

This is an HTML working draft that led to an article publication. A reference to this work should always be done using the following citation:

[Dimitrios Lekkas](#), [Dimitris Gritzalis](#), "e-Passports as a means towards the first World-Wide Public Key Infrastructure", in Proceedings: 4th European PKI Workshop (EuroPKI 2007) Mallorca, Spain, Lecture Notes in Computer Science (LNCS), Vol. 4582, Springer (2007)

This material is presented to ensure timely dissemination of research and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by all the copyright holders. In most cases, these works may not be reposted or distributed without the explicit permission of the copyright holders.

e-Passports as a means towards the first world-wide Public Key Infrastructure

Dimitrios Lekkas¹, Dimitris Gritzalis²

¹ Dept. of Product and Systems Design Engineering, University of the Aegean
Syros GR-84100, e-mail: dlek@aegean.gr

² Information Security and Critical Infrastructure Protection Research Group,
Dept. of Informatics, Athens University of Economics and Business (AUEB)
76 Patission Ave., Athens GR-10434, e-mail: dgrit@aub.gr

Abstract. Millions of citizens around the world have already acquired their new electronic passport. The e-passport is equipped with contactless communication capability, as well as with a smart card processor enabling cryptographic functionality. Countries are required to build a Public Key Infrastructure to support digital signatures, as this is considered the basic tool to prove the authenticity and integrity of the Machine Readable Travel Documents. The first large-scale worldwide PKI is currently under construction, by means of bilateral trust relationships between Countries. In this paper, we investigate the good practices, which are essential for the establishment of a global identification scheme based on e-passports, together with the security and privacy issues that may arise. We argue that an e-passport may also be exploited in other applications as a globally interoperable PKI-enabled tamperproof device. The preconditions, the benefits, and the drawbacks of using e-passports in everyday electronic activities are further analyzed and assessed.

Keywords: Security, Trust, Digital Signatures, Machine Readable Travel Documents, PKI, RFID, Smart card, Passport

Introduction

The citizens of many countries around the world obtained their new electronic passport (e-passport), within the last year or so. Most European countries have already implemented the infrastructure for the issuance of the new passports. The requirements for a new type of passport are imposed by the United States and the International Civil Aviation Organization (ICAO), demanding a higher level of security at the inspection points of the countries borders. The e-passport incorporates three state-of-the-art technologies: Radio Frequency Identification (RFID), Biometrics and Public Key Infrastructure (PKI). While RFID is used for practical reasons in the communication with the inspection systems, Biometrics and PKI are considered capable of reducing fraud and enhancing security in worldwide digital identification.

From its side, ICAO published a series of technical reports, describing the technical and procedural details on how a Machine Readable Travel Document (MRTD) must be implemented [1]. Face recognition is specified as the only mandatory globally interoperable biometric for identity verification of travelers. MRTDs including e-passports, are equipped with an Integrated Circuit Chip (ICC), where all digital data, including biometric information are stored. Among several other issues, ICAO technical reports describe the details of the communication between the e-passport and the local inspection points, the specifications for biometric data, the structure of the data stored (called the Logical Data Structure – LDS [2]), and the PKI support.

The ICAO PKI Technical Report [3] is intended to provide standards for a simple worldwide Public Key Infrastructure, which should support digital signatures applied to Machine Readable Travel Documents. These digital signatures are intended to permit authentication of basic data produced by the issuing Country and stored in the chip embedded into the e-passport. The stored signed data include the Machine Readable Zone (MRZ) of the passport plus digitized biometric measurements, as well as other personal data of the passport bearer.

Using the digital signature, the receiving Countries can verify that the stored data is authentic (i.e. generated by the issuing Country, and not been altered), just as the physically readable passport booklet is secured from unauthorized alteration or substitution by strong physical security measures. ICAO has recognized that one of the most effective ways of doing this is using Public Key Cryptography to digitally sign the data stored on the chip. Issuing Countries are requested to implement a PKI, following specific interoperable standards, and to properly manage their own keys, which are used to digitally sign the data stored in the e-passports.

Given that the US and the ICAO initially demanded from the Countries to implement the PKI within a very short period (just a few months), the ICAO Technical Report states that it does not aim at describing a full implementation of a PKI within each Country. ICAO states that PKI does not provide the sole measure for determining the authenticity of the passport and, thus, it should not be relied upon as a single determining factor. The passport still maintains its physical security characteristics, and it should be verified by check-points using conventional manual mechanisms, along with the automated check of its electronic contents. Due to this restrained approach, the ICAO report seems that it sacrifices several security characteristics of a strong PKI implementation, such as the existence of client X.509 certificates, as well as the existence of passport revocation mechanism. Moreover, perhaps due to the increased cost of passports with crypto-processor chip, the active security mechanisms, which could protect the e-passport's data against eavesdropping and cloning, are not mandatory, allowing a weak e-passport implementation.

