised e-passports securely	ICAO 7, ISO2.Ch9
Usage					
V.48	*Chip can be disabled*		*O.3, O.4, O.5*	*Issue a procedure to follow when a (partially) non-functional e-passport chip is found during border control*	-

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
V.49	*Chip communication can be jammed*		*O.3, O.6*	*Issue a procedure to follow when a (partially) non-functional e-passport chip is found during border control*	-
V.50	European National Identity Cards (or any other accepted travel documents, like residence permits) can be used if they are less secure than the e-passport		O.5	Ensure that all travel documents accepted for international travel have the same security level	-
V.51	*Insufficient guidance provided by border system to border guard*		*O.5, O.6*	*Clear communication of different results of inspection procedure (e.g. failure of PA, AA, EAC or biometric matching?)*	-
V.52	Insufficient quality of e-passports		O.4	Sufficient quality controls in issuance process	ICAO – 5.2
V.53	*False fingerprints during border control ("gummy fingers")*		*O.1*	*Training and vigilance of border guards or high-quality inspection systems*	-

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
V.54	*Insufficient operational ability for border control to evaluate security mechanisms (BAC, PA, AA, EAC) of the e-passport*		*O.4, O.5*	*Have all necessary systems (and related infrastructure, for example for EAC) and training available for border guards*	-
V.55	Insufficient reporting or registration of lost/stolen e-passports		O.4		ICAO 10
V.56	*Inability to verify biometrics during border control*		*O.3, O.5*	*Proper procedures and equipment*	-
V.57	Too long validity time of e-passport		O.3, O.4	Recommended at five years	ICAO 6.4
V.58	Multiple passports per person		O.3, O.4	Only provide one valid passport to one person. Invalidate old passports immediately.	ICAO 6.4
V.59	*Insufficient biometric quality*		*O.3*	*Quality control during issuance*	*ICAO - 5.2*

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
V.60	*Insufficient integrity protection of (storage of) public key certificates (DS certificates, CSCA)*		*O.6*	*- Use a trusted source for DS, CSCA certificates (e.g. bilateral or ICAO PKD)* - Use an integrity checking mechanism to validate that certificates may be used in inspection operations	-
V.61	*Insufficient confidentiality protection of (EAC) private keys*		*O.4, O.6*	*Usage of security modules, e.g. compliant to FIPS 140-2 level 2 or equivalent*	-
V.62	*Insufficient border guards available when border control systems are not available*		*O.5*		*ISO2.Ch14*

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
V.63	*Automated border control eliminates human experience and expertise in border checks*		*O.5*	Randomly select travellers to go through a manual border check after passing the ABC check As the secondline check requires additional expertise, we recommend using only ABC for first line control.	-
		Generic			
V.64	Insufficient logical/network access controls in border control systems		O.4, O.6		ISO2.Ch11
V.65	Insufficient security in Systems Development Life Cycle of border control systems		O.6	Develop inspection systems with high security requirements Common Criteria evaluation	ISO2.Ch12
Invalidation					

Life cycle step	Vulnerability	Explanation	Incident outcome	Relevant, specific Countermeasures	Ref
V.66	Insufficient registration of lost/stolen passports		O.3, O.4	Keep a central registry of invalidated e-passports (e.g. SIS, Interpol SLTD[11] database), accessible to all relevant relying parties.	ICAO 10
V.67	Insufficient public awareness of the need to report stolen or lost passports		O.3		ICAO 10
V.68	*Inadequate e-passport destruction upon invalidation*		*O.3, O.4*	*Disable or remove and destroy the e-passport chip*	-
		Generic			
V.69	Insufficient physical security		O.1		ICAO 7, ISO2.Ch9

Vulnerabilities given in *Italics* are specific for e-passports. Other vulnerabilities are also applicable to other travel documents.-

[11] Stolen and Lost Travel Document

5. *Questionnaire results*

5.1. *Conclusions from the questionnaire*

Below we have summarised the main conclusions from the questionnaire focusing on possible risks identified. Further details can be found in Section 5.3 (issuance), Section 5.4 (technical security) and Section 5.5 (usage) below.

The reliability of the e-passport issuance process is considered vital for EU border control by the respondents, but they indicate significant lack of harmonisation on issuance of passports among Member States.

A substantial majority of the respondents indicate that vulnerabilities in the national e-passport issuance process might cause unauthorised border passage. This emphasises the importance of the issuance process in EU border control. The questionnaire results also indicate that there is a significant lack of harmonisation on the issuance of passports among EU/Schengen Member States. To this end, multiple respondents indicate non-compliance with recommendations for the *ICAO guidelines on assessing the security of handling and issuance of travel documents*, even though it is generally agreed that these guidelines form a good basis to secure the issuance of e-passports.

Some examples of possible non-compliance are:

- Issuance process is not under dual control
- Regular audits at passport offices are not performed
- Screening of personnel is not always employed
- Abroad issuance process security is not equivalent to domestic process
- E-passports are not always stored in safes
- E-passports are sometimes sent by regular mail.

Lookalike fraud (a.k.a. imposter fraud) with legitimate e-passports is considered a substantial risk for EU border control by half of the respondents. Approximately 40% of the respondents indicate that better quality of the facial image stored in the chip would contribute to a reduction in lookalike fraud.

- Individual comments indicate that lookalike fraud is specifically relevant in the context of automated border control.
- Respondents indicating that lookalike fraud is not a substantial risk refer to the usage of fingerprints, which are hardly used.

Although all Member States are required to issue e-passports since August 2006, only around half of the Member States actually read the chip in first-line border control. Some of the Member States do not intend to start reading the chip.

The situation of fingerprint reading appears to be even worse, with the possible exception of one or two Member States, fingerprint verification does not yet take place. Some respondents indicate that the e-passport cannot be read at the passport office either.

Many Member States experience operational problems in employing or deploying the public key infrastructures supporting the e-passport inspection.

- All respondents indicate that the Document Signer (DS) certificate required for Passive Authentication verification is available in the e-passports. Formalisation of this would eliminate the need for DS certificate exchange via the ICAO PKD or via any other means.

This would make certificate exchange simpler, since the (long-lived) CSCA root certificates are exchanged bilaterally anyway.

- Although twelve Member States indicate that they have exchanged CSCA root certificates for Passive Authentication verification bilaterally, only six indicate that they participate in the ICAO PKD (at the time of the questionnaire, December 2010). Of these Member States, only four have already made information available via the ICAO PKD and no countries seem to use the information available about other countries from the ICAO PKD in their own inspection infrastructure.

- In many countries, the verifying PKI, needed to access fingerprint data on second-generation e-passports, is not yet operational. 10 countries indicate that they already issue CVCA certificates, but only four have an SPOC up and running for exchanging such certificates and many have not yet implemented fingerprint verification at inspection.

Cloning of e-passport chips is considered a serious concern by the respondents, but not all Member States currently issue e-passports with mechanisms to verify the authenticity of the chip. Moreover, when e-passports support these mechanisms, not all Member States currently use these mechanisms while reading the e-passport.

Active Authentication and Chip Authentication are security mechanisms meant to prove the authenticity of the chip i.e. to prevent cloning of the chip (data). This is especially relevant in automated border control where the physical security features of the e-passport are checked less thoroughly or hardly checked at all. In ABC systems, a cloned chip could suffice to pass border control in case the chip data of a lookalike is available, certainly if the threshold for automated biometric verification is low.

Support of Active Authentication is left optional in both ICAO guidelines and the supplementary EU agreements. Chip Authentication is part of Extended Access Control and, according to EU agreements, it should be present in second-generation e-passports. When Chip Authentication is supported by the chip and verified by the inspection system, Active Authentication does not add to the security.

Five Member States indicate that their first-generation e-passports do not support Active Authentication. For second-generation e-passports, three Member States indicate that their e-passports do not (yet) support Extended Access Control and, hence, Chip Authentication. These Member States may, however, support Active Authentication. For second-generation e-passports, four countries indicate that they do not support Active Authentication. Although Chip Authentication can replace the functionality of Active Authentication, support of Active Authentication is relevant when Chip Authentication is not supported by the inspection system.

National identity cards of Member States are also accepted as travel documents at the EU/Schengen border. As the security of national identity cards is not standardised, they might be considered as a weak link in border control.

Ten Member States indicate that their national identity card is used as a European travel document. Eight Member States indicate that their national identity card conforms to ICAO Doc 9303 part 3, five Member States indicate that it does not. Please note that this may only mean compliance to part 3, Volume 1 (physical characteristics) and not Volume 2 (chip characteristics), i.e. the identity card does not necessarily contain a chip or an ICAO compliant chip. Six Member States indicate that their national identity card contains a chip, five indicate that it does not. The chip may also be a contact chip.

Since national identity cards are not standardised like e-passports, the security features may vary and national identity cards of some Member States may be more sensitive to fraud than those of others. Besides, because national identity cards are not standardised, interoperability when trying to read the chip is not guaranteed.

One respondent indicates that the technical security of their e-passports is not certified against the applicable Common Criteria protection profiles and not all respondents confirm that they do. Not all Member States seem to be in the process of phasing out the usage of the SHA-1 hashing algorithm as part of signing e-passport information.

- According to C(2006) 2909 [2], Member States are required to have their e-passport certified against specified Common Criteria protection profiles.

- E-passport information is digitally signed (Passive Authentication) to ensure its authenticity. As part of the digital signature algorithm, a so-called secure hashing function is used. Until cryptographic vulnerabilities were discovered in the SHA-1 secure hashing algorithm in 2005, it was commonly used in the context of e-passports. Since the end of 2010, the SHA-1 secure hashing algorithm is no longer considered suitable to be used in digital signatures, e.g. to sign information in e-passports. Compare NIST Special Publication 800-57 [48].

5.2. *Questionnaire set-up*

The questionnaire was published online and over 100 people across Europe (and the US) were invited to complete the questionnaire. This group consisted mostly of European border guards or e-passport issuance officials, but also includes industry experts and relevant international organisations (like Interpol). The questionnaire was divided into six parts, a general part applicable to all participants and five specific parts that were presented only to the respondents if they indicated that they had expertise or experience in the respective field. These parts are:

1. General (personal information, expertise and first risk assessment)

2. Issuance of e-passports

3. Technical production of e-passports

4. Functional usage, focusing on border control

5. Technical usage of e-passports

6. Policymaking

The questionnaire was online during the period 16 November to 31 December 2010.

5.2.1. Questionnaire responses

We would like to thank all respondents for the time and effort they have spent in completing the questionnaire. Total 59 people have responded to the questionnaire, of which 35 have fully completed it. A list of respondents is included in Appendix A.2.

Respondents are officials of Belgium, the Czech Republic, Estonia, European Commission, Finland, France, Germany, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, the United Kingdom and Interpol.

Given the number of respondents and the fact that not all countries responded in equal numbers, we can only use the questionnaire results indicatively and as a basis for further discussion.

5.3. *Results on issuance*

5.3.1. Main results

In this section, the results of the issuance questions in the questionnaire are discussed[12]. Only the most relevant/interesting results are discussed here, especially results where there is no consensus between different Member States or indicative of high risk issues. These are presented along the following three topics:

- General
- Application and entitlement
- Production, delivery and invalidation.

General

The value of a secure e-passport issuance process is considered high by most of the respondents (75%), as they consider a poorly secured issuance process to result in an increase of illegal/unauthorised border passages.

Over half (55%) of the questionnaire respondents indicate that the governance of e-passport issuing is not centralised in a single (government) organisation within their country. Although we could not deduce any further information on how scattered the e-passport exactly is, it is generally considered harder to secure e-passport issuing (as it is for any other process) without assigning this responsibility to a single entity. At the same time in a large majority (90%) it is considered that there are already sufficient security guidelines in place at a national level secure e-passport issuing.

In line with these results, many respondents (75%) do not see a need for additional EU guidelines/regulation and consider the existing ICAO guidelines suitable and appropriate to provide guidance in securing the e-passport issuance process. However, half (50%) of the respondents indicate that no regular audits on all parties involved in the issuance process takes place, so not for all countries it is certain that the guidelines are sufficiently followed.

Some interesting other results are:

- More than half the respondents (60%) indicate that higher-quality images than those currently in DG2 would contribute to a substantial further detection of lookalike fraud.
- Only some respondents (15%) indicate that the issuance process abroad (e.g. embassies) is less secure than the domestic issuance process.

Application and entitlement

The questionnaire responses show that applications are processed very differently in the EU/Schengen countries. For instance, about half (45%) of the respondents indicate that there is no distinction between a first-time application and a renewal, while the other half do make this distinction. Furthermore, some countries can use alternative (trusted) sources to verify the application (e.g. a national citizens registry), while a significant minority (25%) can only rely on

[12] This relates to questionnaire questions 8-47 and 124-127

paper documents (e.g. birth certificates) provided by the applicant to establish the applicant's identity.

Another example is that the countries' national ID card is generally accepted as sufficient evidence to establish the applicant's identity, while the security of the national ID card varies widely per Member State.

There is a high level of variation with respect to how the loss history of an applicant is used. All countries indicate that they register reports of lost/stolen e-passports; however, only a minority (40%) of respondents indicate that this information is considered when a new application is processed.

The respondents indicate that facial images are captured very differently per Member State. Some countries require applicants to bring their own photo, while others require a photo to be captured during application at the application station (15%). Generally, these two options are both available to applicants. An interesting result is that the majority of respondents (60%) indicate that an increase in the quality of the captured (and stored in DG 2 of the e-passport) facial image could significantly improve the detection of lookalike fraud during border control.

The questionnaire responses also show a different approach with respect to personnel security related to issuance officers. Some respondents (30%) indicate that e-passports are regularly issued under single control and others (30%) that not all issuance officers are screened.

Production, delivery and invalidation

A single respondent indicated that in his country the personalisation of e-passports is performed in a local passport office. Other countries seem to personalise e-passports in a single or limited number of central locations, which are generally well secured.

The delivery of the e-passport is generally done at many locations (e.g. local town halls or police stations), so securing all these locations is much harder. This is visible in the questionnaire results, where respondents indicate that for some countries personalised e-passports awaiting delivery are not stored in safes (25%) or that delivery of e-passports is done via regular or registered mail (1 respondent).

Also how e-passports are treated at the delivery station varies:

- For half of the countries (50%), the delivery officers are not (properly) trained to establish the identity of the collecting applicant, before the e-passport is delivered.

- Some countries (25%) indefinitely keep uncollected e-passports at the local passport office/delivery station awaiting pickup.

- Half of the respondents (50%) indicate that the biometrics contained in the e-passport (facial image and fingerprints) cannot be matched against the collecting applicant, due to insufficient equipment available in the local passport office to read and match biometrics.

All respondents indicate that when a new e-passport is issued the old e-passport is usually invalidated. To invalidate the old e-passport, various methods are deployed, which are not all effective to invalidate/destroy the e-functionality of the e-passport (e.g. by punching a hole in the data page). Furthermore, some respondents (35%) indicate that there are exceptions (e.g. when a valid visa remains on the old e-passport) where the old e-passport is not invalidated at all.

5.3.2. *Detailed results*

This section describes the results of the questionnaire related to issuance in more detail.

5.3.2.1. General

5.3.2.1.1. Life cycle steps (question 19)

All respondents support the high-level life cycle steps as depicted in the questionnaire and in the life cycle description of Chapter 4.

5.3.2.1.2. Security organisation (questions 39-44, 124-127)

Half of the respondents (50%) indicate that a single organisation within their country is responsible for the whole issuance process. As a result, for the other half there is no single organisation present.

A large majority of respondents (85%) indicate that issuance abroad is as secure as domestic issuance. Some issues mentioned here are transportation of blank booklets to the embassies and delivery of personalised e-passports in remote areas (sometimes via mail).

Most respondents (90% at a national level and 65% at an EU level) consider that sufficient security guidelines are in place to properly secure the issuance process over all parties involved. All respondents consider the ICAO Guidelines to form a good basis. Some respondents indicate that these ICAO Guidelines are currently used to improve existing procedures. FIPS 140-2 is widely used as a standard for cryptographic key management. Respondents mention the following topics as especially important for guidance: setting up PKI and SPOC infrastructure, choosing DVCA algorithm suites, issuance procedures, physical security, secure transportation, vetting of staff and establishing the applicant’s identity.

Almost half of the respondents (40%) indicate that not all parts of the issuance process (application, entitlement, production and delivery) are regularly audited.

5.3.2.2. Application and entitlement

5.3.2.2.1. Application offices (questions 9-10)

The responses show that application offices are organised in different ways in different countries. With respect to domestic applications, the majority (55%) of respondents indicate that citizens can apply for an e-passport in any application office, while 25% of respondents indicate that a citizen can only apply at his/her local application office.

Abroad this is reversed, as 55% percent of respondents indicate that a citizen can apply only at his/her local consulate/embassy for an e-passport and approximately 25% at any consulate/embassy in the world.

5.3.2.2.2. First-time application (questions 11- 13)

Two-thirds (65%) of the respondents indicate that a first-time applicant is additionally scrutinised. The additional scrutiny can range from an interview to additionally required evidence of identity (e.g. birth/naturalisation certificates, statements of relatives, national ID cards, etc.). Especially, ID cards are often mentioned by respondents.

A small number of respondents (25%) indicate that applications where the old passport expired over two years ago also receive additional scrutiny.

5.3.2.2.3. Biometrics capturing (question 14)

With respect to the facial image, 40% of respondents answer that an applicant must always bring his/her own photo, 15% answer that the facial image must be captured during application and 65%

are somewhere in the middle (either both is possible or the image must be made at a licensed [i.e. trusted] photographer's).

5.3.2.2.4. Evidence of identity (questions 15-18)

We have asked respondents to indicate what kinds of sources are used in order to:

A. Establish that the claimed person (ever) exists

B. Establish that the claimed person is not deceased

C. Establish that the claimed person matches the applicant

D. Establish the claimed person's whereabouts (supporting information on the applicant's identity)

Only a small number of respondents (25%) indicate that they want to achieve D. Most of the respondents indicate that they want to achieve A-C (A, 75%, B, 50%, C, 70%). In order to achieve these goals, approximately 80% utilise a trusted government source (e.g. a citizens' registry), while 20% only rely on applicant-supplied documents.

During application, all respondents indicate that presented identity documents are checked against a stolen document database and that the loss history of the applicant is investigated. However, only 35% of respondents answer that a suspicious loss history can be grounds to refuse issuing a new e-passport.

5.3.2.2.5. Personnel security (questions 45-47)

We have asked respondents to indicate per issuance officer type (application officer, entitlement officer, personalisation officer and delivery officer) how training, screening and job experience is managed. In general, half of the respondents (50%) indicate that official training is given to issuance officers, while 75% indicate that screening is mandatory for such positions. Only a small number of respondents (30%) answer that training with respect to verifying the authenticity of personal documents and official tests to finish such training are done.

The emphasis with respect to training, screening and job experience seems to go to application and personalisation officers and not to entitlement or delivery officers, although the differences are (very) small.

5.3.2.3. Production

5.3.2.3.1. Physical security of production (questions 20-24, 27)

A large majority of respondents (80%) indicate that production of blank e-passports and personalisation are performed at central, but distinct locations. Transportation between these two locations takes place via a dedicated secure delivery service (50%) or via a secure commercial parcel delivery service (35%). Some respondents indicate that local personalisation takes place for regular e-passports or in the case of emergency passports.

5.3.2.3.2. Accounting and quality assurance during production (questions 25, 26, 28, 29)

Respondents indicate that various techniques are used to ensure accounting for produced (blank) e-passports. These include: using a trusted (government) supplier (e.g. a National Mint), usage of production and transport keys which are kept separate from the physical chip/document, serial numbering and strict stock management with accounting/control procedures.

The respondents answer that quality control procedures focus mostly on the physical quality of the chip and e-passport booklet (70%) and less on the quality of supplied biometrics (facial image (50%) and fingerprints (35%)) and quality of the personalisation (50%).

5.3.2.4. Delivery and invalidation

5.3.2.4.1. Delivery and invalidation of passports (questions 30-35)

Unsurprisingly respondents indicate that e-passport can be picked up by the applicant. 35% of the respondents indicated that an e-passport may also be picked up by a person other than the applicant, as long as he or she is authorised by the applicant to do so. A small number of respondents (10%) indicate that e-passports may be delivered via (secure) mail service.

Awaiting pickup, the e-passports are regularly stored in safes, however not in 35% of the cases. When the applicant fails to pickup his/her e-passport, the e-passport is usually destroyed after a waiting period. 20% of respondents indicate that e-passports awaiting pickup are stored indefinitely.

The vast majority of respondents (95%) answer that old passports are invalidated upon delivery of a new passport. However, there are some exceptions as 35% of respondents indicate: in case of need for two passports (e.g. Arab states and Israel) or when still valid visa reside on the old passport.

E-passports are physically invalidated by registering it as invalidated (e.g. in SIS), cutting the MRZ, puncturing holes in the booklet or disabling the antenna. However, this commonly does not irreparably disable the e-passport chip itself.

5.3.2.4.2. Quality controls at delivery (questions 36-38)

Some respondents (30%) answer that it is not technically possible in their country to check/read the e-passport functionality at the delivery station. Furthermore, half of the respondents indicate that reading the fingerprints is not (yet) technically possible. Only one respondent indicates that reading the fingerprint upon delivery is mandatory.

5.4. *Results on technical security*

This chapter describes the results of the questionnaire related to technical security. It should be noted that the outcomes are sometimes ambiguous since some questions have been interpreted differently by different respondents; respondents from the same country sometimes give contradictory answers. Also, for some questions we only have answers from respondents of relatively few countries, so one has to be careful in extrapolating these results or treating them as being representative of all EU countries.

5.4.1. *Main results*

There is some diversity when it comes to EU e-passports when it comes to the support of Active Authentication (AA), as support for this is left optional in both ICAO Guidelines and the supplementary EU agreements. There seems to be an even split between having AA or not in first-generation of e-passports, where AA is the only way of establishing authenticity of the chip.

Some Member States have been using SHA-1 as hashing algorithm, and not all seem to be in the process of phasing this out, though some are.

People report few compliance problems with the passports they issue, which seems to contradict some experiences in inspection, and calls by some interviewees for having defect lists.

According to the respondents, the majority of countries certify their e-passports against the applicable Common Criteria protection profiles, but one respondent say they do not, and not all respondents confirm that they do.

All respondents say they supply the Document Signer certificates in e-passports, implying that these need not be available in the inspection systems (obviously the country signing certificates need to be available).

Many Member States already have exchanged CSCA root certificates for Passive Authentication. Less than half of the Member States participate in the ICAO PKD. Not all of these countries have already made all information available to the ICAO PKD, and apparently no countries seem to be using information from the ICAO KPD for their own inspection systems yet.

Still, support for the signing PKI is more developed than support for the verifying PKI, needed to access fingerprint data on secondgeneration e-passports. Many countries already issue CVCA certificates, but less than half of these have an SPOC up and running for exchanging such certificates.

5.4.2. *Detailed results*

This chapter describes the results of the questionnaire related to technical security in more detail.