In this paper we focus on the PKI-related issues of e-passports, proposing a series of good practices in order to implement a Country PKI, conforming to ICAO rules. We examine how the required global interoperability can be achieved by building an appropriate worldwide Trust architecture. We then specify some important security and privacy issues, which are emerged by the use of digitized personal data. As the e-passports infrastructure seems to implement the sole globally interoperable PKI of today, we investigate how we can exploit this infrastructure in different areas and applications, by using the e-passport not only as a digital identity, but even as a signature creation device, or as an Internet authentication certificate, although it was not initially designed for such purposes.

Building a Country Public Key Infrastructure

The Public Key Infrastructure for the issuance of e-passports does not issue conventional digital certificates for citizens. However, it has all the characteristics of a full-scale PKI, with only one part missing from this implementation, i.e. the management of end-entity certificates. In other words, it does not maintain a public key directory, and it does not provide a passport revocation mechanism.

As a large-scale PKI, it is necessary to examine whether the ICAO technical report covers the baseline for the implementation, as well as to provide a brief additional set of ‘Good Practices’ (as described in []). The areas where a PKI must focus is (a) the adoption of the proper trust architecture, (b) the legal status of the certification provider, (c) key and certificate management, (d) interoperability, and the technology used.

(a). In respect to the *Trust Architecture*, ICAO proposes a single autonomous hierarchy for each country. The independency of countries in citizen identification is crucial and it is, thus, respected. This hierarchy consists of two levels: The root CA, called Country Signing Certification Authority – CSCA, and one level of one or more subordinate CA, called Document Signing Certification Authorities – DSCA. The Document Signing CA signs the passport’s data, including a public key (Active Authentication key) stored in each passport, thus providing a kind of ‘identity certificate’ to the citizen. ICAO avoids providing any kind of trusted information to Countries (e.g. a directory of Root Country certificates), as it was not desired to establish a worldwide Single-Point-Of-Trust (SPOT) and not even a European Union CA. It is true that the risk taken by a unique organization to serve as a global Trust Anchor is very high and, additionally, it may not be globally acceptable for political reasons. Our view is that this approach is quite reasonable, in terms of flexibility, security, and nations’ independency.

(b). As of the *legal status* of the passport issuance service, the organization hosting this activity is always a governmental authority. The authority acts as a Certification Services Provider and it must conform to the legal framework for the provision of certification services. ICAO does not refer to any legal requirements of the issuing authority. However, it briefly describes some security requirements (e.g. the use of secure-signature-creation-devices), that partly conform to the European law for the provision of ‘qualified digital signatures’. We argue that if a recognized accreditation scheme exists at the issuing country, then the passport authority must follow the required inspection and accreditation procedure of this country.

(c). The *key and certificate management* obligations of the issuing authority are restricted only to the management of the two levels of CA. The requirements for key protection and renewal for the secure out-of-band distribution of Root certificates and for the issuance of CRL (by the root level only) are well known in PKI []. ICAO will provide a Public Key Directory (PKD) for publishing the second level certificates (the DSCA certificates) and the relevant CRL, in order to facilitate the verification procedure at the local inspection points. Today, the ICAO PKD is not yet operational. As additional good practices in key and certificate management, we may propose:

- The existence of a secondary set of a Root private key and the respective self-signed certificate, which is counter-signed by the primary CSCA (by means of a cross-certificate). This secondary set would enable a quick recovery from an eventual loss of the primary keys. A trust path to the secondary keys is already established and, therefore, there is no need to redistribute the Root certificate by offline cumbersome means.
- As the volume of the signed passport data is expected to be very high, the DSCA keys are heavily exposed to 'known cipher-text' cryptanalysis. The frequent renewal of DSCA keys and certificates (e.g. a monthly basis would be a feasible approach) is a requirement. On the other hand, the CSCA keys must be long lasting (order of decades), as long as we have no dramatic changes in IT.
- Due to the frequent renewal of DSCA certificates, the inspection points have to be aware of a large number of Document Signer certificates (e.g. $5 \times 12 = 60$ different valid DSCA certificates issued within five years) to efficiently perform the verification of the signed passport data. To facilitate the verification procedure (although it is optional for ICAO), the DSCA certificates must be included within the data structure of the passport signature, according to the proposed Cryptographic Message Syntax standard [].