5.4.2.1. Passports with chip (e-passports)

5.4.2.1.1. Protection profiles (questions 62, 63)

A majority of countries (9 and 7 respectively) indicate their e-passports are certified against the Common Criteria Protection Profiles BSI-CC-PP-0017/0055 (Basic Access Control) and BSI-CC-PP-0026/0056 (Extended Access Control). Not all respondents confirm that Common Criteria certifications take place for their e-passports. Only for one country does a response indicate that there is no Common Criteria certification.

5.4.2.1.2. Physical layout (questions 53, 54)

Eight (8) countries indicate that the chip is in the data page of the e-passport, six (6) indicate it is in the cover. For nine (9) countries, the chip antenna is located behind the data page containing the MRZ when the passport is open and the MRZ is read via optical character recognition, two (2) indicate that the antenna is facing the data page. For DE, the situation is not clear since different respondents give different answers.

5.4.2.1.3. E-passport application (questions 55, 56, 57)

According to the responses to question 55, there are no other applications in the chip besides the e-passport application. The countries are not aware of any non-compliancy issues regarding ICAO Doc 9303 or EC 2252/2004 for their e-passports.

5.4.2.1.4. Technical security (question 85)

Three countries indicate that SHA-1 has not been used within the e-passport context, and five countries indicate that it has been or is used. One country indicates that there are no plans to stop using SHA-1, for one country it is unclear when use of SHA-1 will be finished, and one country indicates that use of SHA-1 will be stopped by 2012.

5.4.2.2. Security mechanisms

5.4.2.2.1. Passive Authentication, Signing PKI, and ICAO PKD (questions 64, 66, 67, 68, 69, 70, 71, 72, 73, 74, 81, 82 83, 111, 112, 113)

Quite a few countries (12) have exchanged their CSCA root certificate for Passive Authentication with other countries. All respondents indicate that their e-passports have the DS certificate available in the chip.

Regarding use of the ICAO PKD: six (6) countries indicate that they participate in the ICAO PKD and eight (8) indicate that they don’t. Of the latter, all have plans to start participating in the ICAO PKD, not all of these countries already know when participation will start. Uploading information to the ICAO PKD is the responsibility of the Ministry of Interior, the Ministry of Justice, the police, or national security agency. In all but one country, this is the same party which is also responsible for the SPOC.

Four (4) countries indicate that they have their information available via the ICAO PKD, i.e. DS certificates (all 4 of these countries), CRLs (all 4), CSCA link certificates (3), and/or Master lists (2). However, three of these countries indicate in another question that they will only start making this information available via the ICAO PKD in 2011. No country seems to use the information available in the ICAO PKD from other countries for their own inspection systems, but this may also be due to a lack of available information in the ICAO PKD. Information provided by Master lists is not trusted by the countries which have answered question 112.

Seven (7) countries indicate it takes less than 48 hours to place a revoked certificate on the CRL. Six (6) countries indicate that CRLs are (also) distributed via means other than the ICAO PKD as e.g. bilaterally or via the World Wide Web (a website).

Nine (9) countries indicate the cryptographic key lengths and eight (8) countries indicate the validity periods of CSCA and DS keys and certificates are in line with the recommendations from ICAO Doc 9303. Two countries indicate that there is a maximum number of e-passports signed with the same DS private key, one country indicates that this maximum number is 100000.

5.4.2.2.2. Active authentication (questions 58 & 59, 60, 83)

For their first-generation e-passports four (4) countries indicate some or all of these e-passports support Active Authentication, five (5) countries indicate that they don’t, and six (6) countries have not answered this question. For NL different respondents give conflicting answers (though we know that first-generation passports from NL do support AA). For second- generation e-passports, six (6) countries indicate that they support Active Authentication, four (4) indicate that they don't, and five (5) have not answered this question. There are no countries which plan to change support of Active Authentication in their e-passports. Nine (9) countries indicate that the cryptographic key length of the AA key pair is in line with the recommendation from ICAO DOC 9303.

5.4.2.2.3. EAC, Verifying PKI and SPOC (questions 48, 60, 75, 76, 77, 78, 79, 80, 81, 82, 84, 115, 118, 121, 122, 123)

Eleven countries indicate that their e-passports are compliant with EC directive 2252/2004 and hence support EAC. UK, BE and MK do not have fingerprints in the e-passport and hence do not support EAC. One country indicates that it will issue e-passports with fingerprints and EAC from 1 March 2011. One country indicates that it does not have plans to start issuing e-passports with EAC.

Ten (10) countries indicate that they issue CVCA certificates. CVCA certificates are required to store as trust points in e-passports with EAC. Countries indicate that they are exchanging (or plan to exchange) verifying certificates and DVCA certificate requests via an SPOC (4) or via other means e.g. bilateral (4). Four (4) countries indicate that they have an SPOC in place, six (6) indicate that they don't have this yet. The SPOC is either under the control of the Ministry of Interior, the Ministry of Justice, the police, or national security agency. In all but one country, this is the same party which is also responsible for uploads to the ICAO Public Key Directory. Six (6) countries have indicated that processing a foreign DVCA certificate request by their CVCA should take less than 96 hours. None of the countries have indicated that it should take more than that. Quite a few countries have not answered the technical questions regarding the verifying PKI. One country has indicated that it normally takes more than 96 hours before its DVCA certificate request is processed by other countries. Nine (9) countries indicate that the validity periods of the CVCA and DVCA certificates are in line with the recommendations from EC 2909/2006.

5.5. *Results on usage*

This chapter describes the results of the questionnaire related to inspection. It should be noted that the outcomes are sometimes ambiguous since some questions have been interpreted differently by different respondents; respondents from the same country sometimes give contradictory answers.

5.5.1. Main results

5.5.1.1. EU MRTDs and MRTD inspection

The questionnaire results show that the last EU passports without chip will expire in 2017 and that almost all EU Member States will issue e-passports according to the EU-passport specification.

The questionnaire results also show that most Member States' national identity cards are accepted as travel documents. However, not all national identity cards contain a chip, and not all chips in identity cards conform to the chip specification of e-passports.

Regarding inspection at border control: about half of the Member States always or usually read the chip at first line border control. Some Member States do not read the chip and do not intend to start reading the chip. A broken chip leads to first line manual inspection.

Most respondents perceive fingerprint verification as a major solution to lookalike fraud. (This seems at odds with other findings, notably the responses concerning fingerprints discussed in 5.5.1.2 and 5.5.2.2.3 below.)

5.5.1.2. Biometric verification

When the chip is read at border control, the face images stored in the chip is almost always displayed to the border guard. Automated biometric verification of the face only takes place in a limited number of Member States and independent of the situation at border control (manned booth, mobile reader, automated border control system).

The quality of the facial image is not always good. Respondents believe that lookalike fraud can be reduced by improving the facial image quality.

Fingerprint verification does not (yet) take place at border control, except perhaps in two Member States at second line border control and perhaps in one member state at first line border control. Its cost effectiveness is doubted by some respondents. Also the quality of the stored fingerprints and the resulting automated biometric verification is doubted. Some respondents consider the verification time too long. This results in the decision taken by some countries that they will not implement fingerprint verification at (first line) border control.

5.5.2. Detailed results

5.5.2.1. Travel documents (questions 48, 49, 50, 51, 52 & 61)

The majority of respondents, eleven (11) Member States, indicate that all e-passports they are issuing comply with EC 2252/2004 i.e. contain fingerprints protected via EAC. Four (4) Member States indicate that their e-passports are not (yet) compliant. UK, MK, and BE indicate that fingerprints are not included. MK will have a compliant e-passport as of 1 March 2011.

Nine (9) Member States indicate that they issue emergency passports without chip. The responses indicate that all diplomatic and service passports contain a chip.

Six (6) Member States indicate a passport validity period for adults of 5 years and nine (9) Member States indicate a passport validity period for adults of 10 years. CZ, NO, LU, and LV have a limited passport validity period for children. Of the Member States who responded to the question about start and stop dates of issuing certain types of passports, the last stopped issuing passports without chips in 2007. Combined with the answer on the validity period of the passport for these Member States, this means there will be valid passports without chip till at least 2017.

The majority of respondents, ten (10) Member States, indicate that their national identity card is used as a European travel document, three (3) indicate that it does not and two (2) have not answered. Eight (8) Member States indicate that their national identity card conforms to ICAO Doc 9303 part 3, five (5) Member States indicate that it does not. The situation for DE is not clear since different respondents give different answers. Please note that this may only mean compliance with part 3 Volume 1, i.e. the identity card does not necessarily contain a chip. Six Member States (6) indicate that their national identity card contains a chip, five (5) indicate is does not. When the requirements in the chip in the national identity card are not same as for the chip in the e-passport, the respondents indicate that this is because a contact chip is used in the national identity card (BE, EE) or the national identity card has stronger access control (DE) to better protect the holder's privacy.

5.5.2.2. E-Passport inspection

5.5.2.2.1. Reading of the MRZ and the chip (questions 88, 89, 90, 91, 92, 93, 94, 95, 96)

Twelve (12) Member States indicate that the optical MRZ on the data page is always or usually read at first line border control, in one Member State this is done occasionally, but this Member State plans to start doing this on a regular basis in 2011. In nine (9) Member States, the optical MRZ is always, usually or occasionally compared to the MRZ in DG 1 (not implicitly via BAC). Apart from border control, the optical MRZ is read at check-in (7 Member States) and boarding (4 Member States).

The results of the questionnaire show that seven (7) Member States always or usually read the chip in the e-passport at first line border control, and five (5) only occasionally or never read the chip. The situation of NL is unclear since the answers from the respondents differ from usually via occasionally to never (since technically not possible). Four (4) Member States indicate that they have plans to start reading the chip at first line border control between 2011 and 2013, two (2) Member States explicitly indicate that they do not have plans to start reading the chip at first line border control. Apart from border control, the chip is rarely used.

When the chip is read at first line border control, ten (10) Member States indicate that they perform BAC (this is necessary to be able to read the chip at all), five (5) indicate that they perform PA, four (4) that they perform AA, five (5) that they perform CA and two (2) that they perform TA. This contradicts with the fact that at least one of these particular Member States does not yet issue IS certificates as follows from another question in the questionnaire.

If Member States read the chip, they occasionally or regularly encounter technical issues with inspection of EU passports of countries other than their own and more frequently with non-EU passports (e.g. problems reading the MRZ, initiating the RF communication between chip and reader, problems regarding the cryptography) (please refer to Section 5.5.2.2.4).

5.5.2.2.2. Facial verification at border control (questions 98, 99, 100, 101, 102, 103, 127)

The image from the chip is displayed to the border guard at first line inspection in eight (8) Member States. Three (3) Member States do not show the picture from the chip and for one (1) Member State the situation is not clear. Automated facial image verification takes place sometimes or always in a limited number of Member States for manned booths (4 Member States) and mobile readers (5 Member States). Answers for Member States are not always very clear since respondents from the same Member State give contradicting answers. The question whether there are plans to start automated facial image verification if not done yet, has not been answered by the respondents. In case of ABC system, automated verification of the facial image always takes place in five (5) Member States and not in four (4) others. It is not clear from the questionnaire if these latter Member States make use of another form of biometric and possibly also an additional secure document/token.

For second line border control, the facial image from the chip is verified manually or automated in eight (8) Member States. This is not done in four (4) other Member States.

40% of the respondents think that better quality of the facial image stored in the chip would contribute to reduction in lookalike fraud.

Some respondents encounter problems with automated face verification in EU passports due to the bad quality of the stored image. Also unknown errors regarding automated face verification occur and errors because of the wrong image stored in the chip (error in personalisation or issuance process). About half of the Member States have standard procedures when errors occur during face verification or when face verification fails, half indicate they do not.

5.5.2.2.3. Fingerprint verification at border control (questions 75, 76, 104, 105, 106, 115, 128, 129)

All Member States but one indicate that fingerprint verification at first line border control does not take place. One respondent of a certain Member State indicates that verification of fingerprints at first line border control takes place in approximately 10% of the cases, although a second respondent of this Member State indicates that this does not take place.

All Member States but two indicate that fingerprint verification at second line border control does not take place. One respondent of a certain Member State indicates that verification of fingerprints at second line border control takes place in approximately 50% of the cases, although a second respondent of this Member State indicates this does not take place at all. One respondent of another Member State indicates that verification of fingerprints at second line border control takes place in approximately 5% of the cases, although a second respondent in this Member State indicates that this does not take place.

Four Member States indicate that there are no plans to start fingerprint verification at second line border control, 5 Member States indicate that they have plans to start doing this, for one Member State the respondents are in disagreement. The date on which Member States think to have fingerprint verification operational varies between 2011 and 2017.

Ten (10) Member States (77 % of the respondents) think cost effectiveness of fingerprints to prevent lookalike fraud is good or neutral. Three (3) Member States (23 % of the respondents) think that cost effectiveness is bad or very bad. Some Member States are working on implementing fingerprint verification, others have decided not to implement. Quite a few Member States have a verifying PKI in place and have their DVCA certificates signed by other countries via the SPOC or via other means so this does not seem a limitation for implementation.

Mentioned possible barriers to use fingerprints at border control are:

- PKI infrastructure with certificate exchange, key management, etc. for all is considered too complicated or too expensive (for first line border control)

- Quality of fingerprints

- Verification time (too slow)

- Not enough advantage over face biometrics
- Acceptance by the public (linked too much to criminal investigations)

5.5.2.2.4. Problems at inspection (questions 86, 97)

The responses indicate Member States are not aware of problems by other EU countries with inspection of their e-passports.

Seven (7) Member States have standard procedures when the chip cannot be read, two (2) indicate they have not. For two (2) Member States, the answers from different respondents do not match. When one of the security mechanisms fails six (6) Member States have standard procedures and three (3) do not. For one (1) Member State, the situation is not clear.

The following diagram shows how often specific problems are encountered with national, EU- and non-EU passports according to the respondents. Please note that these are the numbers of individual respondents, not by Member State. Total 20 respondents have answered these questions. Sometimes they chose not to answer, probably because they did not have experience with a verification mechanism.

Problem	***Passports***	***Never***	***Occasionally***	***Usually***
MRZ cannot be read due to OCR problems	Own passports	9	3	0
	EU passports	3	7	1
	Third country passports	0	11	1
Metallic shielding prevents reading of chip	Own passports	9	1	0
	EU passports	7	2	0
	Third country passports	4	7	0
Chip cannot be read due to low-level problems	Own passports	7	4	0
	EU passports	4	6	0
	Third country passports	1	9	0
Chip and MRZ cannot be simultaneously read, e.g. due to the antenna location with regard to MRZ and/or the passport reader geometry	Own passports	10	1	0
	EU passports	4	5	0
	Third country passports	6	5	0

Basic access control failed	Own passports	7	5	0
	EU passports	3	8	0
	Third country passports	1	9	1
Passive Authentication failed due to non-correspondence of hashes	Own passports	7	1	0
	EU passports	4	4	0
	Third country passports	2	6	0
Passive Authentication failed because DS certificate is not available/cannot be read	Own passports	7	1	0
	EU passports	3	5	0
	Third country passports	2	5	0
Passive Authentication failed because CSCA certificate is not available	Own passports	6	2	1
	EU passports	1	5	2
	Third country passports	1	5	1
Passive Authentication failed because signature is incorrect	Own passports	7	1	0
	EU passports	4	3	0
	Third country passports	3	3	0
Passive Authentication failed because of another reason	Own passports	4	3	0
	EU passports	3	1	0
	Third country passports	3	2	0
Active Authentication failed	Own passports	5	1	0
	EU passports	3	1	0
	Third country passports	3	1	0
Chip Authentication failed	Own passports	3	2	0
	EU passports	2	1	0
	Third country passports	2	2	0
Terminal Authentication: No complete certificate chain (signed by the issuing country of the passport) present in the inspection system	Own passports	3	1	0
	EU passports	2	1	0

	Third country passports	1	2	0
Terminal Authentication: Inspection system certificate or DVCA certificate expired	Own passports	3	1	0
	EU passports	2	1	0
	Third country passports	1	2	0
Terminal Authentication: CVCA certificate in passport expired and attempts to update failed, e.g. because there was no valid link certificate available in the inspection system	Own passports	3	1	0
	EU passports	2	1	0
	Third country passports	1	2	0
Terminal Authentication failed for another reason	Own passports	3	1	0
	EU passports	2	1	0
	Third country passports	2	1	0
Other	Own passports	4	0	0
	EU passports	1	0	0
	Third country passports	2	1	0

A respondent indicates that shiny laminates can cause OCR reading problems which will also result in a BAC error and make it impossible to access the chip. One respondent reports problems with a specific type of reader having problems with a particular type of passports.

5.5.2.3. Perceived risks (*question 7)*

The respondents were asked about the likeliness that certain incidents lead to unauthorised border passage while making use of second-generation e-passports. Unfortunately the questions have not been interpreted in the same way by all respondents. Some respondents were considering the current situation at border control where not all possible verifications on second-generation e-passports have (yet) been implemented. Others were considering a situation with all possible verifications implemented in an inspection system used by a border control guard to help him in his decisions. Others again were considering the situation of automated border control (ABC) where the actual inspection is fully performed by a machine, not a border guard.

Still, overall the risks due to lookalike fraud (if fingerprints are not used) and issuance fraud are considered higher than the more technical risks due to problems with chips or inspection terminals.

Many respondents (45%) rate the disabling of chips as likely cause of fraud. However, many people also think that disabling the passport chip only draws additional attention at border control, and is, hence, not an effective strategy for someone to fraudulently cross the border.

Many respondents (50%) consider the risk of cloned e-passport high when only PA is relied upon to check authenticity of e-passports.

A clear majority of respondents do not consider accidental or deliberate misconfiguration of inspection systems and readers as a likely cause of fraud.

Regarding the quality of biometrics, there is slightly more concern about the quality for fingerprints and for facial images. Clearly there is not much experience with the use of these biometrics, especially fingerprints, yet. There seems to be a need for good data or experience reports with automated border control.

The detailed results are discussed below:

Lookalike fraud

Very likely	Likely	Not likely
8	12	17
17.0%	25.5%	36.2%

The respondents think fingerprint verification works well against lookalike fraud, but only if the stored fingerprints are of good quality, and it is guaranteed that no spoofing takes place. Certain respondents think fingerprint verification will not be introduced at first line inspection.

Fraudulently issued passports

Very likely	Likely	Not likely
9	18	8
19.1%	38.3%	17.0%

Non-functioning chips in e-passports

Very likely	Likely	Not likely
2	19	14
4.3%	40.4%	29.8%

Respondents stress the importance of an exception process and referral to second line border control with thorough manual inspection

Cloned chips that only pass Passive Authentication

Very likely	Likely	Not likely
4	14	15
8.5%	29.8%	31.9%

The comments are non-conclusive. The question has been interpreted differently by different respondents. Some respondents say this should be detected by an inspection system checking AA and EAC. However, AA is not mandatory and EAC is not used for first generation e-passports and not mandatory outside the EU. As a result, absence of them may be accepted by the inspection system.

Too much/Over-reliance on machines

Very likely	Likely	Not likely
10	9	14
21.3%	19.1%	29.8%

Respondents do not want to hand over responsibility to a system alone. Almost all respondents stress the importance of border guards which can best check the physical security characteristics of the e-passports. The respondents indicate that with ABC systems, it depends on the False Acceptance Rate set in the system.

Lack of specific training of border guards on e-passport handling

Very likely	Likely	Not likely
4	17	12
8.5%	36.2%	25.5%

Border guards are important so the respondents indicate that they should be properly trained. Respondents have trust in the professionalism of border guards, but they indicate that proper continuous training should get attention.

Misconfigured e-passport terminals/readers

Very likely	Likely	Not likely
2	13	18
4.3%	27.7%	38.3%

When a terminal/reader does not function or when an error occurs, the respondents indicate that this should not lead to automated border passage but to manual (second line) inspection. The respondents also indicate that e-passport readers should follow the correct protocol, but no complete specifications for this exist.

Purposely misconfigured e-passport terminals readers by organisation wanting to bypass border control

Very likely	Likely	Not likely
0	9	23
0.0%	19.1%	48.9%

This is considered very unlikely by the respondents.

Technical communication problems due to hardware

Very likely	Likely	Not likely
0	14	18
0.0%	29.8%	38.3%

Communication problems due to hardware problems are unlikely to occur according to the respondents. If they occur, the respondents indicate that the e-passport must be checked manually.

Technical communication problems due to software

Very likely	Likely	Not likely
1	14	16
2.1%	29.8%	34.0%

Communication problems due to software problems are unlikely to occur. If they occur, the e-passport must by checked manually. This is not considered a big risk by the respondents.

Technical problems with interpretation of e-passport data

Very likely	Likely	Not likely
0	9	21
0.0%	19.1%	44.7%

The respondents consider this exception to happen. They indicate that this is no real risk if it is handled properly, i.e. by thorough manual inspection.

Non-availability of signing certificates for Passive Authentication

Very likely	Likely	Not likely
9	18	5
19.1%	38.3%	10.6%

Non-availability of signing certificates is considered a serious problem by the respondents.

Non-availability of verifying certificates for EAC

Very likely	Likely	Not likely
8	12	10
17.0%	25.5%	21.3%

Respondents note that most of the countries issuing and using EAC passport are EU countries where the risk is minimal.

Poor quality of facial image in chip

Very likely	Likely	Not likely
3	20	7
6.4%	42.6%	14.9%

Poor quality of fingerprint image in chip

Very likely	Likely	Not likely
5	17	8
10.6%	36.2%	17.0%

Additionally, respondents mentioned the following risks:

- Denial of service attack on readers
- Spoofed CSCA which signs the e-passport data. This works if the signature and the signing certificates are not properly checked by the inspection system.
- Missing CSCA certificates for Passive Authentication.

6. *Risk workshop results*

In this report, we discuss the results of the risks workshop on the security of e-passports in Europe, which was held in the Warsaw office of Frontex on 27 and 28 January 2011. Although also other presentations were given, we only reflect the results of the afternoon workshop on 27 January and the plenary discussion on 28 January here.

The afternoon workshop session on 27 January was performed in three parallel sessions (on issuance, technical and usage security respectively). These sessions are the core of the workshop as most interactions and discussions took place there. We will first give overall conclusions and results from the workshop, then present the set-up of the workshop and finally give more detailed results for each of the three parallel workshop sessions.

The workshop conclusions and recommendations are those of the study consortium based on the risk scores provided by the workshop participants and discussions that took place at the workshop. As such, they will not necessarily be shared or endorsed by all persons who participated in the workshop.

In performing the study for Frontex, the consortium did not limit itself to scope of Frontex's authority, so in some respects its conclusions and recommendations might stray beyond the limits of the remit of Frontex.

6.1. *Conclusions and recommendations from the workshop*

Conclusions

- Issuance procedures and border control procedures should be tuned to each other so that the overall security provided is optimal.

- As Schengen introduces dependencies of countries not only on each other’s border control procedures, but also on each other’s issuance procedures, there is a need for communication/harmonisation.

- Use of the e-passport chip at border control is still in the early stages. Relatively, in only a few places in a limited number of countries, the chip is now being used. Nowhere are the full possibilities of the chip (e.g. fingerprints) used.

- Not all Member States currently issue e-passports that support a mechanism to authenticate the passport chip itself which is a strong countermeasure against e-passport cloning, especially in the context of automated border control.

- The Member States experience high operational complexity in setting up and actively using the various needed PKI systems (i.e.. for Passive Authentication and reading of fingerprints).

Recommendations

General

Further promote structural information exchange between the issuance and the border control community on e-passport security matters.

As the Schengen Acquis necessitates mutual trust between its Member States, especially when it comes to issuing and inspecting e-passports, it can be very beneficial to the security of the external borders if structural and frequent information exchange take place. This will help to effectively manage both border control and e-passport issuance. Possible information that can be shared are: defects lists, persons restricted for travel and incidents (e.g. attempts to use a forged e-passport) at border control.

As Frontex only has a mandate within the border control context and not in the e-passport issuance context, Frontex will have to approach different organisations to facilitate this information exchange in cooperation with these other organisations and can stimulate stakeholders and decision-makers to support this information exchange.

Further investigate the security role of national ID cards in the issuance process and border control.

When compared with e-passports, national ID cards are often less secure. A possible cause is that they are less regulated and standardised. They are however extensively used within the e-passport life cycle, both in applying for an e-passport or even as a complete replacement of the e-passport during border checks. As attackers will normally attack the weakest link in border control to illegally enter the Schengen area, the effectiveness of enhancing the security of the e-passport further can be questioned as long as the national ID cards are not addressed.

Issuance

Provide training (and possibly tool provisioning) for the verification of breeder documents by issuance officers.

Frontex invests heavily in the training and provisioning of tools for document authentication within the border guard community; however, the security of the issuance process also relies on the ability of issuance officers to verify the authenticity of a breeder document during application for or delivery of an e-passport. Frontex could investigate whether the training and tools it has or is developing can also be used within the issuance context.

Compile and structure good practices from the various Member States on the issuance process.

Although the ICAO Guide on assessing the security of travel document issuance and handling provides a number of good practices for the issuance process, it makes specific choices on how to secure the issuance process. These choices cannot always be implemented by all Member States. For example, the ICAO Guide does not give any guidance in case that segregation of duties is hard to implement because of capacity/manpower constraints. Currently, Member States have found various ways to deal with these challenges, it would be valuable to compile and structure these so that they can be shared among all EU/Schengen Member States.

Discussing voluntary EU common guidelines for issuance of e-passports

As a follow-up on the previous recommendation, Frontex could discuss voluntary common EU/Schengen guidelines for the issuance of e-passports in the relevant EU forum. These would incorporate the various requirements of different EU/Schengen Member States and could form a basis for further harmonising the issuance processes.

Investigate the possibility of voluntary inter-country review of the e-passport issuance

In line with the Schengen Standing Committee on implementation and evaluation of the Schengen Border Code, similar inspections can be performed by the Issuing Authorities of the Schengen Member States. This could take the form of voluntary missions, promoting sharing of good practices or in the form of official reviews, if common guidelines are available.

Technical

Stimulate the adoption of chip authentication mechanisms in all EU e-passports.

During the workshops, the usage of cloned e-passports in automated border control was rated as a high risk. Support of chip authentication mechanisms can be a strong mitigating control to prevent illegal border crossings.

Investigate formalising the de facto practice of placing the document signing certificates in the e-passports.

Although this is already the case in practice, adding this requirement would remove the need for Member States to collect all Document Signer certificates and insert them into their inspection systems, reducing the inspection systems' operational hassle.

Press for SHA-1 phase- out

The online questionnaire showed that some countries are already phasing out SHA-1 as a secure hash function, but not all. The e-passport's security mechanisms, mainly Passive Authentication, crucially rely on the security of the hash function. Especially given the lifetime of e-passports, of 5 or 10 years, phasing out SHA-1 seems a sensible precaution. This is in line with many recommendations to retire SHA-1 for the use of digital signatures, mainly by the US National Institute of Standards and Technologies (see NIST Special Publication 800-131A, January 2011).

The risk of using SHA-1 was not rated high at the risk workshop and hence not discussed there. The quality of hash functions is a specialised technical topic; one would not expect many people in the broader passport issuance and border control community to have such expertise in cryptology. So the recommendation to phase out SHA-1 is not an outcome of the risk workshop, but is based on our own assessment, given the responses to the online questionnaire.

Only the future can tell if continued use of SHA-1 will turn out to be a serious risk in the long term, but phasing it out is a relatively cheaper measure – it only requires a small, localised change in the production process, and only in the software used for personalisation, and none for the e-passport itself or for inspection systems (as inspection systems already need to support all allowed hash functions) – so it seems unwise to run this risk.

Collect real-life performance data from ABC system pilots

With a few countries carrying out experiments with ABC gates, it would clearly be good to collect some data on experiences with such systems, to get a clear picture of the performance and accuracy of such systems, and to gather experiences and suggestions for best practices in deploying and operating ABC gates.

Inspection

Investigate the harmonisation of MRTD inspection (usage) at the border. This includes both manual and automated border control.

As there are no effective internal borders, Schengen Member States rely on the border control of other Schengen Member States to keep unwanted persons outside their territory. Sound and shared inspection procedures of e-passports could improve the overall security of border control in various Schengen Member States.

Provide training of border guards on the specifics on e-passport inspection.

Further reinforce Frontex initiatives to train border guards in establishing the authenticity of e-passports as well as provision tools to support border guards in verifying the chip.

Investigate the benefits for border control to further improve the quality of the digital facial image.

Although the image quality of the digital facial images is already much better when compared with the image quality of the hardcopy document, it could still be improved. During the workshop, it was suggested that this might improve possibilities to detect attempts at lookalike fraud.

Investigate the future of the usage of fingerprints in border control.

Currently fingerprints are hardly used during border control. Frontex may investigate which obstacles Member States are facing to start using fingerprints and coordinate possible actions on a European scale to facilitate fingerprints' usage.

Investigate the required level of standardisation for fingerprint biometrics quality.

We recommend further investigating the level of standardisation for fingerprint biometrics quality, to evaluate what minimum quality is required for reliable usage at border control, and to establish guidelines in this respect, which can be used by both issuing authorities (biometric capture at enrolment) and inspection authorities (biometric capture at border control).

6.2. *Set-up of the workshops*

The goal of the workshop is to validate and rate potential (security) incidents in the e-passport life cycle. The potential security incidents are based on combinations of threats and vulnerabilities which were compiled in the life cycle description of e-passports based on the document study and interview results (please refer to Chapters 2 and 3). The life cycle here serves as a framework to relate various vulnerabilities and threats to a specific step in the e-passport issuance and usage processes. Based on the different life cycle steps, the workshop was divided into three parallel sessions and, within the sessions, into different topics.

The overall workshop was structured in the following way:

1. Presentation of questionnaire results (morning, 27 January 2011)

2. Presentation of risk analysis method (afternoon, 27 January 2011)

3. Break-out in three parallel interactive sessions (afternoon, 27 January 2011)

4. Plenary presentation and discussion of workshop results (morning, 28 January 2011).

6.2.1. Methodology used in parallel sessions

In the workshop the methodology described in the ISO 27005: 2008 standard titled “Information technology – Security techniques – Information security risk management” [47] and NIST special publication 800-30 titled “Risk Management Guide for Information Technology Systems” [45] was followed. Although any risk assessment technique has its advantages and disadvantages, we chose this method as it is relatively simple and is the de facto international standard on risk assessment. We introduce and use the following terms in line with this standard:

- **Vulnerability**
  A flaw or weakness in system security procedures, design, implementation or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.
- **Threat**
  The potential to accidentally trigger or intentionally exploit a specific vulnerability. Threats can be Natural/Environmental or Human.

A fundamental difference between a threat and vulnerability is that the latter can be mitigated or even completely removed, while in principle, a threat cannot be influenced.

A manifestation of a threat (explaining the intent, methods etc.) is called an **attacker.** A (potential) **incident** is based on a combination of a threat (“who” or “what”) and a vulnerability (“exploit”). A (potential) incident has an **impact** and a **likelihood of occurrence**. A **control** can be implemented to reduce either the impact or the likelihood of occurrence of a potential incident to reduce the risk. This is schematically depicted in Figure 9.

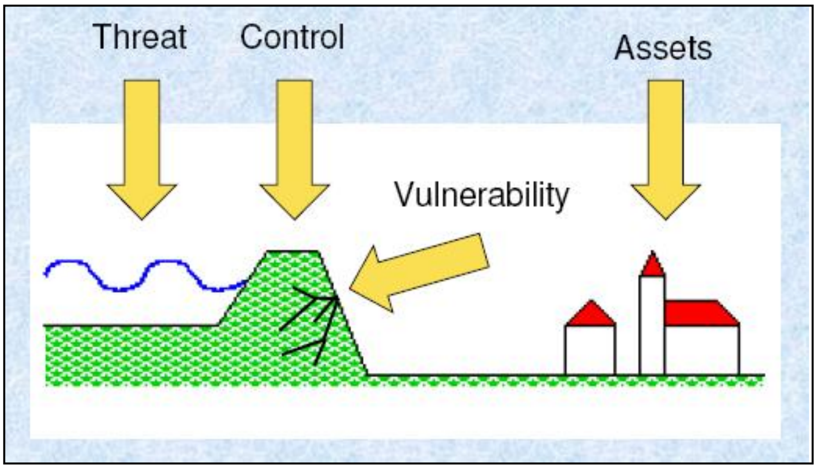


Figure 9 - Graphical representation of risk assessment methodology

The **risk** related to an incident is based on its **impact** and **likelihood of occurrence**. In the model we use (based on ISO 27005), an incident impact can vary from very low (1) to very high (5). Moreover, the likelihood can vary from very unlikely (1) to very likely (5). The risk is the product of the two, as indicated in Table 4.

		Incident likelihood of occurrence				
		Very unlikely(1)	Unlikely (2)	Possible (3)	Likely (4)	Very likely (5)
Incident Impact	Very low (1)	**1**	**2**	**3**	**4**	**5**
	Low (2)	**2**	**4**	**6**	**8**	**10**
	Medium (3)	**3**	**6**	**9**	**12**	**15**
	High (4)	**4**	**8**	**12**	**16**	**20**
	Very high (5)	**5**	**10**	**15**	**20**	**25**

Table 4 - Risk rating methodology

In the preparation of the workshops, we have preselected potential incidents for discussion during the workshop. A more extensive list of potential incidents is available in the life cycle document and was compiled using information from the document study and expert interviews.

In the parallel workshop sessions, the participants were asked to rate both the impact and likelihood of occurrence for a number of preselected potential incidents. They were asked to rate this not for their individual country situation, but for Europe as a whole and regardless of possible controls in place. For this they used forms which were present in the workshop reader. These ratings were subsequently collected and processed in order to rank the potential incidents from highest to lowest perceived risk.

The highest perceived risks were discussed in the workshop session and for these, a brief risk **treatment** was performed. To treat a risk, a number of options are available:

- **Reduce or remove** the risk by taking appropriate controls/countermeasures (e.g. screening of personnel to reduce the risk of bribery)
- **Avoid** the risk (e.g. do not issue e-passports abroad when that issuance process is less secure)
- **Transfer** the risk to another organisation (e.g. performing extra border controls to compensate for low issuance security)
- **Accept** the risk (e.g. continue current practices, as there is no alternative or the risk is acceptably low).

6.2.2. *Participation*

In total, 53 attendees participated in the workshop, from various EU/Schengen countries, non-EU countries and international organisations. Participation in the workshop was voluntary, and the attendees were given the choice of which workshop to attend. 13 attendees participated in the issuance workshop, 16 in the technical security workshop and 24 in the usage workshop.

Through Frontex, all EU/Schengen Member States were invited to attend the workshop with a two-person delegation. In the invitation, we requested that Member States send their experts in the area of risk management, who are also familiar with current (security) issues in border control and e-passport issuance.

6.3. *Risk workshop results on issuance*

Although there was a limited time available for the completion of the issuance risk workshop and not all EU/Schengen Member States were represented, the results offer valuable insights into perceived risk levels of the various hypothetical vulnerabilities.

6.3.1. *Topics identified on issuance*

Three topics were distinguished for the issuance workshop:

1. Application and Entitlement
2. Production, Delivery and Invalidation
3. Security Management

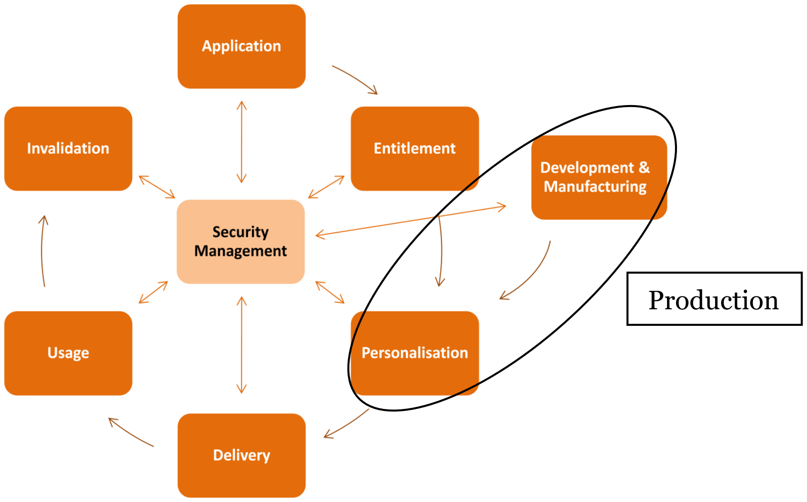


Figure 10 - Issuance topics in e-passport life cycle

The focus of the issuance workshop was more on organisational and procedural risks, and not on technical risks, as this is the focus of the Technical Security session (please refer to Section 6.4). Together the three topics cover all e-passport life cycle steps, except for the Usage step, as this is the focus of the Usage session (please refer to Section 6.5). Here the three topics are introduced:

Application and Entitlement

In the Application and Entitlement topic, we focused on hypothetical vulnerabilities and incidents during application and the entitlement decision. As in these stages the authorisation to produce a genuine e-passport is given, manipulation in these steps can result in false, but technically genuine and valid e-passports. Attention was given to how the identity of the applicant can be verified, if all information is available to make an informed entitlement decision and on biometrics capturing.

Production, Delivery and Invalidation

In the Production, Delivery and Invalidation topic, vulnerabilities and incidents in these steps of the life cycle were discussed. Specific attention was given to physical security of e-passport (materials), delivery methods and how to properly invalidate an e-passport.

Security Management

The final topic, Security Management, was engaged in how on a national and possibly international level, the security of the issuance (and usage) of e-passports can be ensured. Attention was given to how security standards and guidelines can be used, what the role of audits can be and how incidents should be dealt with.

Please see related sections 6.3.3.2-4 for the full list of discussed potential incidents, highest ranked risks and possible countermeasures.

6.3.2. *Main workshop results on issuance*

General results

Threat agents

The identified list of threat agents (please refer to Section 4.2.3.3) was accepted by the participants. A threat agent "internal malfeasants" was added, as although the threat is usually in the service of another threat agent s/he can also autonomously seek to exploit his/her insider access.

Different perceptions of risks among participants

The results show that participants display a very different perception of risks. This can be observed in the high variation in the rating of risks by participants. A possible cause is that in different countries, risks are perceived very differently. This can be illustrated by the example that in some countries it is currently possible to deliver e-passports through regular mail service, while in others it is only delivered in person by the delivery officer, after verification of the biometrics.

Results on Topic #1: Application and Entitlement

Based on participant responses, the highest rated risks in the Application and Entitlement topic are:

1. *Application and entitlement officers do not receive formal training on assessing the authenticity of breeder documents.*
2. *The procedures for verifying the identity of the applicant are not documented or not comprehensive.*
3. *Frequently losing a passport is no ground for investigation before issuance or even refusal of a new passport.*
4. *Application and entitlement procedures do not incorporate "segregation of duties": one person is able to issue passports under single control.*
5. *Insufficient exclusion data for passport issuance available for officers (e.g. criminal records or trial pending, renouncement of nationality, tax debt and excessive loss history).*

Please see Section 6.3.3.2 for the detailed information on the ranking and identified countermeasures for these highest risks.

We found it unexpected that the potential vulnerabilities related to biometrics (e.g. gummy fingerprints or morphing of facial photos) were generally rated low, although in another session of the workshop, a speaker showed border control incidents related to morphing. Possibly this can be explained because it was perceived that biometrics from the e-passport are currently hardly used at border control.

It was discussed that there is no simple solution to process first-time applicants, as they are not yet in the system. Some countries struggle with data protection laws, which require them to (partially) delete previous applications for an e-passport, resulting in many applications effectively being processed as first-time applications.

When discussing possible countermeasures, it was remarked that for risk #3 it is usually not legally possible to refuse to issue a passport, although extra penalties (e.g. monetary fees, limited validity period) to discourage frequent renewal can be deployed. If these penalties are not sufficiently high, this would allow attackers to easily build up a large collection of e-passports (i.e. a "library"). The larger this collection is, the higher the probability is of a lookalike possibility.

Risk #5 relates to persons illegally fleeing the Schengen area under their own name.

Results on Topic #2: Production, Delivery and Invalidation

Based on participant responses, the highest risks in Production, Delivery and Invalidation are:

1. *Passports are delivered to the applicant through regular mail.*
2. *Insufficient physical security in the production and delivery environment.*
3. *Personalisation is done at many (e.g. > 10) locations: the more locations, the more possibilities of attack.*
4. *Officers do not receive formal training on assessing the authenticity of identity documents at delivery.*
5. *Production and delivery officers are not screened.*

Please see Section 6.3.3.3 for detailed information on the ranking and identified countermeasures for these highest risks.

We found it unexpected that the risk of uncollected e-passports was rated low. Also, at least one country in the EU uses regular mail service to deliver e-passports. Some mitigating controls are in place at their border control (cross-check against Interpol SLTD[13] database for all entries); however, as this is not in place in all other countries, this risk is unmitigated for most of the EU/Schengen external border.

Related to risk #1, retrieving passports out of mailboxes was discussed. It appears that some EU Member States also allow application through regular mail.

As a mitigating control for risk #3, a traceability of personalisations to the individual personalisation officer was discussed, followed up by regular audits focusing on personalisations under single control. This was perceived as a good solution when segregation of duties is not feasible.

Various difficulties and cost aspects (related to the level) of screening were discussed when discussing risk #5.

Results on Topic #3: Security management

Because of lack of time, the security management topic was not fully discussed.

There was a discussion on whether oversight on issuance on an EU/Schengen level was appropriate for this workshop. Some participants felt that this topic should be discussed from a policy perspective at the European Commission.

The US has partially based its Visa Waiver Program (VWP) on trust in the security of other countries' travel documents. Not all EU/Schengen countries are included in the VWP. This indicates a possible difference in the level of trust the US places in some EU/Schengen countries' e-passports.

[13] Stolen and Lost Travel Document

It was indicated by one of the participants that there exists an inter-country review of border control at an EU/Schengen level. This inter-country review set-up might also be interesting for issuing[14].

6.3.3. Detailed results of the issuance workshop

6.3.3.1. General feedback

In the issuance workshop, the following topics were discussed:

- List of threat agents
- Rating of hypothetical vulnerabilities related to Topic #1 (Application and Entitlement)
- Rating of hypothetical vulnerabilities related to Topic #2 (Production, Delivery and Invalidation)
- Rating of hypothetical vulnerabilities related to Topic #3 (Security Management)

Threat agents

The following threat agents were identified in the life cycle document:

- **Non-deliberate threats**
  Examples: Programming errors, system failure, human errors, etc.
- **Internal malfeasants**
  Example: Officials actively seeking to sell blank e-passports
- **(Unorganised) private individuals**
  Goal: Crossing a border checkpoint without being correctly identified
- **Organised criminal and terrorist organisations**
  Goal: Crossing a border checkpoint without being correctly identified, e.g. human trafficking or criminals going abroad to escape detention
- **Foreign governments**
  Goal: Crossing a border checkpoint belonging to a foreign country, without being correctly identified
- **Hackers**
  Goal: Generating publicity about security issues related to e-passports

On this list, the threat agent “internal malfeasants” was added during the workshop. Although they are usually in the service of one of the other threat agents, they can also autonomously seek monetary gain with their insider access. The other threat agents were supported by the participants. It was remarked that (unorganised) private individuals are usually responsible for the bulk (i.e. high volume) of the incidents, while the terrorist organisations are responsible for the incidents with the highest impact.

[14] After the workshop, we looked into this further and discovered relevant European legislation on setting up a Standing Committee on the evaluation and implementation of Schengen (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:41998D0026:EN:NOT), which gives this committee powers to investigate the application of the Schengen Code in Member States.

6.3.3.2.Topic #1: Application and Entitlement

The following potential incidents were discussed and rated in the issuance workshop:

#	Hypothetical vulnerabilities	Average risk rating [1-25]
11	Application and entitlement officers do not receive formal training on assessing the authenticity of breeder documents.	15
7	The procedures for verifying the identity of the applicant are not documented or not comprehensive.	13
13	Frequently losing a passport is no ground for investigation before or refusal of a new passport.	13
12	Application and entitlement procedures do not incorporate “segregation of duties” – one person is able to issue passports under single control.	13
9	Insufficient data is available for officers on exclusion data for passport issuance (e.g. criminal records or trial pending, renouncement of nationality, tax debt, excessive loss history).	12
15	Procedures for and quality of national ID documents – used as breeder documents for e-passports – are less stringent than those for passports.	12
14	Application and entitlement need to rely on hard copy breeder documents (e.g. birth certificates, electricity bills) provided by the applicant.	12
10	Application and entitlement officers do not receive formal training on procedures.	11
6	Application and entitlement procedures abroad (e.g. embassies) are less secure than domestic.	11
8	The procedures for verifying the identity of the applicant are based on “happy flow” and do not deal with exceptions.	10
3	Application and entitlement officers are not screened.	10
2	Insufficient network and computer security in the systems used for application and entitlement.	10
20	Insufficient quality biometrics (facial, fingerprints) is captured.	10
23	The instruction to produce a passport (based on entitlement decision) can be manipulated.	9
17	Application and entitlement procedures allow photos brought in by applicant to be of insufficient quality.	9
5	Application and entitlement officers have many other civil servant tasks.	9
16	Application and entitlement procedures are not more scrutinised for first-time applicants or for applicants with passport/ID expired over two years.	9
18	Application and entitlement officers do not receive formal training on assessing the quality of biometric data (photos, fingerprints).	8
22	The entitlement decision is non-traceable (e.g. no audit trail).	8
19	It is not possible to extract fingerprints of sufficient quality from some people.	8

4	Security guidelines (e.g. on clear desk, locking workstations) for application and entitlement officers are not formalised.	8
1	Insufficient physical security in the application and entitlement environment.	7
21	Application and entitlement procedures do not incorporate check on “gummy fingers”, i.e. glued fake fingerprints.	7

Table 5 - Average risk ratings issuance Topic #1

The following charts were produced based on the attendee responses. Per hypothetical vulnerability, the ratings are displayed as a 25% percentile to 75% percentile box, with the average displayed as the border between the light and dark red box. The minimum and maximum ratings are depicted in error bars. Thus, 50% of the respondents rated the risk within the range of the box (and 25% below and 25% above), while the average is the change in colour of the box.