(d). *Interoperability* is crucial for Machine Readable Travel Documents, since the initial purpose is their use at inspection points outside the home country. ICAO standardizes the technology used, and it enforces a common approach in the algorithms and the data structures [] used for the security functions of the e-passports. However, ICAO still leaves many optional features, in favor of countries wishing to implement a simpler infrastructure and use a cheaper chip in e-passports (e.g. without processing capabilities). For example, it is possible to avoid the implementation of Basic Access Control and Active Authentication and use a simple memory chip. Additionally, some fields in the data structures of signatures, the LDS, and the certificates are optional, in favor of chips with restricted memory capacity. These options multiply the complexity of an interoperable software package that must successfully read and validate the passports of the countries of the world, but its implementation remains feasible. In a future version of the report, the access control and the active authentication (based on asymmetric key pairs) mechanisms should become mandatory, thus increasing both security and interoperability. The second important factor of the interoperability is the establishment of trust, which is accomplished by means of bilateral cross-certifications (as explained in the next sections).

Digital Signatures as the Basic Tool for Passport Authenticity and Integrity

The verification of the authenticity of the data stored in the e-passport is based on digital signatures. The mechanism for signing and validating data is called 'Passive Authentication'. Permitted signature algorithms are RSA, DSA, and Elliptic Curves DSA (ECDSA).

The structure of the data stored in the passport's chip (the LDS – Logical Data Structure), including the digital signature, is briefly illustrated in Figure 1. Data is separated in two parts (Dedicated Files – DF): (a). the user files, which is a writable area, and (b). the LDS, providing read-only access. The LDS contains the cryptographic keys, supporting the Basic Access Control and Active Authentication mechanisms, as well as some general information about itself (EF-COM). Sixteen Data Groups, containing the holder's identification and biometric data, follow. The MRZ (including document number, name of bearer, nationality, date of birth, etc.) is stored in the 1st Data Group, the biometric facial image is stored in the 2nd Data Group, and the Active Authentication public key is stored in the 15th Data Group. The hash values of all the present Data Groups form a new structure, called LDS Security Object. This is, then, signed, according to the 'Cryptographic Message Syntax', thus producing the Document Security Object – SO_D, which is stored in the chip.

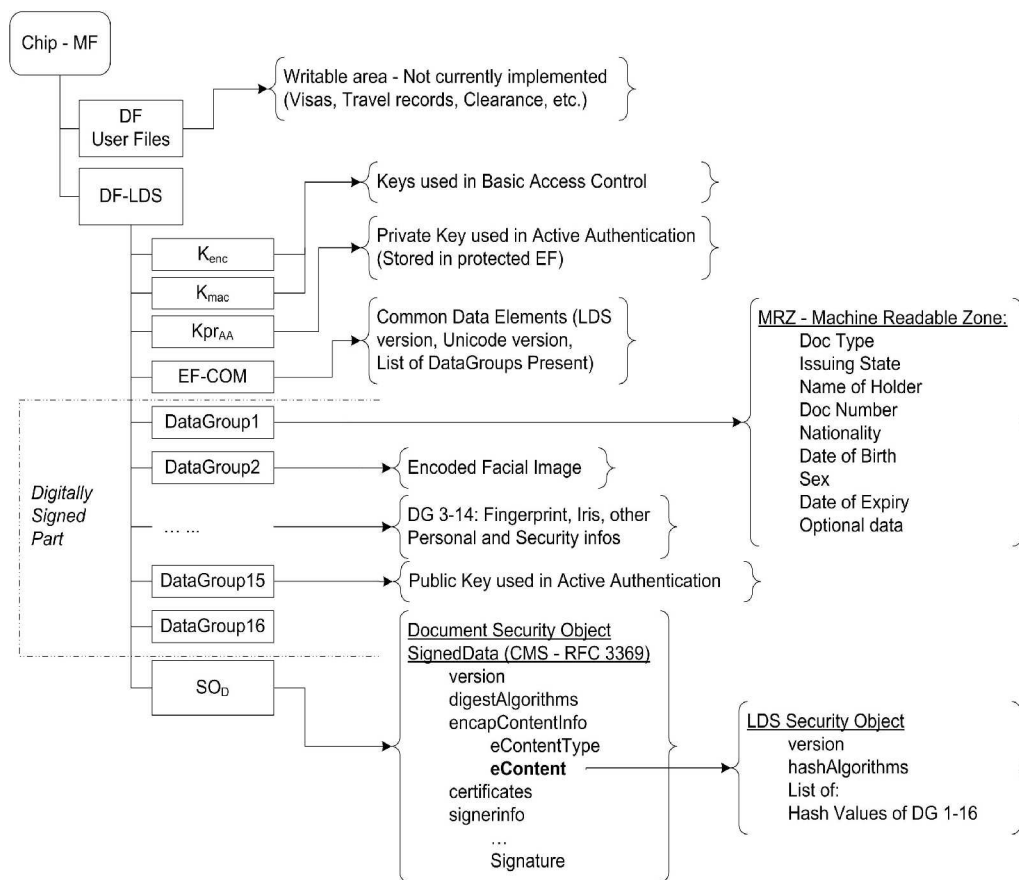


Fig. 1. Overview of data signed and stored in e-passport's chip

A valid digital signature proves that the stored data are produced by the authorized issuer and they are not altered. However, it does not prove that the container of the data (i.e. the e-passport booklet) is authentic. Therefore, the signature alone does not prevent chip cloning or substitution, unless there is a strong binding between signed data, the chip, and the booklet. The signed data must contain information that is also physically and securely printed on the booklet (binding to printed data to avoid substitution), as well as information that is uniquely bound to the chip (to avoid data cloning).

Binding to printed data is mandatory, as the MRZ of the passport is both, printed on the booklet, and included in the signed data. Binding to the chip is based on the existence of 'Active Authentication' keys, which is only optional. The Active Authentication private key is securely created and stored in the chip and it remains secret throughout the lifetime of the e-passport. The respective public key is included in signed data (LDS Data Group 15), thus providing unambiguous connection between the whole signed data set and the chip. Similarly, the serial number of the chip may be

stored in the LDS Data Group 13, thus providing secure logical and physical binding (but this also optional).

Establishing Global Trust

It is true that ICAO, or any other international organization, cannot and will not play the role of a Single-Point-Of-Trust (SPOT) for the PKI of the whole world, but it will only serve as a regulatory authority. In other words, ICAO will not build a worldwide Root CA, will not server as a Bridge CA, and will not even maintain a Certificate Trust List of countries' root CAs. Each country may build an autonomous Public Key Infrastructure, starting from a top-level Certification Authority (the CSCA). Each country has the possibility to decide about the design parameters of its infrastructure, the implementation of its security policy, and the technology used, conforming to ICAO PKI report and supporting global interoperability.

On the other hand, a global trust infrastructure [] seems necessary, in order to facilitate the validation of the digitally signed passport of any Country, at the borders of any other Country. Since a global consensus towards an organization which indicates 'who do we trust' may not be feasible in international relationships (even the United Nations could not probably gain that consensus), the most appropriate solution seems to be the establishment of bilateral trust relationships, toward a 'web-of-trust' model. A web-of-trust is built by establishing a subset of NxN trust relationships between Countries.

Technically, a trust relationship is established when a Country decides to trust the root certificate (the certificate of the CSCA) of another Country. First of all, a secure offline channel for the distribution of one country's root CA to another country must be established. This is achieved through out-of-band secure diplomatic means. Given that the whole infrastructure of a country trusts its own root certificate (i.e. the CSCA plays the role of a SPOT for this country), there are two alternative mechanisms to implement the web-of-trust, as shown in Figure 2:

- *Cross-certification*: The Country issues a cross-certificate (signed by the home CSCA) for each root CA of all the countries it trusts. The cross-certificates are then distributed to the inspection systems of the Country, where the cross-certified countries will be trusted. This kind of trust link can be reciprocal or one-way.
- *Certificate Trust List - CTL*: The Country maintains a secure structure (signed by the home CSCA) containing unique referrals to all root CA of the Countries it trusts. The CTL is then distributed to the inspection systems of the Country, where the countries contained in the CTL will be trusted.