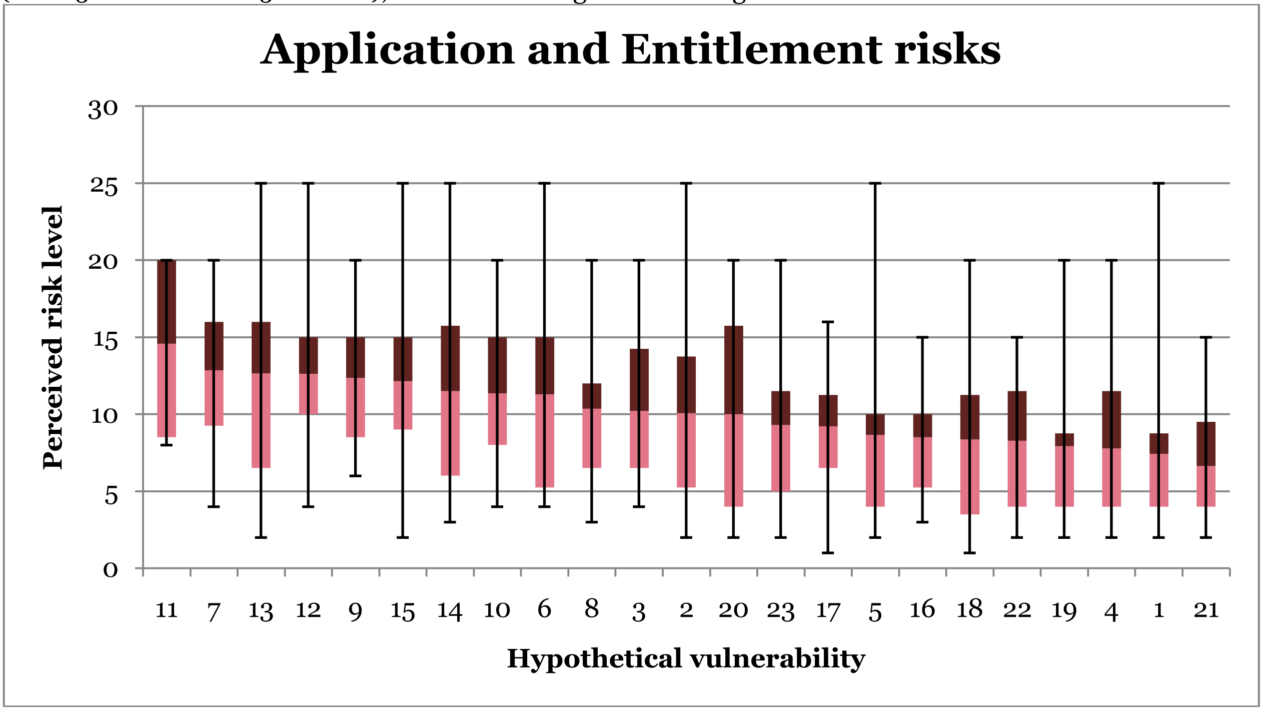


Figure 11 - Issuance Topic #1 risk rating

In the chart above, it can be observed that although the average risk ratings are quite stable, the individual responses (indicated by the maximum and minimum error bars) vary a lot.

Countermeasures for highest risks

After rating the risks, the following countermeasures were identified during the workshop:

1. ***Application and entitlement officers do not receive formal training on assessing the authenticity of breeder documents.***
    - *Provide central database(s) as reference for/replacement of paper documents*
    - *Invest in extra training and experience for application and entitlement officers*

2. ***The procedures on verifying the identity of the applicant are not documented or not comprehensive.***
    - *Similar to 1.*

3. ***Frequently losing a passport is no ground for investigation before issuance or even refusal of a new passport.***
    - *Issue passports with a limited lifetime to applicants with a frequent loss history*

    - *Monetary penalty for early renewals (possibly increasing further after multiple losses)*
    - *Performing criminal investigations*

4. ***Application and entitlement procedures do not incorporate "segregation of duties" – one person is able to issue passports under single control.***
    - *Ensure dual or triple control for issuance (issue with small application stations)*
    - *With single control: Ensure issuance traceability (to individual issuance official) and perform consistent audits to check for irregularities, focusing on issuance under single control.*

5. ***Insufficient exclusion data for passport issuance available for officers (e.g. criminal records or trial pending, renouncement of nationality, tax debt and excessive loss history).***
    - *Ensure availability of these registries/databases during application and entitlement*

Other attention points/notes

- *Fingerprints are not perceived as relevant in the issuance process at the moment as they are hardly used in both the issuance process and at border control.*
- *Privacy regulations may frustrate a secure issuance process, e.g. by prohibiting record keeping on the previous applications so that comparison of images/fingerprints with those on the previous applications is not possible.*
- *Related to highest risk #1 (related to potential incident #11): It was discussed that no/limited mitigation is possible for first-time applicants*
- *Related to highest risk #3 (related to potential incident #13): There seems to be no possibility to permanently deny a passport to an applicant with a frequent loss history, as there is often a legal obligation of a country to issue passports to its citizens.*

6.3.3.3. Topic #2: Production, Delivery and Invalidation

The following potential incidents were discussed and rated in the issuance workshop:

#	Hypothetical vulnerability	Average risk rating [1-25]
11	Passports are delivered to the applicant through regular mail.	12
1	Insufficient physical security in the production and delivery environment.	12
9	Personalisation is done at many (e.g. > 10) locations; the more locations, the more possibilities to attack.	11
6	Officers do not receive formal training on assessing the authenticity of identity documents at delivery.	11
3	Production and delivery officers are not screened.	11
10	Passports are delivered to the passport offices via a commercial courier service.	10
13	Passports can be picked up by a person other than the applicant.	10
7	The old passport is not invalidated, e.g. as there are valid visas inside it.	10
16	Personalised e-passports are not stored in a safe at the delivery station	10
5	Officers do not receive formal training on procedures.	9
8	The chip on the old passport is not technically invalidated, e.g. only a hole is punctured or the MRZ is cut off.	8
4	Security guidelines for production are not formalised; this includes specification of security in contracts with outsourced production facilities.	8
15	At pick-up of the passport, it is not possible to check the fingerprints of the applicant.	8
12	Passports are delivered to the applicant through registered mail.	8
17	Non-collected passports are kept indefinitely at the passport office and are not destroyed.	8
2	Insufficient computer security in the systems used for production and delivery.	7
14	At pick-up of the passport, it is not possible to read the chip inside the passport.	7

Table 6 - Average risk ratings issuance Topic #2

The following charts were produced based on the attendee responses. Per hypothetical vulnerability, the ratings are displayed as a 25% percentile to 75% percentile box, with the average displayed as the border between the light and dark red box. The minimum and maximum ratings are depicted in error bars. Thus, 50% of the respondents rated the risk within the range of the box (and 25% below and 25% above), while the average is the change in colour of the box.

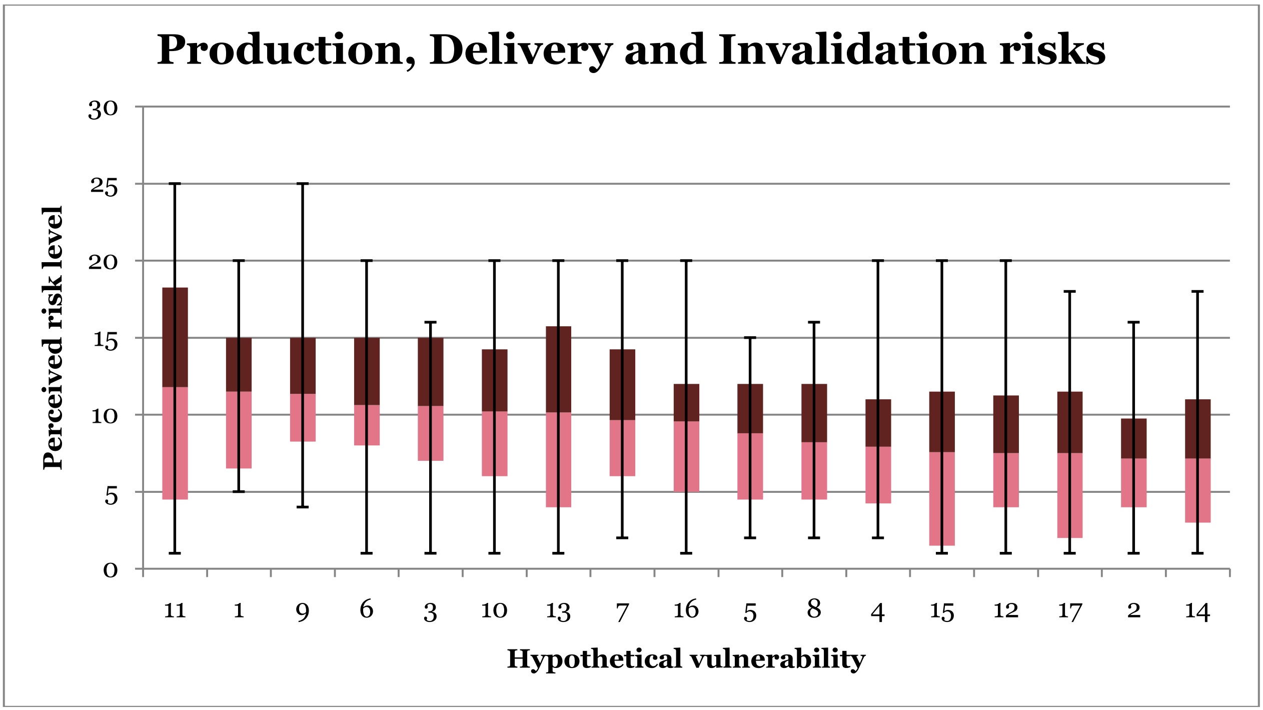


Figure 12 - Issuance Topic #2 risk rating

In the chart above, it can be observed that although the average risk ratings are quite stable, the individual responses (indicated by the maximum and minimum error bars) vary a lot.

Countermeasures for highest risks

After rating the risks, the following countermeasures were identified:

1. ***Passports are delivered to the applicant through regular mail.***
   - *Only deliver passports via regular mail to "low-risk" areas*
2. ***Insufficient physical security in the production and delivery environment.***
   - *ICAO Guidelines (e.g. segregation of duties between production and QA, secure waste disposal)*
   - *Usage of unique transport keys for blank e-passports related to personnel*
   - *Strictly configured issuance systems*
3. ***Personalisation is done at many (e.g. > 10) locations – the more locations, the more possibilities to attack.***
   - *Assign unique batches to personalisation locations/persons*
   - *Individual traceability of personalisations and follow-up audits*
4. ***Officers do not receive formal training on assessing the authenticity of identity documents at delivery.***
   - *See Topic #1*
5. ***Production and delivery officers are not screened.***
   - *Different levels of screening should be tailored to the need, basic level (e.g. check against criminal records and financial situation) should always be performed*
   - *Foster employee awareness and morale and impose heavy sanctions and penalties.*

Other attention points

- *Discussion on the rating of highest risk #1 (related to potential incident #11): Some participants disagreed this was a big risk as personalised e-passports are much harder to abuse when compared to unpersonalised e-passports.*

6.3.3.4. Topic #3: Security Management

The following potential incidents were planned to be rated and discussed in the Security Management topic:

#	Hypothetical vulnerability	Average risk rating [1-25]
1	Lack of European information security regulations on issuance and production of passports, e.g. screening and training of personnel, segregation of duties, network and computer security.	NA
2	Lack of European information procedural regulations on issuance and production of passports, e.g. minimal (security) requirements on breeder documents and their authenticity.	NA
3	No single national organisation responsible for issuance and production of passports with governance responsibilities.	NA
4	No single EU body responsible for issuance and production of passports with governance responsibilities.	NA
5	Lack of (security) audits on parties involved in issuance and production of passports (including passport offices)	NA
6	Lack of communication on (security) incidents among parties involved in issuance and production of passports (including passport offices) on national scale.	NA
7	Lack of communication on (security) incidents among parties involved in issuance and production of passports (including passport offices) on EU scale.	NA
8	Lack of periodic holistic (security) reviews on e-passports from issuance to usage on national scale, e.g. risk-based requirements, incidents and audits.	NA
9	Lack of periodic holistic (security) reviews on e-passports from issuance to usage on EU scale, e.g. risk-based requirements, incidents and audits.	NA

Table 7 - Average risk ratings Issuance Topic #3

Because of lack of time, only the following hypothetical vulnerabilities were discussed briefly:

1. Lack of harmonisation of security regulations on issuance and production of passports, e.g. screening and training of personnel, segregation of duties, network and computer security.
2. Lack of harmonisation of procedural regulations on issuance and production of passports, e.g. minimal (security) requirements on breeder documents and their authenticity.
3. Lack of communication on (security) incidents among parties involved in issuance and production of passports (including passport offices).

4. Lack of (security) audits on parties involved in issuance and production of passports (including passport offices).

Other attention points/notes

- There was a discussion on whether discussion on oversight on issuance on an EU level was appropriate for this workshop.
- The US has partially based its Visa Waiver Program on trust in security of other countries' travel documents. Not all EU/Schengen countries are included in the VWP.
- It was indicated by one of the participants that there exists an inter-country review of border control at an EU/Schengen level. This inter-country review set-up might also be interesting for issuing[15].

[15] After the workshop, we looked into this further and discovered relevant European legislation on setting up a Standing Committee on the evaluation and implementation of Schengen (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:41998D0026:EN:NOT), which gives this committee powers to investigate the application of the Schengen Code in Member States.

6.4. *Risk workshop results on technical security*

Although there was a limited time available for the completion of the technical security risk workshop and not all EU/Schengen Member States were represented, the results offer valuable insights into perceived risk levels of the various hypothetical vulnerabilities.

6.4.1. Topics identified on technical security

In the Technical Security risk assessment workshop, we clustered the discussion around two topics:

- Topic 1: Technical issues in inspection
- Topic 2: Technical issues in production (excluding the broader issuance process).

We explicitly limited the scope of Topic 2 to the manufacture of blank passports and the personalisation of these blanks and excluded the other steps in the issuance process (such as application, entitlement and delivery).

For Topic 1, we also tried to get a more precise ranking of the perceived likelihoods of various types of e-passport fraud, such as lookalike fraud vs. passport forgery, fraud using various types of travel documents (EU passports, non-EU passports and national ID cards), and ABC gates vs. human border guards. The ranking of these vulnerabilities is treated below under Topic 1a.

6.4.2. Main workshop results on technical security

As expected from the results of the online questionnaire, there is a considerable spread in perceptions of risks among the participants. There was a clear trend, however, in that the risks in the production were rated lower than those in inspection.

As most of the people at the workshop were from the inspection community, nearly all the time was spent discussing inspection issues. This also made sense given the higher risk ratings for the inspection issues than the production issues.

A recurring pattern when discussing specific technical aspects of the e-passport chip was that people noted that this issue had already been extensively discussed at ICAO level, at EU level or at the BIG (Brussels Interoperability Group) meetings, and that discussion seems to be going over old ground.

Topic #1a: Relative likelihood ratings

As part of the session on inspection, participants were also asked to rate relative likelihoods of particular scenarios leading to successful illegal border crossing. Here participants were only asked to rank likelihood, not impact, so these questions did not follow the standard format for the workshops. Instead of using likelihood * impact ratings, participants were asked to rank likelihoods of different types of fraud, choosing whether one scenario was much more likely, more likely, just as likely, less likely or much less likely than another.

Here there was very clear consensus on two issues:

- Successful illegal border crossing using a forged EU passport is less likely than through lookalike fraud with a real one.
- Successful illegal border crossing, by forgery or lookalike fraud, using an EU passport is less likely than using a non-EU passport.

Clearly the second issue cannot be remedied by the EU e-passport, but the first issue could.

Concerning risk mitigation for lookalike fraud through biometrics, opinion was divided on whether showing the facial image from DG2 to border guards made lookalike fraud less likely or whether this made no difference. This is one way in which the chip is seen to be able to contribute towards reducing one of the bigger risks, namely lookalike fraud.

Concerning the difference between ABC gates and border guards, it was interesting to note that people had wildly different ratings on whether ABC gates or border guards would be better at spotting lookalike fraud.

People also had broadly varying ratings as to whether national ID cards or EU passports were much more likely to be used for illegal border crossings. This contradicts the findings in the inspection workshop, where national ID cards *were* rated highly as a risk, which is what we were also expecting to find here.

Topic #1b: Technical risks in inspection

In the risk assessment of potential incidents in inspection, the top 5 were as follows:

- *Automated border control system accepting a fake e-passport that is electronically a perfect clone but visually obviously fake*
- *Facial image in DG2 – Insufficient quality to prevent lookalike fraud (assuming it is used by automated border control system)*
- *Insufficient attention to security in development of inspection systems*
- *Non-compliance/Lack of interoperability of e-passports undermining trust of border guards in e-passport chip*
- *Attacker travelling on stolen/bought e-passport disabling the chip, when border control is done by border guards who also read chip.*

The full list of ratings for all incidents, and the discussion of the top risks and possible mitigation strategies for them are given in Section 6.4.3.1.

Topic #2: Technical risks in production

In the risk assessment of potential incidents in production, the overall ratings were a lot lower, and the top 3 – which were the only incidents scoring over 7 – were as follows:

- *Insufficient trustworthiness of personnel in personalisation*
- *Insufficient attention to security in the development of the personalisation system*
- *Theft of blank passports (with programmable/configurable chip).*

The full list of ratings for all incidents, and the discussion of the top risks and possible mitigation strategies for them are given in Section 6.4.3.2.

6.4.3. Detailed results of the technical security workshop

6.4.3.1. Topic #1: *Risks related to inspection*

Topic #1 was split into two different subtopics, 1a and 1b, where 1a focused on relative likelihood perceptions in attack scenarios, and 1b focused on actual potential incidents.

Topic #1a Relative likelihood perceptions

To rank the relative likelihoods of scenarios leading to illegal border crossing, people could choose between "much more likely", "more likely", "just as likely", "less likely" or "much less likely". We assigned numeric weights 2, 1, 0,-1 and -2 for computing average scores, given in brackets below.

There was very clear consensus on two issues:

- *Successful illegal border passage using a fake EU passport is* ***less likely (-1)*** *than it is through lookalike fraud with a real one.*

  Here there was very clear consensus, with nearly everyone deeming this "less likely" or "much less likely", and only two people (out of 15) ranking it "just as likely".

- *Successful illegal border passage (by forgery or lookalike fraud) using a foreign passport is more* ***likely (0.9)*** *than using an EU e-passport.*

  Here there was clear consensus, with nearly everyone deeming this "more likely" or "much more likely", and two persons ranking it "just as likely" or "less likely".

Clearly the second issue above cannot be remedied by the EU e-passport. The first issue possibly could, given the e-passport chip carries biometric data (facial image and possibly fingerprints).

For the other issues, there was less outspoken consensus:

- *Lookalike fraud is* ***a bit less likely (0.5)*** *if DG2 (the facial image) is shown to border guards.*

  Here opinion was divided, with roughly half the people thinking it made no difference, and the other half rating that the showing of the facial image from the chip made lookalike fraud less likely.

- *Lookalike fraud is* ***a bit less likely (0.3)*** *if ABC gates using facial images are used instead of border guards.*

  Here there was no consensus, and ratings varied wildly ranging from "much less likely" to "more likely".

- *Successful illegal border passage (by forgery or lookalike fraud) using an EU national ID card is* ***just as likely (0)*** *than using an EU e-passport.*

  Here there was no consensus whatsoever, with people voting for "(much) more likely" and "(much) less likely" in exactly equal numbers, cancelling each other out.

Topic #1b: Technical risks in inspection

The following potential incidents were rated in the technical security workshop:

#	Hypothetical vulnerability	Average risk rating [1-25]
6.	Automated border control system accepting a fake e-passport that is electronically a perfect clone but visually obviously fake	14
7.	Insufficient attention to security in development of inspection systems	11
16.	Facial image in DG2 – Insufficient quality to prevent lookalike fraud (assuming it is used by automated border control [ABC] system)	10
3.	Non-compliance/Lack of interoperability of e-passports undermining trust of border guards in e-passport chip	9
5.	Attacker travelling on stolen/bought e-passport disabling the chip when border control is done by border guards who also read chip	8
2.	Non-compliance/Lack of interoperability of e-passport resulting in confusing error messages for border guard	8
17.	Fingerprint in DG3 – Insufficient quality to prevent lookalike fraud (assuming fingerprints are used)	7
15.	Facial image in DG2 – Insufficient quality to prevent lookalike fraud (assuming it is used by human border guard)	7
18.	Fake fingerprints presented in border control (assuming fingerprints are used)	7
10.	Accidental misconfiguration of mobile inspection systems	7
1.	Non-compliance/Lack of interoperability of e-passports causing operational hassle at border control	7
4.	Non-compliance/Bad interoperability of e-passports allowing illegal border crossing	7
8.	Accidental misconfiguration of stationary inspection systems	6
12.	Denial of Service (Dos) attack on inspection systems via malicious RFID input	5
13.	Mass disabling of many passport chips (e.g. to mount DoS attack on e-passport usage at an airport)	5
9.	Deliberate misconfiguration of stationary inspection systems (e.g. including wrong certificates)	5
14.	People disabling their own passport chip because of privacy concerns	5
11.	Deliberate misconfiguration of mobile inspection systems	5

Table 8 - Average risk ratings Technical Security Topic #1

The following charts were produced based on the attendee responses. Per hypothetical vulnerability, the ratings are displayed as a 25% percentile to 75% percentile box, with the average displayed as the border between the light and dark red box. The minimum and maximum ratings are depicted in error bars. Thus, 50% of the respondents rated the risk within the range of the box (and 25% below and 25% above), while the average is the change in colour of the box.