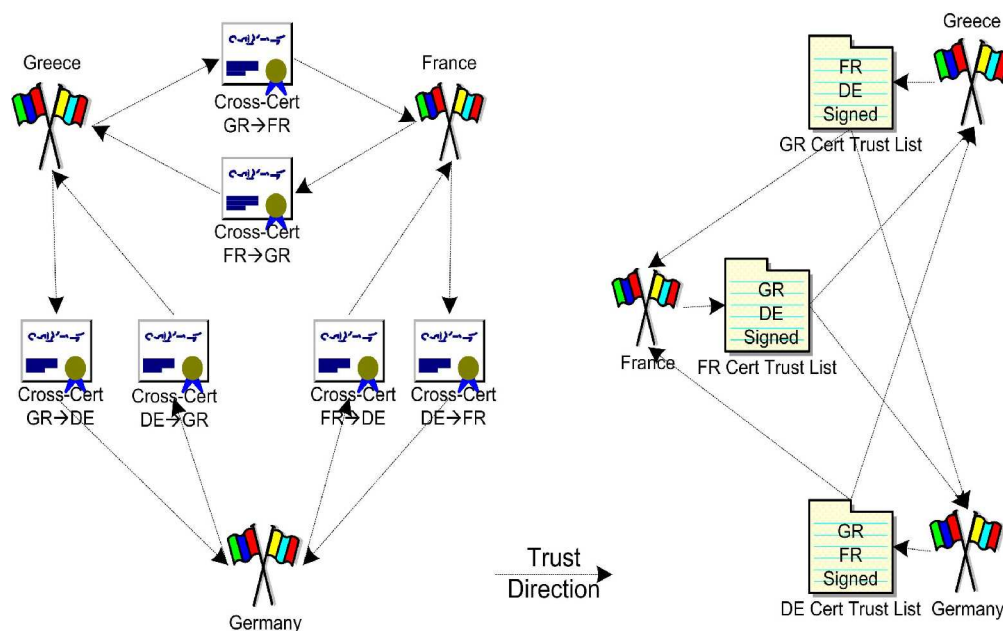


Fig.2. Alternatives for establishing global Trust: Cross-certification and Certificate Trust Lists

Although the CTL seems to be an easy and neat method to maintain the trust relationships, we consider that the cross-certification is more efficient and countries should prefer it. Three reasons support this argument:

- Only one CTL should be considered as valid at any time. However, since CTL are distributed to inspection points, there is no common mechanism to revoke a previously issued CTL and to impose the use of the newest one. This problem is intensified in case a revocation of a trust relationship occurs. The maintenance of the issued CTLs adds complexity, and it must be based on proprietary protocols. []
- CTL is not standardized in a widely accepted format, while cross-certificates are based on the X.509.v3 standard. Cross-certificates are issued and revoked by the existing infrastructure in the same way as issuing and revoking Document Signing certificates.
- Cross-certificates can be autonomously issued, communicated, and revoked for each trust relationship without affecting the other trust relationships. Revocation of cross-certificates can be communicated to the inspection points through the distribution of CSCA CRLs. These CRLs are already distributed to inspection points, informing the status of the Document Signing CA.

Security and Privacy Issues

Researchers have already exposed a number of security and privacy issues regarding the possession and the use of e-passports [, ,]. As expected, there are several potential

e-passport threats, due to two factors: (a). the *proximity (RFID) communication* of the passport with other systems, and (b). the existence of *sensitive biometric data* within its chip.

A basic security concern is the unauthorized skimming or eavesdropping of the information stored in the passport, resulting in an identity theft. This concern is further intensified due the contactless nature of the passport's chip, giving the possibility of skimming its contents without the awareness of its holder. There are reports [,] exhibiting that a passive eavesdropping (while a passport is communicating with a legitimate reader), or an active eavesdropping (the initiator of the communication is the eavesdropper), is possible from a distance of tens of meters.

RFID technology may also provide the means to track the movements of an individual, since the RFID chip transmits a unique anti-collision code during its initial handshaking (clandestine tracking). On the same line, the leakage of biometric information not only consist a violation of privacy, but it may enable forgery and movement tracking as well.

We also focus our attention on three weaknesses related to the cryptographic functionality of the e-passports: (a). the lack of management for 'Active Authentication' keys, (b). the access control on sensitive biometric data, and (c). the low entropy of 'Basic Access Control' keys.

(a). *Active Authentication key management*: Active Authentication renders the e-passport as a strong authentication token. The e-passport securely creates and hosts the private key, while the public key is a part of the signed data and, therefore, it is bound to the identity details. The authentication procedure is based on a challenge-response mechanism, where the passport proves the possession of the private key. Although the active authentication keys upgrade the e-passport to a smart authentication token, the mechanism is not fully implemented, therefore it is weak. Specifically, there is no means to revoke an AA key, in case of passport loss or compromise, although the key pair cannot change during the lifespan of the passport. Secondly, there is no publication mechanism (i.e. public key directory) for AA public keys. The latter may be not affecting the passport functionality, but it constitutes an important drawback for using the e-passport in other applications, such as e-commerce or citizen digital signatures.

(b). *Separation of access control for biometric data*: Access to the data stored in e-passports is allowed at many stages of its use and by many different systems. For example, airport staff and hotel clerks are allowed to read the biometric data stored in the e-passport, since they have physical access to the booklet. In case the e-passport is used in additional applications, such as driving license or national identification, the points able to read sensitive data are multiplied. Extended access control [] is an additional optional mechanism proposed to address this problem by restricting access to biometrics only to the bearers of a specific cryptographic key. However, the implementation of extended access control requires significant effort and introduces additional key management. We argue that the existence of biometrics (except the facial image) should be avoided, whenever possible, since: (a). it considerably increases the threats against the e-passports; (b). it reduces the value of the e-passport as a public identification token and (c). it restricts its use in other applications.

(c). *Entropy of Basic Access Control keys*: ICAO provides the specifications for implementing an optional mechanism to protect unauthorized reading (and possibly duplicate) of the contents of an e-passport. It is called 'Basic Access Control'. According to this mechanism, a secure communication channel between the reader and the passport must be established, before reading the identity contents. The secure

fast-track implementation and to avoid the complexity of managing client certificates and keys.

ICAO considers the need for CRL for end-entities as a complicating factor, and restricts the usage of CRL only to indicate a CA compromise. Furthermore, even in the unlikely event of a CA compromise, the e-passports remain valid and only a caution mechanism warns the authorities to view these documents more closely.

We consider that the timidity of ICAO to implement client certificates and to use CRLs is not justified. First of all, the e-passport itself is in fact a client digital certificate, in case it contains an Active Authentication key pair. Although the e-passport does not contain an X.509.v3 certificate and it is not designed for everyday Internet transactions, it exhibits all-but-one of the characteristics of a typical PKI-enabled smart card containing a private key and the relevant digital certificate, i.e.:

- The LDS of the e-passport binds a public key (Active Authentication key stored in DG15) to the identity details of a physical person.
- The data structure binding the keys and the identity is digitally signed by a globally trusted authority (the e-passport issuer CA)
- The private key is securely produced and stored within the RFID smart card data file system, as required by European and International laws for digital signature creation devices.
- The e-passport is personalized within a highly secure environment and the identity details are validated according to a strict procedure, conforming to the requirement for secure client registration before obtaining a digital certificate.

The only missing characteristic of digital certificates is a proper publication and revocation mechanism. We argue that the implementation of a baseline certificate management, including the issuance of CRL for e-passports, can be implemented at a considerably low effort, proportionally to the existing infrastructure. At the same time, the existence of a mechanism confirming the good status of an e-passport adds considerable value to the security and the usability of the whole infrastructure. There are several reasons supporting our argument:

- There is already an established semi-manual mechanism in several of the European Union Member States for reporting invalidated or lost passports, based on the “Schengen Convention” [1].
- Issuance of CRL by the e-passport authority is a trivial task, since the existing infrastructure for Document Signing can be used for periodically issuing and signing CRL without additional effort. CRL may include revoked e-passports by referring their serial number, similarly to the X.509 CRL.
- Distribution of CRL can be easily done through the already established Public Key Directory supporting the worldwide distribution of Document Signer certificates. Inspection points may easily periodically download CRL, which may be subsequently used for off-line passport validation. The size of CRL can be a potential problem, but it can be solved by adopting deltaCRLs (differential CRL, containing only the differences from the previous CRL).
- Existing Public Key Directories may be used for publishing client certificates at a reasonable additional effort.

Exploiting e-Passports in Other Applications

While the research community is discussing for years how we can implement a globally acceptable and trusted Public Key Infrastructure, it seems that the e-passports infrastructure - currently under construction in several countries - provides a potentially friendly environment for building the necessary global trust. This 'de-facto' implementation by Countries gives us the opportunity to investigate whether we can exploit the passport's PKI capabilities in other applications, provided that some preconditions are met.

The global e-passports implementation seems to be an attractive PKI establishment, since:

- The passport itself plays the role of a tamperproof device for the storage of private keys and certificates, as already described in the previous section.
- The passport as a digital identity is issued by governmental authorities, under very strict and reliable identification and issuance procedures for the citizens.
- The technology used throughout the world is compatible and, thus, interoperable.
- A worldwide Web-of-Trust is established through a reliable and secure exchange of countries self-signed certificates.
- It provides simultaneously digital identity capabilities and physical identification means (i.e. the printed booklet itself and the facial image)

Of course the e-passport was not initially designed for a wide use in Internet applications or in public points of interest. Some problems which restrict the public or personal use of e-passport include the cost of equipment, the impossible revocation of a lost passport, and the fact that access key to the passport's data cannot change throughout its lifespan.

In order to investigate the possibility to exploit the PKI characteristics of the e-passport in applications other than the Machine Readable Travel Documents, we distinguish three major categories:

- Applications in point-of-sales or other public points of interest (e.g. strong identification, credit card e-payments).
- Applications requiring reading/writing additional data in passport's chip (e.g. traveler's Visas and e-purses).
- Personal use in Internet transactions (web authentication, digital signatures, and encryption)

In the sequel, we describe the preconditions, under which the exploitation is possible for six prominent applications, including the travel documents. We also note the pro's and con's when using the e-passport as a digital certificate in each of these six applications.