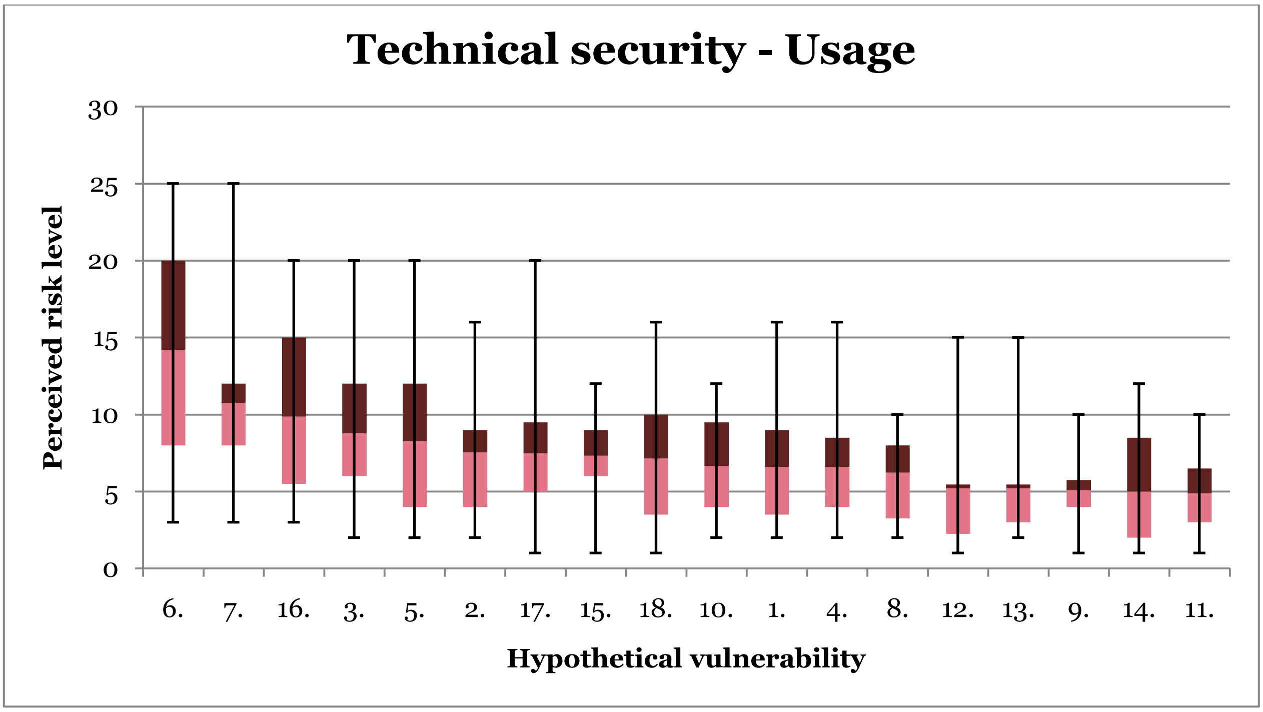


Figure 13 - Technical Security Topic #1 risk rating

Countermeasures for highest risks

- ***Automated border control system accepting a fake e-passport that is electronically a perfect clone but visually obviously fake***
  - *Make sure e-passports support either AA or CA.*
  - *Follow ICAO guidelines on optical checks on the MRZ.*
- ***Facial image in DG2 – Insufficient quality to prevent lookalike fraud (assuming it is used by automated border control system)***
  - *No real countermeasure suggested; however it would be valuable to obtain real-life performance information of pilot ABC systems using DG2 for face recognition.*
- ***Insufficient attention to security in development of inspection systems***
  - *Pay more attention to this, but no concrete operationalisation suggested.*
- ***Non-compliance/Lack of interoperability of e-passports undermining trust of border guards in e-passport chip***
  - *No real countermeasure suggested: Compliance issues have already been on the agenda and this seems the best that can be done.*

- *For real defects: Defect lists*[16]*.*

- ***Attacker travelling on stolen/bought e-passport disabling the chip- when border control is done by border guards who also read chip***

    - *No real solution, as the passport is still a legal travel document with a broken chip; still paying more attention to people with passports with a non-functioning chip can make this disabling the chip an unattractive strategy for the attacker.*

Further discussion

The top 5 of these were discussed:

1. The technical risk that clearly scored highest was the risk of ABC systems accepting a clone of an e-passport that does not have AA or CA that is electronically a perfect copy but visually possibly a very poor one. Concerning mitigation, it was suggested that ICAO guidelines on visual checks on authenticity of the MRZ in ABC systems could still pose an additional hurdle. The obvious mitigation is of course ensuring that all e-passports support AA or CA. Several people expressed regret that e-passports without authenticity check of the passport chip such as AA or CA exist, but pointed out that discussions and agreements at EU level (and ICAO level) thus far have proved incapable of avoiding this situation.

Subsequent discussion of this scenario suggested that although this might be a possibility, and one that is hard to defend against, the risk might actually be small (indeed, risk scores of this issue varied quite a lot, as is clear from the ranges illustrated in Figure 13). It was noted that anyone prepared to go the lengths of making a digital clone might much more easily (and more likely) use the real e-passport. Also, given that the passport data in a clone is still authentic and unalterable, this form of fraud is relatively benign when compared to fraud where passport details are altered.

2. People judged there to be a big risk that the quality of the facial image in DG2 is insufficient to prevent lookalike fraud if used by ABC systems. The quality of DG2 was considered less of an issue when used by human border guards.

When discussing ways to improve the quality of facial images, people observed that standards for the quality have already been discussed and settled for a long time at other fora, and hence expressed little hope of changing this. In particular, the limited resolution of the images is now a given and fundamental limitation, which could only be increased in the longer term.

Now that several ABC systems based on facial recognition are in operation, it would be interesting to see if some clear data on the quality of these systems could be obtained. Of course, getting data on false negatives here is a lot easier than getting good data on the possibility of lookalike fraud.

3. Risks due to insufficient attention to security and development of inspection systems rated high, but did not result in much discussion when it came to the seriousness or possible ways to mitigate it. The clear mitigation strategy here is of course to pay more attention to it, but there were no concrete suggestions on how to effectively operationalise this, e.g. in the form of guidelines, or quality control measures.

4. The risk of fraudsters disabling chips is also rated relatively high. The obvious mitigation strategy is to pay closer attention to people carrying e-passports with non-functioning chips. As a passport without a functioning chip *is* still a valid travel document, ultimately there is little that can be done about this, except treat people with such e-passports with

[16] There is already a proposal underway for defect lists from the joint ISO/IEC JTC1/SC17 Working Group 3 & Task Force 5.

extra attention. As in the online questionnaire, the discussion here showed some difference in opinion on whether the extra attention attracted by disabling the chip in fact outweighs any facilitation of lookalike fraud. (A technical countermeasure, to make disabling the chip by microwave tamper-evident, as apparently employed in UK passports, was only suggested to us after the workshop.)

5. Concerning non-compliance issues and lack of interoperability, people rated the bigger risk here that this would undermine confidence of border guards in the e-passport chips. In the discussion, it became clear that we should distinguish between different forms of lack of interoperability:

   - Operational errors, caused by people putting the MRZ in the incorrect position, or being too impatient and removing the e-passport before the data is read from the chip

   - Real non-compliance or defects, where the chip does not work or contains incorrectly formatted data.

   A border case in this distinction would be MRZs which are more difficult to read with (certain types of) OCR equipment.

   The general impression was that operational errors are much more common than cases of real non-compliance. Moreover, such problems were more likely to be caused by OCR problems reading the MRZ than by problems reading the chip itself.

   People expressed little optimism about reducing this, given that standards and compliance for MRZ is an issue that has already been debated for so long.

   To deal with real defects in specific passport batches, people observed that discussions about formats for "defect lists" are already underway. It was noted that for communicating defect lists one should ideally (re)use an existing mechanism, such as the PKD.

6.4.3.2.Topic #2: *Risk related to production*

The following potential incidents were rated in the technical security workshop:

#	Hypothetical vulnerability	Average risk rating [1-25]
6.	Insufficient trustworthiness of personnel in personalisation	9
9.	Insufficient attention to security in the development of the personalisation system	8
19.	Theft of blank passports (with programmable/configurable chip)	7
20.	Inadequate destruction of chip/e-functionality of old passports	7
18.	Theft of blank passports (with "locked" chip)	7
13.	Insufficient attention to security of the development of the e-passport application	7
10.	Insufficient quality control – passport data (e.g. malformed or incorrect data)	7
7.	Insufficient physical protection of personalisation location	7
11.	Insufficient testing and quality control – personalised passports	6
12.	Insufficient attention to security of the development of chip and operating system	6
8.	Insufficient logical/network access control in personalisation system	6
17.	Insufficient protection of cryptographic keys (especially document signing keys)	6
4.	Insufficient attention to security of the development of the blanks production system	6
14.	Lack of common criteria certification of (the combination of) chip, operating System and e-PASSPORT application	6
16.	Use of a document signing key for too long a period	6
5.	Insufficient testing and quality control – blanks (including chips)	6
1.	Insufficient trustworthiness of personnel production blanks (booklet + chip)	6
15.	Use of SHA-1	5
3.	Insufficient logical/network access control in production system blanks	5
2.	Insufficient physical protection of production location of blanks	4

Table 9 - Average risk ratings Technical Security Topic #2

The following charts were produced based on the attendee responses. Per hypothetical vulnerability, the ratings are displayed as a 25% percentile to 75% percentile box, with the average displayed as the border between the light and dark red box. The minimum and maximum ratings are visualised in error bars. Thus, 50% of the respondents rated the risk within the range of the box (and 25% below and 25% above), while the average is the change in colour of the box.

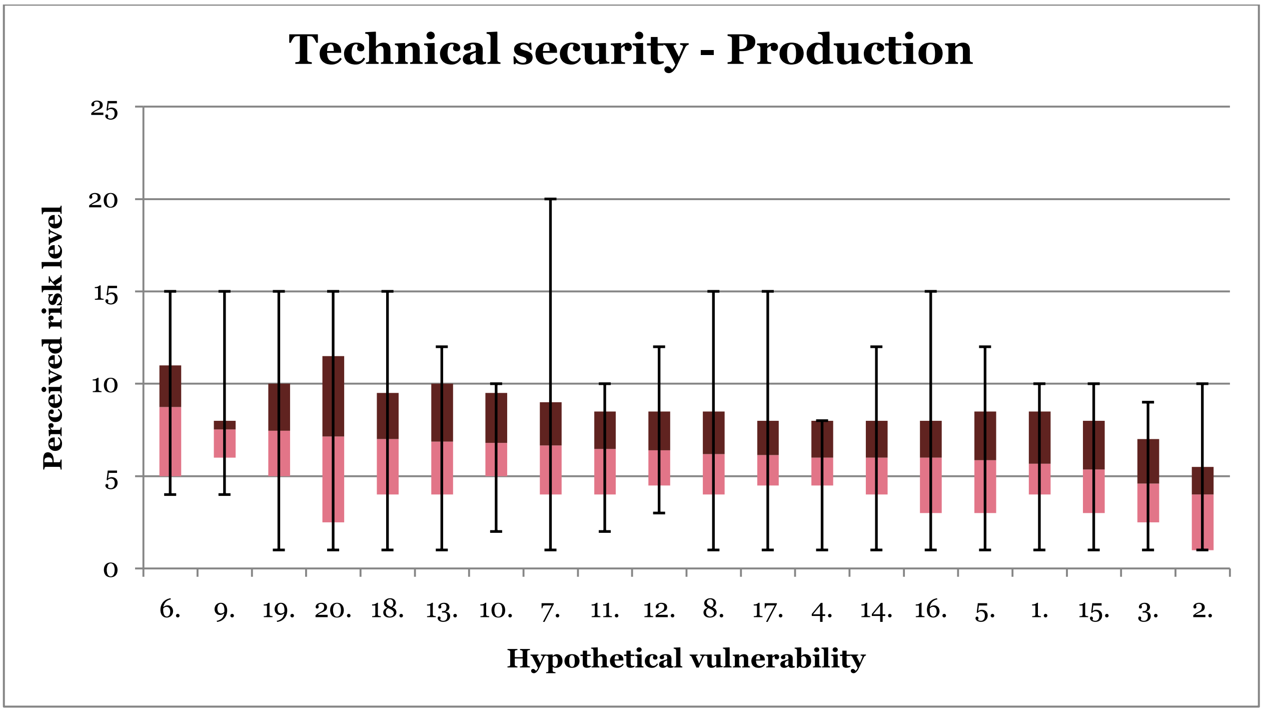


Figure 14 - Technical Security Topic #2 risk rating

Countermeasures for highest risks

- *As a generic countermeasure, perform a study to compare operational conditions across different countries when it comes to production.*
- ***With respect to insufficient trustworthiness of personnel involved in the personalisation of blank e-passports deploy:***
  - *Segregation of duties such that no employee can singlehandedly either personalise or steal an e-passport*
  - *Traceability of individual blank e-passports in combination with good (e.g. audited) accounting procedures.*

Further discussion

For the production issues, people rated the overall risks rather low, and in general, lower than the inspection issues that were discussed. Also, the variation in ratings was a lot higher, perhaps reflecting the fact that people had more of an inspection background.

There was quite some discussion about whether people should estimate risks as they perceive them for the production process in their own country or for production processes across the EU. People noted they had more idea of the situation in their own country than the EU as a whole, but that for border security of the EU as whole the situation across all countries is important in the end. This might also have contributed to the higher variations.

Risks in the personalisation phase were judged to be slightly higher than in the manufacture of blanks, with personnel risks rated as the bigger risk during personalisation. In fact, the risk due to untrustworthy personnel in personalisation, rated at 9, was the only production risk that would have made it to the top 5 of the inspection risk discussed earlier.

Possible risk mitigation strategies for personnel risks are personnel screening, segregation of duties and good (audited) accounting procedures for e.g. blanks discarded as misprints in quality control.

Discussion of the technical risks in production typically led to people arguing that these risks were very small, with the discussion apparently inevitably drifting back to the wider issuance process. There appeared to be a very strong consensus that the actual production and personalisation process was technically the more secure part of the whole issuance process (taking place in highly controlled conditions in secure facilities, with any still blank [i.e. not personalised] e-passports in transit protected by transportation keys), so that there was no real need for further measures to mitigate risks there.

Still, some people expressed concerns that there might be big differences between countries when it comes to production. Indeed, several participants raised the issue that whereas they could judge risks in their own countries, they were in no position to make any good assessment of risks in general across all EU countries. This observation suggests that a comparison of operational conditions across different countries when it comes to production might be useful to detect potential trouble spots, or indeed to confirm that there are none. This is, of course, a broader strategy that concerns many more of the hypothetical vulnerabilities in production.

The use of SHA-1, which we ourselves identified as a potential technical vulnerability with a clear and simple mitigation strategy, only came out very low in the rankings.

6.5. *Risk workshop results on usage*

Although there was limited time available for the completion of the usage risk workshop and not all EU/Schengen Member States were represented, the results offer valuable insights into perceived risk levels of the various hypothetical vulnerabilities.

6.5.1. *Topics identified on usage*

The following topics were proposed and accepted by the workshop participants.

Risk of unauthorised border crossing because of:

Topic 1: Chip of travel document cannot be used or travel document does not have a chip

- Chip broken (on purpose or by accident)
- Document does not have a chip or a non-compliant chip (ID cards)

Topic 2: Possibilities of (second generation) e-passport are not fully used or not used correctly

- Chip not used (by choice)
- Fingerprints not used (lookalike fraud)

Topic 3: Unavailability of a reliable inspection infrastructure

- Inspection system broken or communication not working
- Security mechanisms not verified or not correctly verified

6.5.2. *Main workshop results on usage*

Different perceptions of risk among participants

The results show that participants display a very different perception of risks. This can be observed in the high variation of participants in the rating of risks. A possible cause is that in different countries, risks are perceived very differently.

Even the highest scoring risks do not have an average score of above 15 on a scale of 1 to 25.

Topic #1: Chip of travel document cannot be used or travel document does not have a chip

The high risks (average score of 10 or higher) in the “chip of travel document cannot be used or travel document does not have a chip” topic are:

1. *National Identity Card can be used at border control*
   (can be a weak link: no chip or non-compliant chip, e.g. contact chip)
2. *Chip broken on purpose*
3. *Lack of centralised security standards (referral to second line)*

Risks related to problems in setting up the communication between chip and inspection system, including initiating Basic Access Control, were considered very low by the workshop participants.

The participants indicated that the highest ranking risk, i.e. use of national identity cards as travel documents, could be mitigated by either prohibiting the use of national identity cards as travel documents or by putting requirements on national identity cards used as travel documents similar to the EU passport specification. Both proposed controls would require regulation at EU level.

Regarding the risk of a broken chip, some participants mentioned that the chip is not the only security feature of the passports, that at the moment a significant number of passports do not have a chip yet, and that quite often the chip isn't read at border control anyway. The high score of this risk, however, indicates that many participants consider it a serious risk. A broken chip should not be a way to cross the border more easily with a falsified or counterfeited passport or as a lookalike, so when the chip is broken, thorough visual inspection, preferably at second line, is required. One participant noted that it is possible to choose the material of the data page where the chip can be placed in such a way that breaking the chip on purpose using microwave radiation can be detected.

Lack of centralised security standards is considered a serious risk, since the absence of internal borders within the EU Schengen area means that the quality of external border control in one Member State influences the security of all Member States. Inadequate border control of a Member State poses a risk to all Member States within the Schengen area. A minimum set of central or harmonised security standards for border control would be a way to ensure a base level. This could be realised by EU regulations.

Please see Section 6.5.3.2 for a detailed discussion of possible countermeasures related to these risks.

Topic #2: Possibilities of (second generation) e-passport are not fully used or not used correctly

The high risks (average score of 10 or higher) in the "possibilities of (second generation) e-passport are not fully used or not used correctly" topic are:

1. *No EU rules and regulations on border control*
    a. *No requirement to read the chip when present*
    b. *No requirement on automated biometric verification when chip is present*
    c. *No requirement to use fingerprints when present*
    d. *No requirements for first line fixed inspection systems operated by border guard*
    e. *No requirements for first line mobile inspection systems operated by border guard*
    f. *No requirements for ABC systems (supervised by border guard)*
    g. *No requirements for second line inspection*
    h. *No requirements for referral to second line inspection when first line verification fails (highest score of sub-risks)*
2. *No verification of fingerprints at second line inspection*

3. *Lack of specific training of border guards on e-passport handling*

4. *No standard procedures when the security mechanisms fail*

5. *No standard procedures when reading the chip fails*

The first three risks scored equally high. A remarkable outcome of the risk assessment of Topic 2 is that the absence of fingerprint verification at ABC systems is considered a low risk, while this was considered an intermediate risk for other border control situations. This puts a lot of trust in the automated verification of the face against the image stored in the chip, which might not be based on numbers.

The participants noted that fingerprint verification at first line border control does not seem to be feasible at manned booths or when using mobile inspection systems, since it takes too long. The average time a border guard has for one passenger at first line border control is 10 seconds. However, as the high score indicates, the majority of the participants thought that fingerprint verification at second line border control should be implemented. A participant noted, however, that depending on the situation at the border control post, implementation of fingerprint verification at second line is also not always feasible, e.g. when it is a small border post with a low number of passengers entering from outside the Schengen area. A participant also remarked that at second line the focus is on the traveller, asking him/her questions and doing a background check, meaning that fingerprint verification does not add to the verification process at second line.

Specific training of border guards on the handling of e-passports is considered important since the addition of the chip to the passport is a relatively new development where the border control agencies cannot draw on years of experience.

The lack of EU rules and regulations, especially requirements on referral to second line when first line verification fails, and the absence of standard procedures were considered serious risks by the workshop participants. Just as when discussing the first topic, it was noted that the absence of internal borders within the EU Schengen area means that the quality of external border control in one Member State influences the security of all Member States, and a base level of border control should be guaranteed. This could be guaranteed via EU regulation.

Please see Section 0 for a more detailed discussion of possible countermeasures related to these risks.

Topic #3: Unavailability of a reliable inspection infrastructure

The high risks (average score of 10 or higher) in the “unavailability of a reliable inspection infrastructure” topic are:

1. *Likelihood that fingerprint verification does not work because of:*

    a. *No working verifying PKI up to inspection systems*

    b. *No exchange mechanism for certificates (requests) with other countries (SPOC or bilateral) in own country*

    c. *Other countries are not able to receive or sign DVCA certificate requests*

    d. *Quality of fingerprints stored in chip is too low (reliability)*

2. *No checking of AA or CA*

3. *IS only support AA or only CA (one exclusively, not both)*
4. *Insufficient security in Systems Development Life Cycle of border control systems*
5. *Insufficient confidentiality protection of (EAC) private keys (security)*
6. *Insufficient integrity protection of (storage of) public key certificates (DS certificates, CSCA)*
7. *Not checking PA or not correctly/fully checking PA because of no verification of the signature by IS (only the hash-value)*

There are many high-scoring risks regarding Topic 3. These risks can be categorised according to three subjects:

a) Fingerprint verification does not work because the supporting verifying (EAC) PKI and certificate exchange is not up and running or the quality of the stored fingerprints is too low

b) Verification of security mechanisms (AA, CA, PA) does not work (correctly)

c) Security protection of the inspection systems is insufficient

Just as when assessing the risks related to Topic 1, the risks related to low-level technical interoperability were considered low in Topic 3 as well.

The participants indicate that they consider the fact that fingerprint verification does not pose a serious risk. This indicates that they consider the availability of fingerprint verification at border control important. It is considered a serious risk that fingerprint verification does not work since the implementation, including setting up and operating the verifying (EAC) PKI required to obtain access to the stored fingerprints and the corresponding exchange of certificates and certificate requests, may be considered quite extensive and complex. This could be helped by providing training on the implementation and sharing best practices and lessons learnt. The low quality of stored fingerprints by some countries is also considered a serious risk. This could be mitigated by putting requirements on stored fingerprint quality in Europe, e.g. as part of the EU passport specification.

The second group of serious risks is related to the non-functioning or incorrect functioning of the verification of the chip security mechanisms Active Authentication, Chip Authentication, and Passive Authentication in the inspection systems. The participants indicated they consider a mechanism to determine the authenticity of the chip very important. During the discussion, it was mentioned that AA and CA (if not the whole chip) are considered “just” additional security features for determining that the passport as a whole is authentic. In this way, the function of the chip would be reduced to a security feature, rather than an enabler of biometric ID verification.

The participants mentioned that at the moment not all chips contain such a mechanism, so verification is not always possible. Besides, verification of AA or CA is also not mandatory. Implementation of AA and CA could be stimulated by training and sharing experiences and could be regulated when the EU would issue a standard on inspection systems. For Passive Authentication, the main problem seems to be the absence of CSCA certificates in the inspection infrastructure to verify the DS certificate. CSCA certificates may not be available since the exchange is not yet organised well and since participation in the ICAO Public Key Directory is still limited. This may be solved by promoting participation in the ICAO PKD and training on how to connect to the ICAO PKD.

With respect to the third serious risk, the security of inspection systems, requirements at EU level, e.g. by defining and accepting a Common Criteria Protection Profile for inspection systems, could be the way to go here.

Please see Section 0 for a more detailed discussion of possible countermeasures related to these risks.

6.5.3. *Detailed results of the usage workshop*

6.5.3.1. General feedback

Many risks are considered to be of high or medium importance (average rating of or above 7). Only very few risks are considered of low importance. These are mainly related to technical inoperability.

6.5.3.2. Topic #1: *Chip of travel document cannot be used or travel document doesn't have a chip*

The average risk scores of the different vulnerabilities are indicated in the table below.

#	Hypothetical vulnerability	Average risk rating [1-25]
4	National identity card is used (can be a weak link: no chip or non-compliant chip, e.g. contact chip) (V.50)	**14**
9	Chip broken on purpose	**12**
6	Lack of centralised security standards (referral to second line) (V.1)	**11**
8	Chip broken by accident	**9**
18	No standard procedures for when the chip cannot be read, e.g. referral to second line inspection	**9**
7	Lack of audits/auditability of border guard (V.2)	**8**
19	Too few personnel when a significant number of chips cannot be read	**8**
5	Insufficient quality of e-passports (defects) (V.52)	**8**
10	Chip not present	**7**
3	Chip communication is jammed (V.49)	**7**
1	Insufficient border guards available when border control systems are not available (V.62)	**7**
2	Chip is disabled (V.48)	**7**
13	Jamming of chip-terminal communication	**5**
11	Chip non-compliant with ICAO Doc 9303	**5**

16	Setting up communication (BAC) doesn’t work because OCR of MRZ is not possible because of shiny laminate (take into account whether the MRZ can be given in manually)	**4**
17	Setting up BAC failed for another reason	**4**
14	Chip cannot be read due to low-level problems in initiating the RF communication	**3**
15	Setting up communication (BAC) doesn’t work because of placement of antenna in relation to the MRZ (take into account whether the MRZ can be given in manually)	**2**
12	Chip cannot be read because of metallic shielding	**2**

Table 10 - Average risk ratings Usage Topic #1

The following charts were produced based on the attendee responses. Per hypothetical vulnerability, the ratings are displayed as a 25% percentile to 75% percentile box, with the average displayed as the border between the light and dark red box. The minimum and maximum ratings are depicted in error bars. Thus, 50% of the respondents rated the risk within the range of the box (and 25% below and 25% above), while the average is the change in colour of the box.

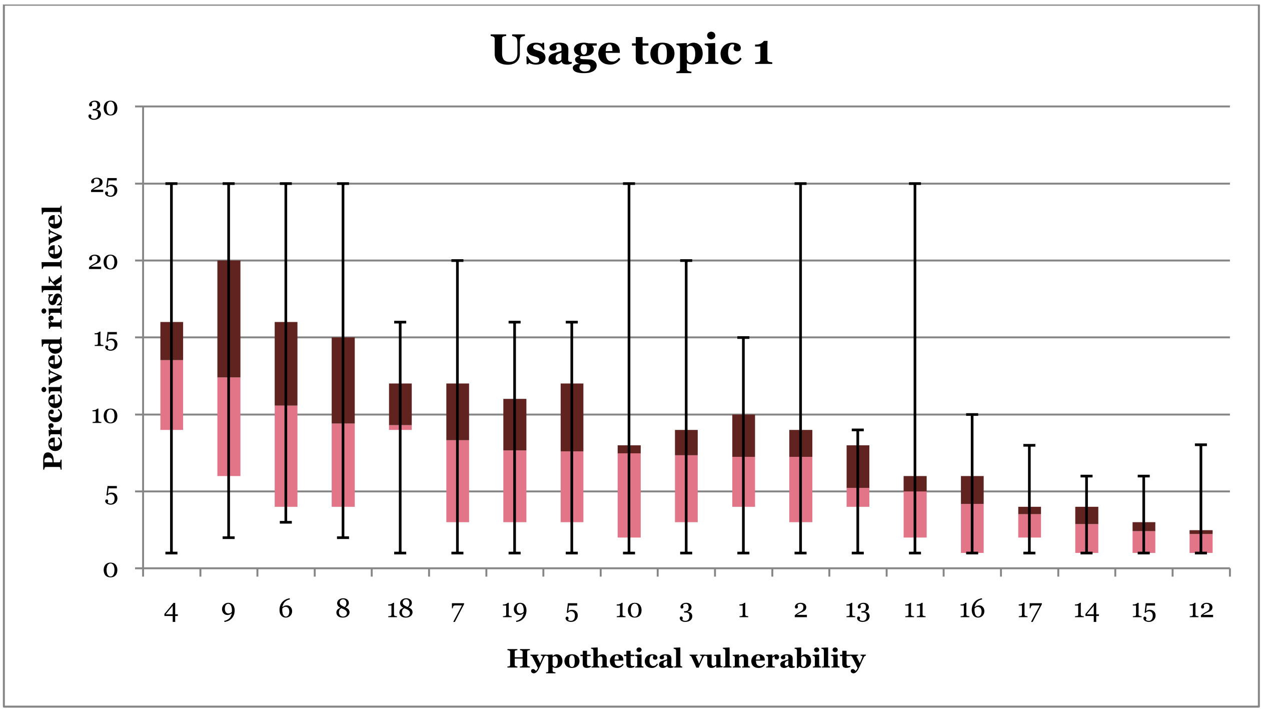


Figure 15 - Usage topic #1 risk rating

Countermeasures for highest risks

The controls to mitigate the high-scoring risks in topic 1 can be:

1. *National identity card can be used at border control*
   Regulation at EU level regarding which documents can be used as travel documents or minimum security requirements on all travel documents.

2. *Chip broken on purpose*
   Thorough second line inspection when the chip of an e-passport is broken so this isn't an advantage to cross the border illegally.

   - Use material for the data page of the e-passport which shows when the e-passport has been microwaved and place the chip in this data page.

3. *Lack of centralised security standards (refer to second line).*
   Regulation at EU level regarding border control standards and procedures.

Further discussion

Risks related to technical interoperability issues score low.

The highest-scoring risk is use of national identity cards as travel documents. Within the European Union, national identity cards can be used as travel documents between Schengen and non-Schengen countries. In certain EU Member States, national identity cards are the most used travel documents by EU citizens to cross the border. All EU citizens can use their national identity cards to return to the European Union from abroad. National identity cards can also be used as travel documents for certain countries outside the EU (based on bilateral agreements).

However, contrary to passports issued by EU Member States, national identity cards do not need to comply with a common specification. National identity cards, for example, do not need to contain a chip or may contain a contact chip. The security of national identity cards can be significantly less compared with EU passports, thus, making unauthorised border crossing on the basis of a falsified or counterfeited national identity card more likely than on the basis of a passport.

To counter the threat national identity cards pose for unauthorised border crossing, participants suggested that regulation at EU level is required. Such regulation may either require the use of passports at external border crossings, or establish (minimum) requirements for security features that national identity cards should fulfil to function as travel documents. Compliance of the identity cards to, for example, the EU passport specification could be required.

The second-highest scoring risk is a (purposely) broken chip in an e-passport. When the chip of an e-passport is broken, the passport is still valid to enter the EU or to cross borders within the EU between Schengen and non-Schengen countries. When the chip is broken, the additional security offered by the chip cannot be used. This additional security includes the possibility of automated face and fingerprint verification, the possibility to show the facial image stored in the chip to the border guard to be compared with the image on the data page and to the holder, the checking of the authenticity of the chip and the chip data and the possibility to compare the biographic data in the chip to the biographic data on the data page. It may, therefore, be advantageous to break the chip on purpose, thus enhancing the possibilities of a lookalike fraud and use of counterfeited or falsified passports. Conversely, a broken chip does attract extra unwelcome attention for the attacker.

Breaking the chip is rather easy (e.g. using microwave radiation) and is hard to detect.[17] Conversely, a broken chip is likely to attract more attention, which may not be welcome for the attacker.

When the chip is supposed to be read at border control, but does not work, the passport will be visually inspected. Although it will not (immediately) be clear whether the chip broke down accidentally or was broken on purpose or perhaps even whether the chip is not working in combination with the inspection system, the passport should be checked more thoroughly than

[17] The UK has passports where the data page containing the chip visibly changes when microwave radiation is applied.

standard visual first line border control inspection to counter the enhanced risk of unauthorised border crossing. Preferably, the passport should be referred to second line inspection.

Some participants mentioned that the chip is not the only security feature of the passports, that at the moment a significant number of passports does not have a chip yet, and that quite often the chip isn't read at border control anyway. The high score of the risk, however, indicates that many participants consider it a serious risk.

The third-highest scoring risk is the lack of centralised security standards, e.g. about referral to second line inspection. Because of the absence of internal borders within the EU Schengen area, the quality of external border control in one Member State influences the security of all Member States. Inadequate border control of a Member State poses a risk to all Member States within the Schengen area. Therefore, a minimum set of centrally imposed or harmonised security standards for border control would be a way to ensure a base level. Topic #2: *Possibilities of (second- generation) e-passport are not fully used or not used correctly*

The average risk scores of the different vulnerabilities are indicated in the table below.

#	Hypothetical vulnerability	Average risk rating [1-25]
6	No EU rules and regulations on border control	
	6-8 No requirements for referral to second line when first line verification fails	**12**
	6-5 No requirements for first line mobile inspection systems operated by border guard	**11**
	6-6 No requirements for ABC systems (supervised by border guard)	**11**
	6-7 No requirements for second line inspection	**11**
	6-3 No requirement to use fingerprints when present	**11**
	6-1 No requirement to read the chip when present	**11**
	6-4 No requirements for first line fixed inspection systems operated by border guard	**11**
	6-2 No requirement on automated biometric verification when chip is present	**10**
12	No verification of fingerprints at	
	12-4 Second line inspection system	**12**
	12-2 First line mobile reader	**8**
	12-1 First line manned booth	**8**
	12-3 ABC system	**6**
9	Lack of specific training of border guards on e-passport handling	**12**

8	No standard procedures when the security mechanisms fail	**10**
7	No standard procedures when reading the chip fails	**10**
1	Insufficient guidance provided by border system to border guard (V.51)	**9**
2	Insufficient operational ability for border control to evaluate security mechanisms of the e-passport (V.52)	**8**
10	Not using the chip at all	**8**
11	No automated verification of facial image at	
	11-3 ABC system	**8**
	11-4 Second line inspection system	**7**
	11-2 First line mobile reader	**7**
	11-1 First line manned booth	**6**
4	Insufficient biometric quality (V.59)	**8**
3	Issues when verifying biometrics during border control (V.56)	**7**
5	Lack of centralised security standards (V.1)	**5**

Table 11 - Average risk ratings usage topic #2

The following charts were produced based on the attendee responses. Per hypothetical vulnerability, the ratings are displayed as a 25% percentile- 75% percentile box, with the average displayed as the border between the light and dark red boxes. The minimum and maximum ratings are visualised in error bars. Thus, 50% of the respondents rated the risk within the range of the box (and, thus, 25% below and 25% above), while the average is the change in colour of the box.

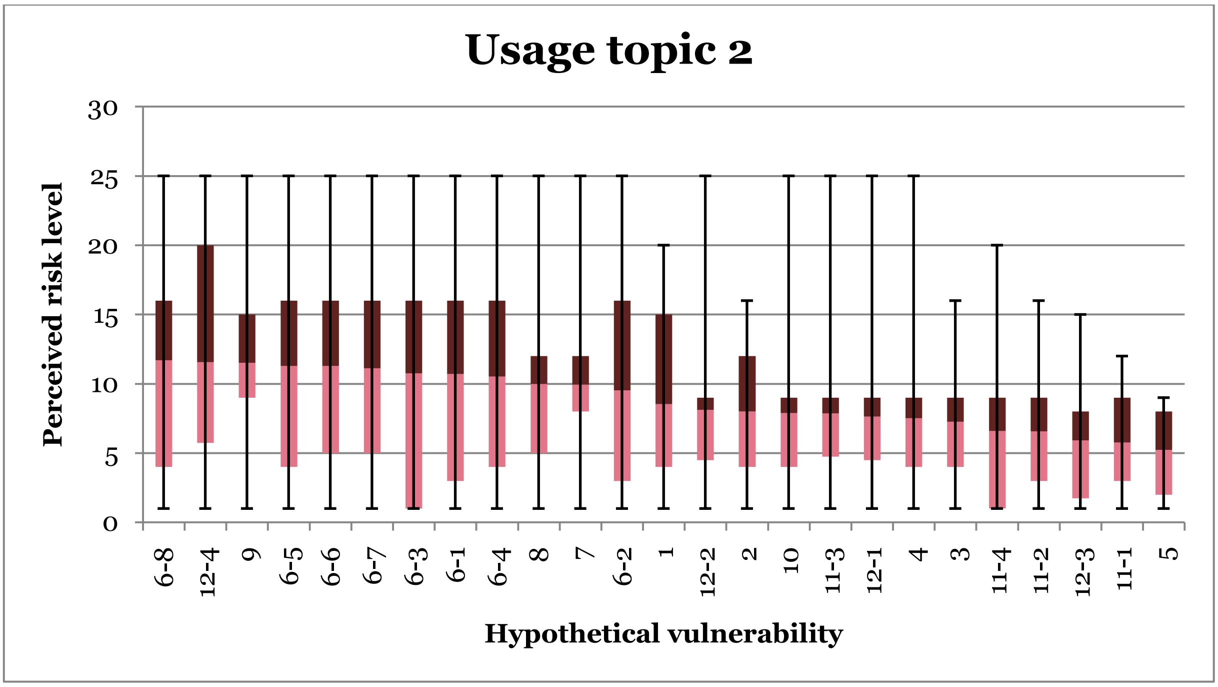


Figure 16 - Usage topic #2 risk rating

Countermeasures for highest risks

The controls to mitigate the high-scoring risks related to topic 2 can be:

1. *No EU rules and regulations on border control*
   Regulation at EU level on border control, i.e. requirements on reading the chip, automated biometric verification, implementation of fingerprint verification, inspection systems, mobile readers and ABC systems, requirements for second line inspection and referral to second line inspection.

2. *No verification of fingerprints at second line inspection*
   Regulation at EU level on implementation of fingerprint verification, inspection systems, mobile readers and ABC systems, requirements for second line inspection and referral to second line inspection.

3. *Lack of specific training of border guards on e-passport handling*
   Training of EU border guards specifically focused on e-passport handling.

4. *No standard procedures when the security mechanisms fail*
   Defining standard procedures, preferably at EU level, but also at a national level, on handling failures in reading the chip or verifying the chip security mechanisms.

5. *No standard procedures when reading the chip fails*
   Defining standard procedures, preferably at EU level but also at a national level, on handling failures in reading the chip or verifying the chip security mechanisms.

Further discussion

There are three types of risks which score high for this topic: (a) that there are no EU requirements or standard procedures, e.g. for referral to second line inspection when first line verification fails, (b) that fingerprints are not verified at second line inspection and (c) that border guards are not sufficiently trained on specifically handling e-passports.

The purpose of border control is to keep ineligible persons (i.e. persons without the correct rights, persons mentioned on watch lists, persons personating someone else) out of the country. First line border control aims to pick all travellers who require more thorough inspection. From an efficiency perspective, first line border control must be performed fast or in an automated way. A border guard has on average 10 seconds to determine whether the passport is genuine, belongs to the holder, and the traveller is eligible to enter the country. When there is doubt, a more thorough investigation is required. This is normally done at second line border control where more time is available to investigate the passport and its holder. The traveller can be questioned, information systems can be checked, and additional means to establish the authenticity of the passport may be available.

When inspection is performed only visually by a border guard, referral to second line when in doubt is obvious. However, when automated inspection of the chip or automated biometric verification fails at a manned booth or border guard operated mobile inspection system, referral to second line may not be done if the border guard at first line inspection does not consider this necessary based on a visual inspection of the passport and its holder. This then, however, undermines the security added by the e-passport chip. Since border control has become a shared task in the EU Schengen area, the participants indicated that a common policy on the importance of the chip in the passport with respect to the passport booklet seems necessary. Similarly, the participants indicated that it seems logical to have a common policy on border control in general, including requirements for first and second line border control, referral to second line inspection, using the chip, automated biometric verification, inspection systems, mobile readers and ABC systems.

Time considerations seem to make fingerprint verification not suitable for first line border control at manned booths or when mobile inspection systems are used by border guards, but it seems to be an effective way to determine or rule out lookalike fraud at second line inspection. Fingerprints have been added to passports to provide a more reliable way to verify the holder's identity. Using this potential seems logical. And since border control has become a shared task in the EU Schengen area, the participants indicated that it seems logical to have common requirements within the EU on the use of fingerprint verification at (second line) border control. One workshop participant, however, remarked that this may be difficult for border control points with a low number of foreign travellers. A participant also remarked that at second line, the focus is on the traveller, asking him/her questions and doing a background check, meaning that fingerprint verification does not add to the verification process at second line.

Border control agencies have years of experience checking paper travel documents. The chip is a relatively new addition only present in passports issued since 2006. Use of the chip at border control is even a more recent development. This means border control agencies are still lacking the experience in chip inspection which they have for inspection of the paper documents. This is considered a serious risk by the respondents. The risk posed by this lack of experience with chip inspection could be diminished by training border control agents specifically on handling e-passports.

A remarkable outcome of the risk assessment on topic 2 is that the absence of fingerprint verification at ABC systems is not considered a serious or even intermediate risk. This puts a lot of trust on the automated verification of the face against the image stored in the chip, which might not be based on numbers.

6.5.3.3. Topic #3: *Unavailability of a reliable inspection infrastructure*

#	Hypothetical vulnerability	Average risk rating [1-25]
13	Likelihood that fingerprint verification doesn't work because of:	
	13-1 No working verifying PKI up to inspection systems	**15**
	13-2 No exchange mechanism for certificates (requests) with other countries (SPOC or bilateral) in own country	**14**
	13-3 Other countries are not able to receive or sign DVCA certificate requests	**11**
	13-8 Quality of fingerprints stored in chip too low (reliability)	**10**
	13-7 No fingerprint scanners at second line inspection	**9**
	13-4 No fingerprint scanners at first line manned booth	**7**
	13-5 No fingerprint scanners at first line mobile inspection system	**7**
	13-6 No fingerprint scanners at ABC systems	**6**
15	Not checking AA or CA	**12**
16	IS only support AA or only CA (one exclusively, not both)	**11**
2	Insufficient security in Systems Development Life Cycle of border control systems (V.65)	**11**
4	Insufficient confidentiality protection of (EAC) private keys (V.61)	**10**
3	Insufficient integrity protection of (storage of) public key certificates (DS certificates, CSCA) (V.60)	**10**
14	Not checking PA or not correctly/fully checking PA because of	
	14-1 No verification of the signature by IS (only the hash values)	**10**
	14-5 Illegitimate insertion of CSCA certificates in IS	**9**
	14-2 No verification of certificates (spoofing of CSCA possible)	**9**
	14-3 (CSCA) certificates unavailable	**8**
	14-4 DS certificates unavailable	**7**
	14-6 No proper use of CRLs (placement/distribution takes too long, CRLs are not	**7**

	downloaded/used)	
5	Lack of centralised security standards (V.1)	**9**
1	Insufficient logical/network access controls in border control systems (V.64)	**9**
11	Not showing the facial image from the chip to the border guard	
	11-2 First line mobile inspection system	**8**
	11-1 First line manned booth	**7**
	11-3 Second line inspection system	**7**
12	Purposely misconfigured terminals	**8**
8	No EU protection profile for inspection systems and ABC systems	**8**
7	No functional specifications for inspection systems and ABC systems	**7**
10	Not explicitly comparing the MRZ from data page to MRZ from chip	**7**
6	Accidentally misconfigured terminals	
	6-2 Technical communication problems due to software	**6**
	6-1 Technical communication problems due to hardware	**4**
9	Technical problems with interpretation of e-passport data	**5**

Table 12 - Average risk ratings usage topic #3

The following charts were produced based on the attendee responses. Per hypothetical vulnerability, the ratings are displayed as a 25% percentile- 75% percentile box, with the average displayed as the border between the light and dark red boxes. The minimum and maximum ratings are visualised in error bars. Thus, 50% of the respondents rated the risk within the range of the box (and, thus, 25% below and 25% above), while the average is the change in colour of the box.

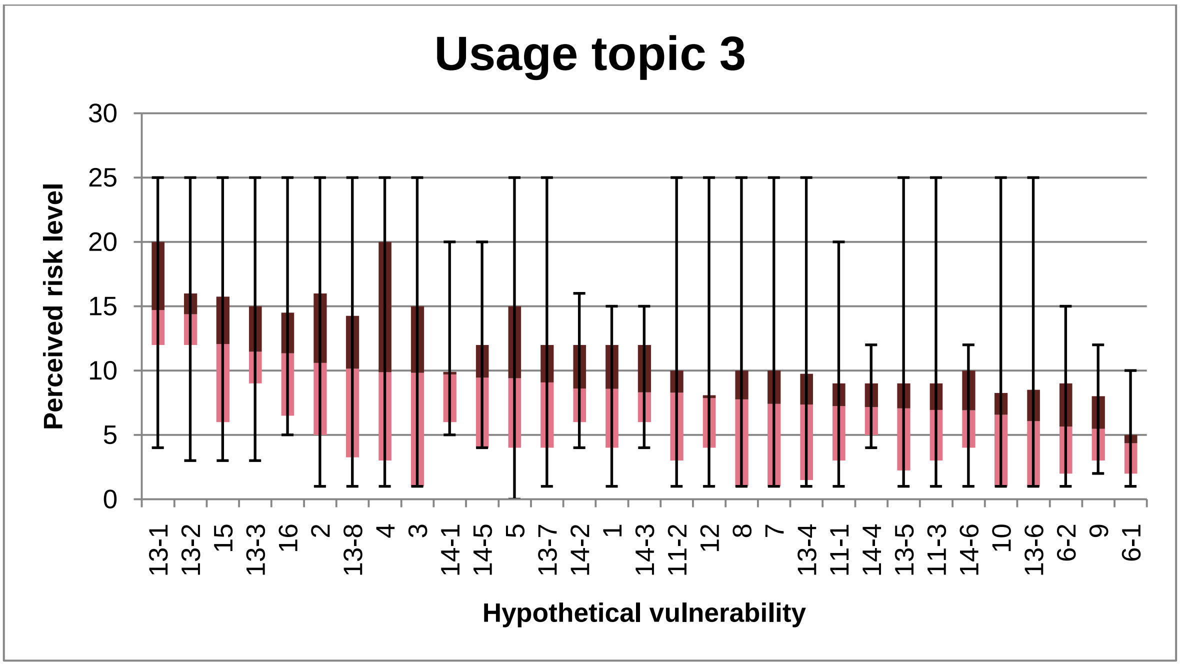


Figure 17 - Usage topic #3 risk rating

Possible countermeasures for topic #3

The controls to mitigate the high-scoring risks related to topic 3 can be:

a) *Fingerprint verification does not work because the supporting verifying (EAC) PKI and certificate exchange is not up and running or the quality of the stored fingerprints is too low*

- Training of EU border guards on implementation of a verifying (EAC) PKI.
- Sharing experiences, best practices and lessons learnt on implementation of a verifying (EAC) PKI.
- Taking a practical approach to implement fingerprint verification already for one's own country nationals' e-passports when certificate exchange is not yet available. By taking the practical approach to implement fingerprint verification for its own national e-passports, the majority of e-passports offered at border control will be subjected to fingerprint verification.
- Regulation on the quality of stored fingerprints at EU level.
- Regulation on the automated inspection process at EU level.

b) *Verification of security mechanisms (AA, CA, PA) does not work (correctly)*

- Training of EU border guards on participation and connection to the ICAO Public Key Directory.

- Sharing experiences, best practices and lessons learnt on participation and connection to the ICAO Public Key Directory.

- Taking a practical approach, determining the DS certificates from a significant number of e-passports read at border control, to implement Passive Authentication verification when certificates and certificate exchange are not yet available. By taking a practical approach, the majority of e-passports offered at border control may be subjected to PA verification.

- Regulation on the automated inspection process at EU level.

c) *Security protection of the inspection systems is not ok*
Regulation at EU level on Common Criteria evaluation of inspection systems according to an EU-wide accepted protection profile.