As shown in Table 1, we examine the preconditions for using the e-passport in public points of interest, other than border control, such as the holder identification (e.g. in hotels, banks and other locations), and the e-purse in Points-of-Sales. In both cases, due to the public nature of the system hosting the applications, the access to stored biometric data must be denied. For the same reason, the system must be widely trusted to ensure that the information included in the MRZ will be not misused, as explained earlier. On the other side, when the passport is used in personal systems, the access control is not an issue, but the existence of the (non trivial for an individual) passport reading equipment is necessary.

The most important advantage of all applications is the established worldwide trust, which is based on a web-of-trust consisting of bilateral relationships between countries. This de-facto trust infrastructure is adding high value at the relevant applications and it overcomes the basic drawback of the most commercial or closed-groups PKIs. Thanks to the PKI-enabled smart-card technology used in e-passports, we have a ready-to-use device for e-purse applications, and most importantly a secure-signature-creation-device conforming to security and legal requirements for digital signatures. Furthermore, a digital signature created by the e-passport can be 'qualified' since the certification provider (passport issuing authority) applies strict citizen identification and infrastructure security procedures, conforming to the legal requirements for qualified certification services provision. Another advantage is the high mobility offered for ubiquitous authentication, since it is based on a portable device and on widely acceptable standards.

The basic disadvantage for using the e-passport in a personal computer is the considerable cost of the equipment for reading (RFID) and scanning (OCR) the e-passport. Of course, the cost of this equipment may significantly decrease in case proximity smart cards become a common need. Since the e-passport does not provide a X509 digital certificate, but a proprietary kind of certificate, its use in today's browsers is not possible, unless special add-ons are installed. The lack of a revocation mechanism (and certificate management in general) by the issuing authorities is a problem for automated Internet authentication, as well as for digitally signing, where no visual inspection of the digital ID is possible and where a fraudulent impersonation cannot be identified. The lack of directory adds some complexity to the verification of a digital signature and to the data encryption for a remote recipient, however it does not prohibit both usages.

Table 1. Using e-passports in applications other than MRTD

Application	Preconditions	Pros	Cons & Threats
<i>Use in public points of interest</i>			

Identification in public points, other than border control	Separate access control for biometric data Widely trusted hosting systems	Worldwide Trust and Standardization	Wide access to MRZ makes passport vulnerable to skimming and eavesdropping
e-purse for usage at point-of-sales	Separate access control for biometric data Widely trusted hosting systems Additional storage capacity in e-passport's chip	Worldwide Trust and Standardization Ready infrastructure for most PKI-based smart card e-purses	Writing capabilities and special access conditions add complexity
<i>Personal use</i>			
Authentication in Internet applications	Supportive Equipment on personal computer	Worldwide Trust Strong authentication High Mobility	No standard X.509 certificates No support from browsers No revocation – cannot prevent identity theft Cost of equipment
Digital Signature	Supportive Equipment and software on personal computer	Covers most legal requirements for 'qualified signatures' Worldwide Trust Can be based on well established standards and algorithms	No revocation possible – used until expiration No directory of public keys Cost of equipment
Data encryption	Supportive Equipment and software on personal computer	Worldwide Trust Can be based on well established standards and algorithms	No directory of public keys No key escrow possible, possible data loss Cost of equipment

We are now able to summarize the preconditions in order to exploit the e-passport PKI capabilities in applications other than its initial purpose:

- *Security features:* The chip has processing capabilities and it supports the Basic Access Control and the Active Authentication as described by ICAO.
- *Equipment:* Reading, validating, and using the e-passport's chip data requires a compatible RFID reader, ideally including a scanner and Optical Character Recognition capabilities for digitizing the Machine Readable Zone printed on the passport. Alternatively, the necessary information of the MRZ (specifically, the

passport's serial number, the holder's date of birth, and the expiration date) can be entered manually by a common keyboard.

- *Trusted Systems:* The MRZ information must be protected or at least be not publicly available, as it is the only information that prevents the unauthorized use of the e-passport in case it is lost. The requirement for keeping the MRZ secret is intensified by the fact that this information cannot change throughout the lifespan of the passport. Using the MRZ in a personal computer is acceptable, since the MRZ is only locally used and it is not disclosed to other parties. A precondition for using an e-passport in a public system is that this system is widely trusted (in the same way as we trust an ATM for the card PIN we enter or a secure e-commerce application where we enter our credit card details).
- *No biometrics disclosure:* The biometric data (but not the facial image) are often considered sensitive personal data; therefore they must be further protected, in order to enable additional use of the passport. We consider that the biometric data are not necessary for the additional applications other than the border control. We, therefore, set as a precondition that the sensitive biometric data must not be present, or they must be kept secret for the applications we examine.