Further discussion

There are many high-scoring risks regarding topic 3. These risks can be categorised according to three subjects: (a) fingerprint verification does not work because the supporting verifying (EAC) PKI and certificate exchange is not up and running or the quality of the stored fingerprints is too low, (b) verification of security mechanisms (AA, CA, PA) does not work (correctly) and (c) security protection of the inspection systems is not good.

Like assessing the risks related to topic 1, also for topic 3 the risks related to technical low-level interoperability scored low.

Accessing the fingerprints stored in e-passports requires a PKI infrastructure stretched out over inspection system, DVCA and CVCA and the possibility of the exchange of certificates and certificate requests between these parties. To be able to access the fingerprints in foreign passports, exchange of certificates and certificate requests between the DVCA of the inspecting country and CVCA of the issuing country is required, so exchange across borders. EU regulation prescribes that this takes place in an automated way via national Single Point of Contacts (SPOCs) which comply with CSN 36 9791.

The workshop participants considered it a serious risk that the PKI infrastructure up to the individual inspection systems is not (yet) in place and the exchange of certificates between countries is not (yet) possible either because the verifying country or the issuing country is not ready for it.

Setting up the verifying PKI and SPOC takes a country time and effort. It can be facilitated by training on the subject and by sharing best practices and lessons learnt between countries.

Besides, the participants suggested that it may be worthwhile to take a pragmatic approach by first setting up the national verifying PKI without bothering about automated certificate exchange with other countries since most passports offered at the border will be from that country's nationals. Being able to verify the fingerprints of these passports ensures the majority of offered passports can be checked on fingerprints. Certificate exchange with other countries can also be done via diplomatic means and requires diplomatic means for first-time exchange anyway, not yet requiring automated exchange via a SPOC.

For reliable fingerprint verification, the stored fingerprints need to meet a minimum quality. When the stored fingerprint images have poor quality, this either gives rise to many false acceptances when a low threshold has been set or to many false rejections when a high threshold has been set. In the workshop, it was discussed to further investigate the required level of quality. To ensure stored fingerprints fulfil these quality requirements as much as possible (assuming the passport holder has suitable fingerprints), regulation may be required.

The workshop participants also considered it a serious risk when the authenticity of the chip was not checked via Active Authentication (AA) or Chip Authentication (CA). This may either be by choice of the inspection authority, because these mechanisms are not supported by the passport, or because the inspection system is not capable to perform the verification e.g. because it only supports one of the two mechanisms, while the chip solely supports the other mechanism.

Active and Chip Authentication are mechanisms to guarantee the authenticity of the chip itself. Active Authentication is optional for EU e-passports; Chip Authentication is mandatory for second-generation e-passports. Support of Active Authentication could be mandated by EU regulation for countries not changing to second-generation e-passports. Verification of either Active Authentication or Chip Authentication during inspection and support of both mechanisms by the inspection system could also be mandated by regulation. Inadequate border control of a Member State poses a risk to all Member States within the Schengen area. The participants think regulation may, therefore, be the way to go.

Besides the risks related to Active and Chip Authentication, the respondents also considered it a serious risk that Passive Authentication is not verified at inspection or not correctly verified. Use of Passive Authentication to protect the data is mandatory. Passive Authentication can be considered the most important security mechanism of the chip.

Passive Authentication verification by the inspection system requires the inspection system to (1) recalculate the hashes over the data which are used as input for the signature, (2) verify the signature itself using the public key from the DS certificate, (3) verify the DS certificate using the CSCA certificate from a trusted store and (4) verify the absence of DS and CSCA certificates on the most recent CRL. Only checking all these different steps assures the authenticity of the chip data. If the DS certificate is not checked, this gives rise to the possibility of introducing a non-existing Document Signer. Similarly, if insertion of a CSCA certificate to the trusted store is possible, a non-existing CSCA can be introduced.

Correct implementation of Passive Authentication requires time and effort. It can be facilitated by training on the subject and by sharing best practices and lessons learnt between countries. Attention could, for example, be paid to information about how to join and access the ICAO PKD. If a CSCA certificate of a country is not available via bilateral exchange or if its DS certificates are not available from the ICAO PKD, another option is to take a pragmatic approach to determine the DS public key. If the DS public keys from a significant number of passports (determined at different times) match, it was suggested in the workshop to assume this as a genuine DS public key with which the PA signature can be verified.

The third serious risk identified by the workshop participants is insufficient security of the inspection systems. This can be caused among others by insufficient security in the inspection system development life cycle, insufficient integrity protection of public key certificates (DC, CSCA) in the inspection system and/or insufficient confidentiality protection of (EAC) private keys in the inspection system.

To ensure a minimum security level of the inspection system, a Common Criteria protection profile for border control inspection systems could be defined and accepted at a European level and a Common Criteria evaluation according to the protection profile could be mandated. This would also guarantee a certain level of security in the development life cycle.

7. Analysis of e-passport samples read

7.1. Scope and purpose

The attendees to the workshop were asked to have their e-MRPs and e-MRTDs read and analysed on a voluntary basis.

This analysis was done for the following purposes:

- To individuate differences in European e-MRTD configurations.
- To make an inventory of security features supported in different European e-MRTD configurations.
- To validate a statement made during the interviews regarding differences in biometrics quality.
- To identify deviations from ICAO and EU standards for European e-MRTDs.
- To raise awareness regarding the e-MRTD chip contents and about the variety in e-MRTDs that can be expected at border control.

7.2. Materials and methods

7.2.1. Approach

Focusing on serving the abovementioned purposes of the e-MRTD analysis, an exploratory research approach was taken. It was not aiming at completeness or on gathering a representative sample of the European e-MRTDs currently in the field.

7.2.2. Set-up of the read and analysis environment

The system for reading and analysis consisted of a PC, the e-MRTD Explorer module of the Collis e-MRTD Test Tool and a full-page passport reader with an antenna for reading contactless chips. This system was installed at Frontex offices, in the meeting room of the risk analysis workshop. The system was operated by Mr. Peter Kok, PhD, technical expert in e-MRTD technology.

7.2.3. Actual reading and analysis

The actual reading and analysis of individual e-MRTDs were done during the risk assessment workshop. Attendees brought their passport for reading and analysis. After reading, the chip contents were automatically analysed, and an e-MRTD Explorer Report, containing the chip contents including an explanation in English, was provided to the holder of the analysed e-MRTD. The results were stored for further investigation.

On the results of the individual e-MRTD reading and analysis, further analysis was carried out in which the following steps were taken:

- To individuate differences in European e-MRTD configurations, the availability of different data groups in e-MRTDs was identified and listed, based upon the interpreted chip contents.

- To make an inventory of electronic security features supported in European e-MRTDs, the supported security mechanisms were identified and listed, based on the interpreted chip contents.

- To validate a statement made regarding differences in biometrics quality, the face biometrics read from all e-MRTDs were analysed and compared.

- To identify deviations from ICAO and EU standards, the interpreted chip contents were analysed by e-MRTD experts.

- To raise awareness regarding e-MRTD chip contents, the attendees received the e-MRTD Explorer Report with the analysis results of their own e-MRTD.

- To raise awareness about the variety in e-MRTDs that can be expected at border control, the preliminary results of this analysis have been presented on the second day of the risk assessment workshop.

7.3. *Results*

7.3.1. Sampling

In total, 35 different e-MRTDs were read. Three of these documents have been excluded from further analysis as they appeared to be test documents rather than real, valid e-MRTDs.

7.3.2. Different e-MRTD configurations

The 32 documents analysed represented 21 different document configurations, originating from 16 different Member States.

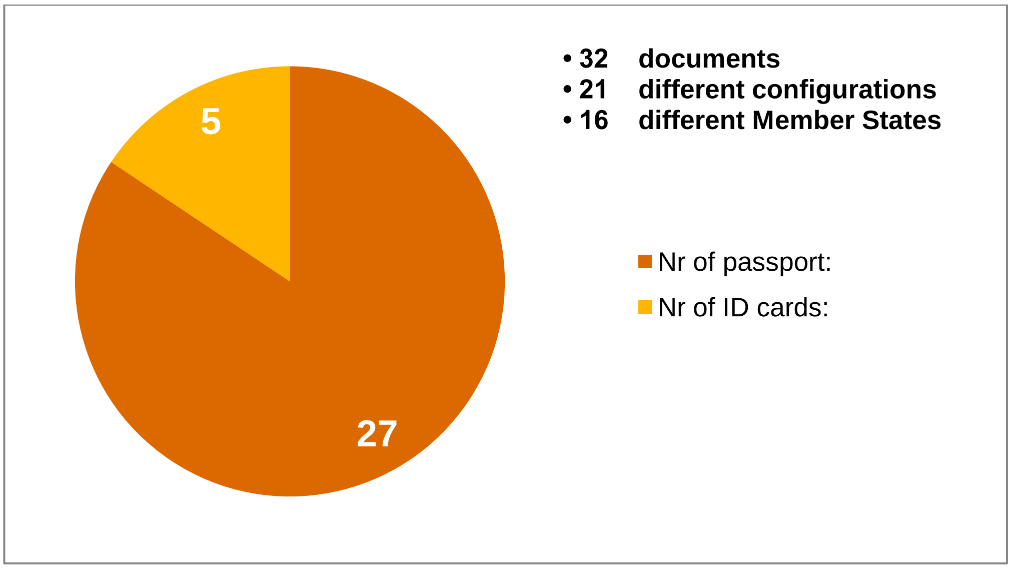


Figure 18 - eMRTD configurations

The availability of data groups present in these 32 documents is distributed as follows:

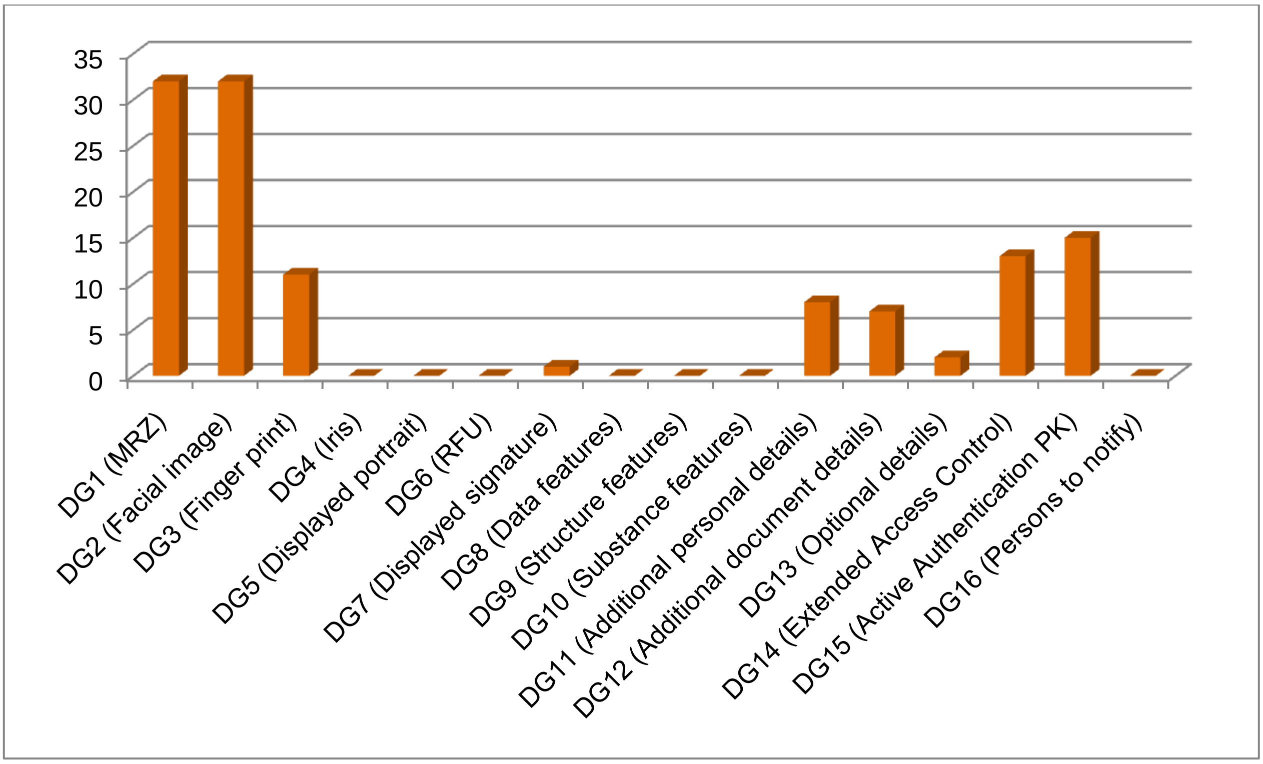


Figure 19 - Available data groups in eMRTD test population

7.3.3. Security mechanisms supported

All the analysed documents support the Passive Authentication (ICAO mandatory) and Basic Access Control (EU mandatory) mechanisms.

Nearly half of the e-MRTDs presented were second-generation e-MRTDs: 13 from the 32 documents support Extended Access Control (EAC).

Not all of the analysed documents support a mechanism that allows for verifying the authenticity of the chip. Support for the Active Authentication (AA) and Chip Authentication (CA, part of EAC) mechanisms are distributed as follows:

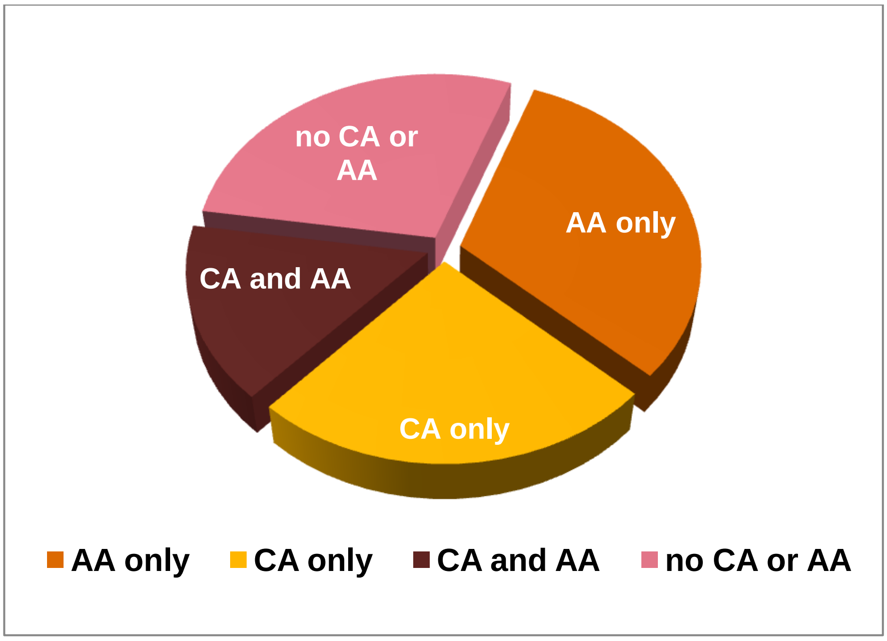


Figure 20 - Supported security mechanisms in eMRTD test population

Nine documents, representing one-third of all configurations, did not support any such mechanism.

7.3.4. Differences in biometrics

The analysis of the biometrics did show several differences.

During analysis of biometrics data groups (data group 2), we observed that only one configuration does store biometric feature points that may help verification equipment in using the biometrics for identity verification.

Through visual comparison, we observed the following:

- Certain face images were captured digitally, while other face images were scanned from printed passport photos.

- There are differences in the resolution of the stored face images.

- There are differences in the level of compression of the stored face images.

To respect the privacy of the attendees to the workshop, no examples are given regarding the differences in face biometrics quality. We have not further analysed the face images in detail.

ICAO Doc 9303 requires conformity to ISO/IEC 19794 Part 5 for the face biometric. This document discusses the relevance of the background of the face image for use in computer face recognition. It states that a typical background to enhance performance is 18% grey with a smooth surface.

Comparison of the background in the e-MRTDs read demonstrates that all face images have a more or less smooth surface. However, the percentage background grey varies significantly. The overview below shows the background colour in face images from 12 of the e-MRTDs read, as well as their greyscale equivalent, against a background of 18% grey.

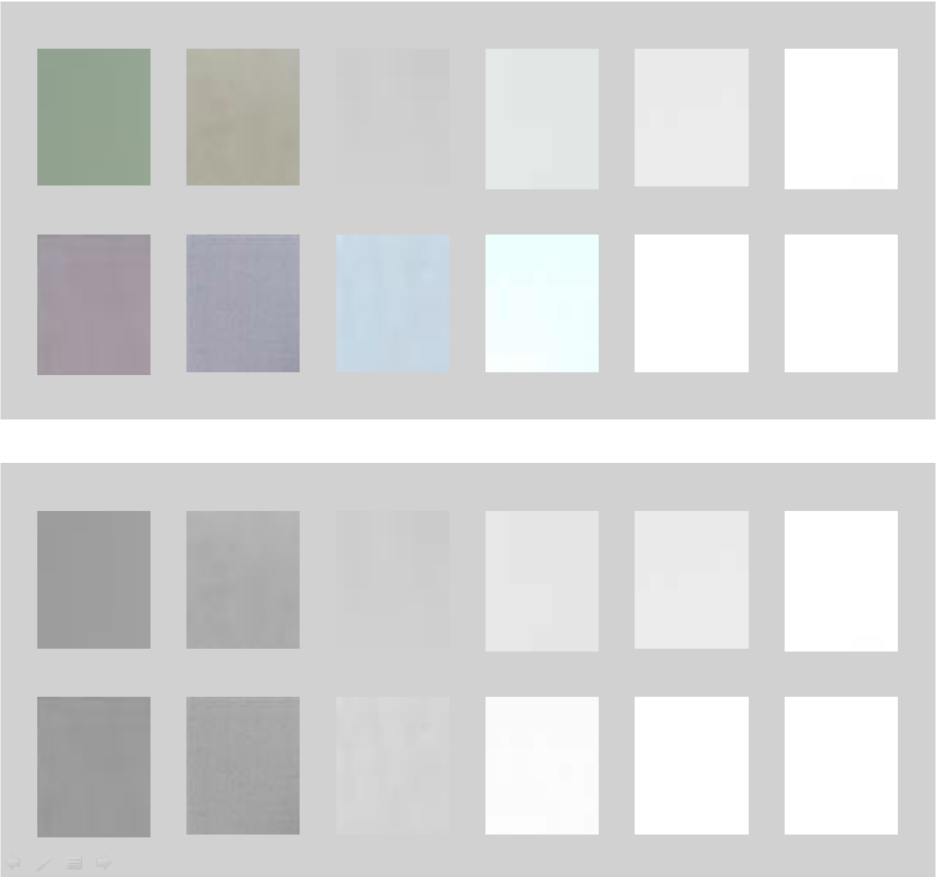


Figure 21 - Background colour (above) and greyscale (below) of 12 tested eMRTDs against an 18% greyscale background

7.3.5. Non-conformities identified

Upon further investigation of the e-MRTD data read, we identified a number of non-conformities in some data structures.

In several e-MRTDs of one configuration, the Machine Readable Zone data stored in data group 1 did not correspond to the MRZ printed on the document. In all cases, the structure of data group 1 did not conform to the requirements of ICAO Doc 9303.

In three different configurations, the Document Security object was not compliant to ICAO Doc 9303. These documents contain an incorrect object identifier to identify the ICAO LDS security object, the data structure that inspection systems must use to validate the authenticity of the e-MRTD data, using Passive Authentication.

7.4. *Conclusions*

Exploratory research was carried out in a sample of 32 European e-MRTDs, consisting of 21 e-MRTD configurations originating from 16 Member States. The results of the analysis of e-MRTDs presented for reading lead to the following conclusions.

Common denominators

All analysed European e-MRTDs have in common that they

- contain data groups 1 (MRZ data) and 2 (facial biometric) (ICAO mandatory)
- support the Passive Authentication mechanism (ICAO mandatory)
- support the Basic Access Control mechanism (EU mandatory).

Incomplete cloning detection

The European e-MRTD scheme/system does not provide full detection of cloning. Currently, one-third of the analysed e-MRTD configurations do not support any of the detection mechanisms for cloning, i.e., Active Authentication or Chip Authentication.

Note: This figure should be reduced in the future as most Member States currently issue e-MRTDs with Extended Access Control, which requires the Chip Authentication mechanism.

Biometrics in e-MRTDs not optimised for performance

The analysis of facial biometric data confirmed statements made regarding biometrics quality.

The facial biometric data in e-MRTDs are not optimised for performance, due to

- variety in background colour (0-40% against an optimum of 18%)
- quality loss due to printing and scanning of passport photographs
- variety in resolution and compression.

Non-conformities

The investigation demonstrated that there are e-MRTDs with non-conformities in the field. Inspection of these e-MRTDs will or may fail, unless a mechanism is introduced for informing receiving states about known issues.

To be expected at border control

At border control, one can expect e-MRTDs

- in a wide variety of configurations
- that support as a minimum DG1, DG2, BAC and PA
- that may not support electronic mechanisms for cloning detection
- including face biometrics with various quality levels
- with non-conformities.

8. Conclusions and recommendations

In this chapter, the conclusions for this study are represented in **bold blue**. Per conclusion, one or more recommendations are given in ***bold italic***.

These conclusions and recommendations are those of the study consortium, based on their impressions from the interviews, the questionnaire results and the discussions at the workshop. As such, they will not necessarily be shared or endorsed by all workshop participants and questionnaire respondents.

In addressing the question posed by Frontex, the consortium did not limit itself to the scope of Frontex' authority; so, in some respects, its conclusions and recommendations might stray beyond the limits of the remit of Frontex.

The reliability of the e-passport issuance process is vital for EU border control. (C1)

The study indicates a lack of harmonisation on issuance of passports among Member States. This hinders the implementation of consistent controls at border inspection to compensate for weaknesses in the issuance process and vice versa.

Because of improvement in the technical security of passports, one can expect a shift of fraudsters from counterfeiting passports to attacks on the issuance process and/or lookalike fraud. This study shows that vulnerabilities in the national e-passport issuance process might cause unauthorised border passage. This emphasises the importance of the issuance process in EU border control. Our results indicate that there is a lack of harmonisation on the issuance of passports among EU/Schengen Member States. Even though it seems generally agreed that the *ICAO guidelines on assessing the security of handling and issuance of travel documents*[18] form a good basis to secure the issuance of e-passports, multiple questionnaire respondents indicate non-compliance with these.

Some examples of possible non-compliance are:

- Issuance process is not under dual control.
- Regular audits at passport offices are not performed.
- Screening of personnel is not always employed.
- The security of the issuance process abroad is not equivalent with the security of the domestic process.
- E-passports are not always stored in safes.
- E-passports are sometimes send by regular mail.

This was confirmed in the workshop, where participants discussed many different situations of the issuance process between various Member States. As a possible cause, participants discussed that the ICAO guidelines are focused on large centralised issuance and harder to adapt to more decentralised, small-scale, issuance organisations.

> ***Further promote structural information exchange between the issuance community and the border control community on e-passport security matters (R1.1)***
>
> As the Schengen Acquis necessitates mutual trust between its Member States, especially when it comes to issuing and inspecting e-passports, it can be beneficial to the security of the external borders if structural and frequent information exchange on e-passport security

[18] Can be downloaded from http://www2.icao.int/en/MRTD/Downloads/

matters related to issuance and inspection takes place. This will help to effectively manage the security of both border control and e-passport issuance. Possible information that can be shared is known e-passport production defects (e.g. via defect lists), persons restricted for travel and border control incidents (e.g. attempts to use a forged e-passport or lookalike fraud).

As Frontex has a mandate within the border control context and not in the e-passport issuance context, Frontex will have to approach different organisations to facilitate this information exchange in cooperation with these other organisations and stimulate stakeholders and decision makers to support this information exchange.

Provide training (and possibly tools) for the verification of breeder documents by issuance officers (R1.2)

Frontex invests heavily in the training and provisioning of tools for document authentication within the border control community. The secure issuance of e-passports, however, also relies on the ability of issuance officers to verify the authenticity of a breeder document during application or delivery of an e-passport. We recommend Frontex to investigate whether its training and tools for border guards can also be deployed within the issuance community.

Compile and structure good practices from the various Member States on the issuance process (R1.3)

The ICAO Guide on Assessing the Security of Travel Document Issuance and Handling provides a number of good practices for the issuance process; however, it makes specific choices on how to secure the issuance process. These choices cannot always be implemented by all Member States. For example, the ICAO Guide does not give any guidance in case that segregation of duties is hard to implement because of capacity/manpower constraints. Currently, Member States have found various ways to deal with these challenges; it would be valuable to compile and structure these so that they can be shared among all EU/Schengen Member States.

Discuss voluntary EU/Schengen common guidelines for issuance of e-passports (R1.4)

As a follow-up on the previous recommendation to compile and structure good practices from various Member States, we recommend Frontex to discuss establishing voluntary common EU/Schengen guidelines for the issuance of e-passports at the appropriate EU forum. These would incorporate the various requirements of different EU/Schengen Member States and could form a basis to further harmonise the issuance processes.

Investigate the possibility of voluntary inter-country review of the e-passport issuance process (R1.5)

In analogy to the Schengen Standing Committee on implementation and evaluation of the Schengen Border Code, similar inspections can be performed on the issuance process of the EU/Schengen Member States. This could take the form of voluntary missions, promoting sharing of good practices or in the form of official reviews, if common guidelines are available.

Lookalike fraud with e-passports is a substantial risk for EU/Schengen border control. (C2)

Because of improvement in the technical security of passports, one can expect a shift of fraudsters from counterfeited passports to attacks on the issuance process and/or lookalike fraud. Individual comments in the questionnaire indicate that lookalike fraud is specifically relevant in the context of Automated Border Control. However, lookalike fraud can be substantially reduced by reading and checking the travellers' fingerprints against the fingerprints stored in the second-generation e-passports. Checking fingerprints at border control is currently not deployed in first line inspection. A number of Member States do not have plans to deploy fingerprint checking. This implies that in current practice, sufficient quality of the facial image is essential to prevent lookalike fraud. Approximately 40% of the questionnaire respondents indicate that better quality of the facial image stored in the chip would contribute to reduction of lookalike fraud.

> ***Investigate the benefits of border control to further improve the quality of the digital facial image (R2.1)***
>
> Although the image quality of the digital facial images is already much better when compared with the image quality of the hardcopy document, it could still be improved. We recommend Frontex to investigate the appropriate level of quality for facial images to significantly reduce lookalike fraud at border control. Another possibility is to enhance the quality of the existing facial image in line with ISO/IEC 19794 (e.g. 18% grey background).
>
> ***Investigate the future of the usage of fingerprints in border control (R2.2)***
>
> Currently, fingerprints are hardly used during border control. We recommend Frontex to investigate which obstacles Member States face with respect to fingerprints. Depending on the outcome of this investigation, we recommend Frontex to coordinate possible actions on a European scale to facilitate fingerprints' usage at border control.

The usage of e-passport functionality by Member States at border control is currently limited and not uniform. (C3)

Although all Member States are issuing e-passports since August 2006, about only half of the Member States actually read the chip in first line border control. Some of the Member States do not intend to start reading the e-passport chip. Reading second-generation e-passports' fingerprints (after EAC) is hardly deployed at this moment. Half of the questionnaire respondents indicate that the e-passport cannot be read at the passport office either.

For the Schengen area, common rules and procedures are described at high level in de Schengen Border Code.[19] The inspection process is described in ICAO Doc 9303 on a high level. The chip inspection procedure is described in ICAO Doc 9303 and in BSI TR-03110. There are no functional specifications or standards for inspection systems which can be considered a serious gap for the security and interoperability of inspection hardware and software.

> ***Provide training of border guards on the specifics on e-passport inspection (R3.1)***
>
> Further reinforce Frontex initiatives to train border guards in establishing the authenticity of e-passports, as well as provision tools to support border guards in verifying the chip.
>
> ***Investigate deployment of e-passport inspection (usage) at the border (both manual and automated border inspection) (R3.2)***

[19] See http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l14514_en.htm

The investigation could look into the obstacles Member States have in deployment of inspection systems that read the e-passport chip.

Investigate harmonisation of the e-passport inspection procedure (R3.3)

Sound and shared inspection procedures of e-passports could improve the overall security of border control of the Schengen area.

Collect real-life performance data from Automated Border Control (ABC) system pilots (R3.4)

With a few countries carrying out experiments with ABC gates, it would clearly be good to collect data on experiences with such systems to get a clear picture of the performance and accuracy of such systems and to gather experiences and suggestions for best practices in deploying and operating ABC gates.

Many Member States experience operational difficulties in deploying e-passport inspection infrastructures. (C4)

All respondents to the questionnaire indicate the Document Signer (DS) certificate required for Passive Authentication verification is available in the e-passports. When this would be formalised, it would not be necessary to provide for DS certificate exchange via the ICAO PKD or via any other means. This would make certificate exchange simpler since the (long-lived) CSCA root certificates are exchanged bilaterally.

Although already 12 Member States indicate that they have exchanged CSCA root certificates for Passive Authentication verification bilaterally, only 6 indicate they participate in the ICAO PKD. Of these Member States, only four have already made information available via the ICAO PKD and no countries seem to use the information available about other countries from the ICAO PKD in their own inspection infrastructure.

When reading the chip at border control, Passive Authentication (PA) to determine the authenticity of the data in the chip cannot always be performed since the CSCA certificates are not always available.

In many countries, the verifying PKI needed to access fingerprint data on second-generation e-passports is not yet operational. Ten countries indicate they already issue CVCA certificates, but only four have a SPOC up and running for exchanging such certificates and many have not yet implemented fingerprint verification at inspection.

With the “Collis e-MRTD Test Tool”, we have analysed the chip and chip data of 27 e-passportsfrom workshop participants. Results of our analysis of the content of e-passport chips show interoperability issues in some Member State e-passports. Some of these issues could result in rejection of legitimate e-passports, implying that they could hamper border control.

Further investigate the obstacles Member States are facing in employing or deploying the public key infrastructures supporting the e-passport inspection (R4.1)

From our study, many obstacles emerge in employing or deploying the public key infrastructures supporting the e-passport inspection, such as the cost and the inherent complicated nature of the required PKIs both in implementation as in operation. The ICAO PKD can play an importing supporting role, e.g. by providing CRLs and CSCA link certificates and possibly “defect lists”, but currently is not used to its fullest potential. We recommend further investigation of these obstacles and the potential role of PKD in overcoming these.

Investigate formalising the de facto practice of placing the document signing certificates in the e-passports (R4.2)

Although this is already the case in practice, adding this requirement would remove the need for Member States to collect all Document Signer certificates and insert them into their inspection systems, reducing the inspection systems operational hassle.

Further investigate the usage of "defect lists" in inspection systems (R4.3)

A mitigating measure for the observed interoperability issues could be the usage of a "defect list" in inspection systems, enabling these systems to recognise e-passports with known issues and interpret (technically wrong) information. As such, lists might introduce security vulnerabilities themselves; further investigation is required. Based on our preliminary results, the (central) maintenance and distribution of a "defect list" seems an important direction of further research. Keeping the list up to date and transferring it to all inspection systems might turn out to form a considerable challenge. However, if the defect decreases the security, extra thorough inspection of the document should be performed.

There is currently a proposal being discussed for defect lists in the joint ISO/IEC JTC1/SC17 Working Group 3 and Task Force 5.

Cloning of e-passport chips is a serious concern. (C5)

Not all Member States currently issue e-passports with mechanisms to verify the authenticity of the chip. Moreover, when e-passports support these mechanisms, not all Member States are currently using these mechanisms when reading the e-passport. From the sample of e-passports read during the workshop, about one-third did not support any of the detection mechanisms for cloning, i.e. Active Authentication of Chip Authentication.

Active Authentication and Chip Authentication are security mechanisms meant to prove the authenticity of the chip, i.e. to prevent cloning of the chip (data). This is especially relevant in Automated Border Control where the physical security features of the e-passport are checked less thoroughly or hardly checked at all. In ABC systems, a cloned chip could suffice to pass border control in case the chip data of a lookalike is available, certainly if the threshold for automated biometric verification is low.

Support of Active Authentication is left optional in both ICAO guidelines and the supplementary EU agreements. Chip Authentication is part of Extended Access Control and according to EU agreements it should be present in second generation e-passports of Schengen countries. When Chip Authentication is supported by the chip and verified by the inspection system, checking Active Authentication does not provide any additional security benefits, as its result is equivalent to Chip Authentication.

Stimulate the adoption of mechanisms for authenticating the chip in all EU e-passports (R5.1)

During the workshops the usage of cloned e-passports in Automated Border Control was rated as a high risk, which can be mitigated by mechanisms for authenticating the chip (e.g. Active Authentication, Chip Authentication).

National identity cards of Member States are also accepted as travel documents at the EU/Schengen border. As the security of national identity cards is not standardised they might be considered as a weak link in border control. (C6)

Many Member States indicate their national identity card is used as a travel document to cross the EU/Schengen external border. Most of these identity cards do not conform to e-passport specifications. As a result, the document security features may vary. National identity cards of some Member States may be more sensitive to fraud than those of other Member States and interoperability is not guaranteed.

Further investigate the security role of national ID cards in border control (R6.1)

National ID cards are extensively used as a replacement of the e-passport during border checks. As attackers will normally attack the weakest link in border control to illegally cross the Schengen/EU border. the effectiveness of enhancing the security of the e-passport further can be questioned as long as this issue of national ID cards is not addressed.

Not all Member States seem to be in the process of phasing out the usage of the SHA-1 secure hash function as part of signing e-passport information. (C7)

The questionnaire showed that some countries are already phasing out SHA-1 as a hash algorithm, but not all. The e-passport's security mechanisms, notably Passive Authentication, crucially rely on the security of the hash function. Especially, given the lifetime of e-passports, of 5 or 10 years, phasing out SHA-1 seems a sensible precaution and is in line with international recommendations to retire SHA-1 for the use of digital signatures.

Press for SHA-1 phase out for Passive Authentication (R7.1)

This recommendation to phase out SHA-1 is not an outcome of the risk workshop, but is based on our own assessment, given the response to the online questionnaire. Only time can tell if continued use of SHA-1 will turn out to be a significant risk in the long term, but phasing it out is a relatively cheap measure — it only requires a small, localised change in the production process, and only in the software used for personalisation, and none for the e-passport itself or for inspection systems (as e-passport inspection systems already need to support all used secure hash functions) — so it seems unwise to run this risk.

This topic could be raised with ISO/IEC JTC1/SC17/WG3/TF5.

A. Interviewees and questionnaire respondents

A.1. Interviewees

List of people who have been interviewed:

We [Frontex], have in post-processing chosen not to divulge the names of the individuals, while leaving information about organisation intact as this provides the reader with some flavour of the competencies involved in the production of the study. It does in no way imply that the results of the study are endorsed by any of the organisations mentioned in the table below:

Interviewee name	Affiliation/Role	Country
-	Issuance manager, BPR	-
-	Standardization manager, ANSI	-
-	National Frontex Point of Contact	-
-	Border Police Commissioner	-
-	Head of Issuing office	-
-	Issuing office	-
-	Department of Advice & Innovation, Expertice Centre for Identity fraud and Documents (ECID), Royal Netherlands Military Police (KMar), Ministry of Defence	-
-	Federal Office for Information Security (BSI)	-
-	European Biometrics Forum	-
-	Brussels Interoperability Group	-
-	No-Q project within the Netherlands government program for Innovation of Border Management.	-
-	Border guard officer (retired)	-

A.2. Questionnaire respondents

Out of a total of over 100 invitees, 59 people have responded to the questionnaire, of which 35 have fully completed it. In the beginning of the questionnaire, the respondents were asked whether they would prefer not to be credited in the report. 29 people did not object to be credited in this report for their participation. *However we [Frontex], have in post-processing chosen not to divulge the names of the individuals, while leaving information about country and organisation intact as this provides the reader with some flavour of the competencies involved in the production of the study. It does in no way imply that the results of the study are endorsed by any of the organisations mentioned in the table below*:

Respondent name	Function/Role (as indicated by respondent in questionnaire)	Country (as indicated by respondent in questionnaire)
-	Belgian Federal Police	Belgium
-	Oberthur Technologies	France
-	Royal Netherlands Marechaussee	The Netherlands
-	Belgian Ministry of Foreign Affairs	Belgium
-	Joint Research Centre	European Union
-	FNMT-RCM	Spain
-	Safelayer Secure Communications S.A.	Industry
-	National Document Fraud Unit	The United Kingdom
-	IPS	The United Kingdom
-	SBGS	Lithuania
-	Spanish National Police	Spain
-	State Printing Works of Securities	The Czech Republic
-	EC, DG Home C.3	Germany/European Union
-	MOD/KMAR/ECID/A&I	The Netherlands
-	Estonian Police and Border Guard Board	Estonia
-	Office of Citizenship and Migration Affairs	Latvia
-	SMIT	Estonia
-	Ministry of Justice	The Netherlands
-	Personalisation of ID documents Centre under the Ministry of the Interior	Lithuania

-	State Printing Works of Securities	The Czech Republic
-	Ministry of Internal affairs	The Netherlands
-	Research Centre	European Union
-	Finnish Border Guard	Finland
-	European Biometrics Group	European Union
-	Ministry of Security and Justice	The Netherlands
-	Swedish National Police Board	Sweden
-	Bundeskriminalamt	Germany
-	General Directorate of Passports	Romania

A further 30 people indicated a preference not to be credited in this report.

B. Acronyms/Glossary

AA - Active Authentication

BAC - Basic Access Control

CA - Chip Authentication

CSCA – Country Signing Certificate Authority

CVCA – Country Verifying Certificate Authority

DS – Document Signer

DV – Document Verifier

EAC - Extended Access Control

ICAO - International Civil Aviation Organisation

IS - Inspection System

(e-)MRP – (electronic) Machine Readable Passport

(e-)MRTD – (electronic) Machine Readable Travel Document

MRZ – Machine readable zone

OCR – Optical character recognition

PA - Passive Authentication

PKD - Public Key Directory

PP - Protection profile

SAC - Supplemental access control

SOd - Security Object directory

TA - Terminal Authentication

UID - User ID

C. References

Nr.	Document
[1.]	Council Regulation (EC) 2252/04 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.
[2.]	Commission Decision C(2006) 2909 of 28.06.2006, adopting technical specification on standards for security features and biometrics in passports and travel documents issued by Member States
[3.]	ICAO Doc 9303, Machine Readable Travel Documents - Part 1: Machine Readable Passport
[4.]	ICAO Doc 9303, Machine Readable Travel Documents - Part 3: Machine Readable Official Travel Documents
[5.]	Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, Bundesamt für Sicherheit in der Informationstechnik, 21 Feb 2008.
[6.]	ČESKÁ TECHNICKÁ NORMA, Information technology – Country Verifying Certification Authority Key Management Protocol for SPOC, ČSN 36 9791, ed. A, Prosinec 2009
[7.]	Doc 9303 Machine readable travel documents Part 1 2. Technical report, ICAO, 2006. Sixth edition.
[8.]	Supplement to doc 9303, version 6 (final). Technical report, ICAO, Sept 2007. Available from http://mrtd.icao.int/
[9.]	Advanced security mechanisms for machine readable travel documents ; Extended Access Control (EAC), Version 1.11. Technical Report TR-03110, German Federal Office for Information Security (BSI), Bonn, Germany, 2006
[10.]	Jens Bender, Marc Fischlin, and Dennis Kügler. Security analysis of the PACE key-agreement protocol. In Proceedings of the 12th International Conference on Information Security, volume 5735 of LNCS, pages 33{48, 2009.
[11.]	Jens Bender and Dennis Kügler. Introducing the PACE solution. Keesing Journal of documents and Identity, (30), 2009.
[12.]	Gaurav S. Kc and Paul A. Karger. Security and privacy issues in machine readable travel documents (MRTDs). IBM Technical Report (RC 23575), IBM T. J. Watson Research Labs, April 2005
[13.]	Dennis Kügler. Security mechanisms of the biometrically enhanced (eu) passport. Presentation at the Security in Pervasive Computing conference, Boppard, Germany, April 2005. www.spc-conf.org/2005/slides/SPC Passport.pdf
[14.]	Ari Juels, David Molnar, and David Wagner. Security issues in e-passports. In SecureComm 2005. IEEE, 2005.
[15.]	Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, and Ronny Wichers Schreur. Crossing borders: Security and privacy issues of the European e-Passport. In Proc. IWSEC 2006: Advances in Information and Computer Security, number 4266 in LNCS, pages 152{167. Springer, 2006.
[16.]	Rishab Nithyanand. A survey on the evolution of cryptographic protocols in epassports. Cryptology ePrint Archive, Report 2009/200, 2009. http://eprint.iacr.org/.
[17.]	Alan Ramos, Weina Scott, William Scott, Doug Lloyd, Katherine O'Leary, and Jim Waldo. A threat analysis of RFID passports. Communications of the ACM, 52(12):38{42, 2009}

[18.] M. Witteman. Is e-passport security effective yet? Keesing Journal of Documents & Identity, 23, 2007.

[19.] Jean Monnerat, Serge Vaudenay, and Martin Vuagnoux. About machine-readable travel documents: Privacy enhancement using (weakly) non-transferable data authentication. In International Conference on RFID Security 2007, pages 15{28, 2007}.

[20.] Serge Vaudenay. E-passport threats. IEEE Security and Privacy, 5(6):61{64, 2007}.

[21.] Wojciech Mostowski, Erik Poll, Julien Schmaltz, Jan Tretmans, and Ronny Wichers Schreur. Model-based testing of electronic passports. In M. Alpuente, B. Cook, and C. Joubert, editors, Formal Methods for Industrial Critical Systems 2009, Proceedings, volume 5825 of LNCS, pages 207{209. Springer, November 2009.

[22.] Wojciech Mostowski and Erik Poll. Electronic Passports in a Nutshell. Technical Report ICIS, Radboud University Nijmegen, 2010. To appear.

[23.] Ingo Liersch. Electronic passports { from secure specifications to secure implementations. Information Security Technical Report, (14):96{100, 2009.

[24.] Gildas Avoine, Kassem Kalach, and Jean-Jacques Quisquater. e-passport: Securing international contacts with contactless chips. In Financial Cryptography 2008, LNCS, pages 141{155. Springer, 2008.

[25.] Henning Richter, Wojciech Mostowski, and Erik Poll. Fingerprinting passports. In NLUUG Spring Conference on Security, pages 21{30, 2008.

[26.] Tom Chothia and Vitaliy Smirnov. A traceability attack against e-passports. In 14th International Conference on Financial Cryptography and Data Security 2010, LNCS. Springer, 2010. To appear.

[27.] PKI for machine readable travel documents offering ICC read-only access, version 1.1. Technical report, ICAO, Oct 2004. Available from http://www.icao.int/mrtd/download/

[28.] Evaluatierapport biometrieproef 2b or not 2b. Technical report, Ministry of the Interior and Kingdom Relations, 2005.

[29.] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[30.] ICAO Document 9303 Part 3 (MRTD), Appendix 3 to Section III: The prevention of Fraud associated with the issuance process.

[31.] US GAO report "BORDER SECURITY; Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use".

[32.] ICAO MRTD Standards & Security Features, Presentation for "ICAO / LACAC Regional Seminar Montevideo 7th & 8th July 2010" by Malcolm Cuthbertson, Found on: http://www2.icao.int/en/MRTD2/ICAOLACAC%20Regional%20Seminar/OAS%20Grenadfav2%20(2)%20Cuthbertson.pdf

[33.] ICAO PKD (online) http://www2.icao.int/en/MRTD/Pages/icaoPKD.aspx (cited: 9/9/2010)

[34.] PKD Fee Schedule 2010 (B-Fin/25), ICAO PKD Board, 24/11/2009 (online) http://www2.icao.int/en/MRTD/Downloads/PKD Documents/PKD Board Fee Schedule - 2010.pdf

[35.] Collis e-MRTD Test Tool (online) http://www.collis.nl/?category/37172/e-passport.aspx (cited 9/9/2010)

[36.] Supplement to Doc 9303, Release 8, ISO/IEC JTC1 SC17 WG3/TF1 for ICAO-NTWG, March 19, 2010

[37.] Jonathan P. Chapman. Determining the security enhancement of biometrics in e-passports, November 2009. Available at http://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/09ws/09ws-sem/biometry-ws09-chapman.pdf.

[38.] Yifei Liu, Timo Kasper, Kerstin Lemke-Rust, and Christof Paar. E-passport: Cracking Basic Access Control keys. In R. Meersman and Z. Tari et al., editors, OTM 2007, volume 4804 of LNCS, pages 1531{1547. Springer, 2007.

[39.] The Register. How to clone the copy-friendly biometric passport. Available at http://www.mrtdanalysis.org/press/English/How_to_clone_the_copy-friendly_biometric_passport.pdf.

[40.] Frontex. Best Practice Guidelines on the Design, Deployment, and Operation of Automated Border Crossing Systems, Release 1.1, March 2011.

[41.] Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code)

[42.] ETSI TS 101 456 v1.4.3, Policy requirements for certification authorities issuing qualified certificates. Available at www.etsi.org

[43.] ISO/IEC 27002:2005, Code of practice for information security management. Available at www.bsi.org.uk

[44.] ISO/IEC 27005:2008, Information Security Risk Management

[45.] NIST Special publication 800-30, Risk Management Guide for Information Technology Systems

[46.] ICAO Guide for Assessing Security of Handling and Issuance of Travel Documents, version 3,4, January 2010

[47.] ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems

[48.] NIST special publication 800-57, Recommendation for Key Management

[49.] Commission Recommendation C (2006) 5186 establishing a common “Practical Handbook for Border Guards (Schengen Handbook)” to be used by Member States’ competent authorities when carrying out the border control of persons

D. List of figures and tables

List of figures

List of tables

List of diagrams

FRONTEX

LIBERTAS SECURITAS JUSTITIA

European Agency for the Management of Operational Cooperation at the External Borders
of the Member States of the European Union

Rondo ONZ 1, 00-124 Warsaw, Poland
Telephone +48 22 544 95 00 Fax +48 22 544 95 01