Conclusions

The International Civil Aviation Organization provides the system developers with the technical standards for the implementation of a simple worldwide Public Key Infrastructure to support digital signatures applied to e-passports. Countries are required to build their hierarchical PKI following specific standards and good practices, in terms of security, trust architectures, key management and interoperability.

Digital signatures are the basic tool to prove passport authenticity and integrity, while additional mechanisms provide access control and authentication. The digital signature unambiguously binds together the stored digital information, the issuing authority, the printed booklet, and the chip itself. Establishing global trust is necessary to efficiently verify the digitally signed e-passports at the inspection points worldwide. Respecting the autonomy of Countries, the establishment of a web-of-trust based on bilateral trust relationships between countries seems to be a promising and appropriate approach.

The e-passport is, in fact, a tamperproof PKI-enabled device, which contains a private key and a kind of digital certificate for the bearer. Since the e-passport is personalized under strict security procedures, as well as there is a worldwide trust and interoperability, it provides an attractive PKI establishment of 'qualified certification' that could be exploited in other applications. By examining the use of e-passports in applications such as the Internet or in public Point-Of-Sales, we conclude that their exploitation is possible if some preconditions are met. The wide use of e-passports exhibit important advantages, such as the existing worldwide Trust and standardization, the high level of security, and mobility and the legal conformance for 'secure signature creation devices'. At the same time, the wide use may be restricted by some drawbacks, such as the need for special equipment, the lack of revocation mechanism, and the non-standard certificates.

Several security and privacy issues are identified, mainly originating from the fact that the e-passport is based on contactless communication and that it contains

biometric data. Actions that strengthen the security of the e-passport include the assignment of random document numbers (that increase the entropy of access control keys), the implementation of a revocation mechanism for active authentication keys, and the separation of access control on the biometric data.

E-passports seem to have the potential to be used as global digital identification devices in everyday activities. The infrastructure that supports them may be proved to be the first worldwide PKI that will bring certificates, keys, and digital signatures close to all citizens and applications.

References

1. ICAO, "Document 9303, Machine Readable Travel Documents", 6th edition (December 2005).
2. ICAO, "Machine Readable Travel Documents: Development of a Logical Data Structure – LDS", Technical Report, ver. 1.7 (May 2004).
3. ICAO, "PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Technical Report, ver. 1.1 (October 2004).
4. Gritzalis S., Katsikas S., Gritzalis D., Stamatou Y., Lekkas D., Marias Y., "PKI Services in the Public Sector of the EU Member States – Chapter 6: Good Practices". University of the Aegean, Report to the Greek Presidency of the European Union (2003).
5. Housley R., "Cryptographic Message Syntax", RFC 3369, IETF (2002).
6. Housley R., Polk W., Ford W., Solo D., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, IETF, (2002).
7. Jonsson J., Kaliski B., "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, IETF (2003).
8. Lekkas D., "Establishing and managing trust within the Public Key Infrastructure", Computer Communications, Vol. 26, No.16 (2003) pp.1815-1825.
9. Bosworth K., Tedeschi N., "Public Key Infrastructures - the Next Generation", BT Technology Journal, Vol. 19, No.3, (2001) pp.44-59.
10. Juels A., Molmar D., Wagner D., "Security and privacy issues in e-passports", in: SecureComm 2005, 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, Greece (2005).
11. Junko Yoshida, "Tests reveal e-passport security flaw", Electronic Engineering Times Vol. 1336:1 (2004).
12. Maurer U., "Intrinsic limitations of digital signatures and how to cope with them", in Proc. of the 6th Information Security Conference (ISC'03), LNCS-2851, (2003) pp.180-192.
13. Hancke G., "Practical Attacks on Proximity Identification Systems", in: Proc. of the 2006 IEEE Symposium on Security and Privacy (S&P'06), (2006) pp.328 – 333.
14. Dimitriou, T., "A Lightweight RFID Protocol to protect against Traceability and Cloning attacks", in: SecureComm 2005, 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, Greece (2005).
15. Kugler D., "Advanced security mechanisms for Machine Readable Travel Documents", Technical Report, Federal Office for Information Security (BSI), Germany (2005).
16. Convey A., Kupiszewski M., "Keeping up with Schengen : Migration and policy in the European Union", The International Migration Review, Vol. 29, No.112, (1995) pp. 939-963.