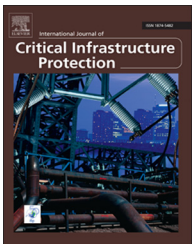
INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION 7 (2014) 233–243

Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Implementation of security and privacy in ePassports and the extended access control infrastructure

*Antonia Rana**, *Luigi Sportiello*

European Commission Joint Research Centre, Via Enrico Fermi 2749, 21027 Ispra (VA), Italy

ARTICLE INFO

Article history:
Received 9 May 2014
Accepted 5 October 2014
Available online 31 October 2014

Keywords:
Machine readable travel documents
Electronic passports
Extended access control
Single point of contact protocol

ABSTRACT

Several researchers have analyzed the security characteristics and weaknesses of electronic passports (machine readable travel documents) introduced by the International Civil Aviation Organization (ICAO) in its Document 9303. However, little, if any, work has focused on the public key infrastructures necessary to manage the certificates that underpin the security measures. This paper discusses the key aspects related to the management of keys and certificates to implement security and privacy measures for machine readable travel documents issued by European Union member states. In particular, the paper concentrates on extended access control and the associated Single Point of Contact (SPOC) protocol.

1. Introduction

Machine readable travel documents (MRTDs) [13], the official term used by International Civil Aviation Organization (ICAO) to describe travel documents that can be automatically read and processed by a computer system, were introduced in the European Union (EU) in 2004 [12]. Machine readable travel documents, also referred to as electronic passports, ePassports or biometric passports, introduce two elements to the traditional paper passport booklets: one or more biometric traits that identify the document owner and a contactless chip that stores data about the owner, including biographical data (e.g., name and date of birth) and biometric data. ICAO identifies the facial image as the mandatory main biometric trait and, optionally, fingerprints and iris image. The authenticity of a machine readable travel document is guaranteed by security measures based on public key cryptography, in particular, by passive authentication. The digital signature of the data stored in a travel document chip by the issuing country is mandatory as is, obviously, its verification by the destination country.

In addition to the authenticity verification measure, the EU has also mandated the use of basic access control (BAC) as defined in [9] and, subsequently, supplemental access control (SAC) [11] based on password authenticated connection establishment (PACE). These two security mechanisms are designed to ensure that only entities that have obtained explicit consent from the machine readable travel document owner may read the biographical data and the primary biometric trait stored in the travel document chip. Machine readable travel documents that implement passive authentication and basic access control are generally referred to as "first generation electronic passports," although this is not an official term.

The EU has also mandated the use of secondary biometrics, the technical details of which are defined in the 2009 [10] and successive amendments [11]. A security mechanism called extended access control (EAC) has been designed to work on top of basic access control and supplemental access control to ensure that only terminals authorized by the passport issuing country can access the secondary biometrics. Machine readable travel documents that implement extended access control to protect access to secondary biometric traits are referred to as

*Corresponding author.
E-mail address: antonia.rana@ec.europa.eu (A. Rana).

http://dx.doi.org/10.1016/j.ijcip.2014.10.001

"second generation electronic passports," while the documents that replace basic access control with supplemental access control are often called "third generation electronic passports."

Security mechanisms implemented in electronic passports are based on public key cryptography and, therefore, on the concept of digital certificates, which are used to manage the key exchanges required to digitally sign passports at the issuing end and to check the digital signatures at the verifying end. In fact, implementing all the security measures discussed above requires multiple public key infrastructures (PKIs). At the minimum (i.e., if only the ICAO-mandated passive authentication is implemented), a country must establish a public key infrastructure to manage the generation of passive authentication signatures. This three-level public key infrastructure has the country signing certificate authority (CSCA) as the root, one or more document signers (DSs) as intermediate nodes and the signed passports as the leaves.

This paper shows that two additional public key infrastructures are needed to implement extended access control. One is used to manage the certificates required to authenticate the terminals that access sensitive biometric information (EAC-PKI) and the other is used to manage the Transport Layer Security (TLS) protocol based secure channel between two endpoints (called single points of contact (SPOCs)), which is required to exchange EAC-PKI certificates between two countries. While it is often confused with the public key infrastructure that manages the certificates used in passive authentication, the infrastructure necessary to manage certificates for extended access control is quite different, and has specific characteristics and requirements.

Although many studies have been published on various aspects of machine readable travel document security (see, e.g., [1,17,18]), to the best of our knowledge, no study or review has dealt with issues related to public key infrastructures and certificate management in the context of the extended access control implementation, including SPOC-to-SPOC communications. This paper focuses on the key management and certification required to implement the infrastructure that supports machine readable travel documents with extended access control (EAC-MRTDs). Additionally, it discusses the challenges involved in managing the certification exchanges required to verify electronic passports.

2. Machine readable travel documents

The structure and content of the machine readable travel document chip, along with the mandatory and optional security measures, are defined in [14]. Basically, the machine readable travel document structure consists of a simple file system with directories called "dedicated files" and files called "data groups" (DGs). Mandatory data groups are DG1 and DG2. DG1 contains biographic data, which are also printed in the data page and the machine readable zone (MRZ), i.e., the set of characters at the bottom of the data page, which contains data about the owner and the document, and can be read automatically through optical means.

In the personalization process, the owner's biographic data and machine readable zone are printed on the data page, while the same data along with the biometric traits are stored in the corresponding data group in the chip protected by passive authentication and the access control mechanisms described below. The process of reading and verifying that a machine readable travel document issued by an EU member state is genuine starts by optically reading the data page and the machine readable zone data, which activates the access control protocol that, if successful, exposes the chip contents. If the machine readable travel document is a second generation passport (i.e., it also contains fingerprints), the associated more restrictive access control mechanism is also executed. Fig. 1 shows that, when checking the identity of a foreign citizen, the visited country can use the biometric data stored in the chip only if authorized to so by the country that issued the ePassport.

As mentioned above, a set of security mechanisms are implemented to guarantee that a machine readable travel document chip is genuine and also to regulate the reading of the chip contents. Inspection systems (ISs) are used to interact with machine readable travel document chips; these systems are official terminals that are entitled to read the chips. At the beginning of an interaction between an inspection system and a travel document, an access control mechanism is executed to verify that the inspection system is authorized to access the chip contents.

Two access control mechanisms exist for machine readable travel documents: basic access control (BAC) and password authenticated connection establishment (PACE) [14,16]. Both mechanisms rely on the same principle, even if they offer different security properties – the machine readable zone of the document has to be known by the inspection system that is attempting access and a string in the zone is used by the two parties as a shared secret to run a mutual authentication protocol. This mutual authentication protocol is also used to set a common secret key that is used to encrypt and authenticate subsequent communications. To make the inspection system aware of the machine readable zone, the relative string can be typed by an official or it could be optically acquired from the document data page; on the other hand, the machine readable zone information is already known to the chip because it is stored in the chip memory. If the access granted, the inspection system can read the machine readable zone information and the document holder's facial image that is stored in the chip. This mechanism is incorporated to prevent unauthorized reading of the chip (note that the document holder has to grant physical access to the document data page to allow the operation).

Table 1 shows the access control mechanisms used for data groups that contain document holder data. Note that, if the inspection system intends to access biometric data stored in a chip, it is necessary to execute the extended access control (EAC) mechanism after the initial BAC/PACE. The access control mechanism enables the inspection system to prove that it has been entitled by the issuing country of the travel document to read the stored biometric data. It also enables the inspection system to verify that the chip has not been cloned. The extended access control mechanism, which has been adopted for European ePassports [10], is described in detail in the next section.

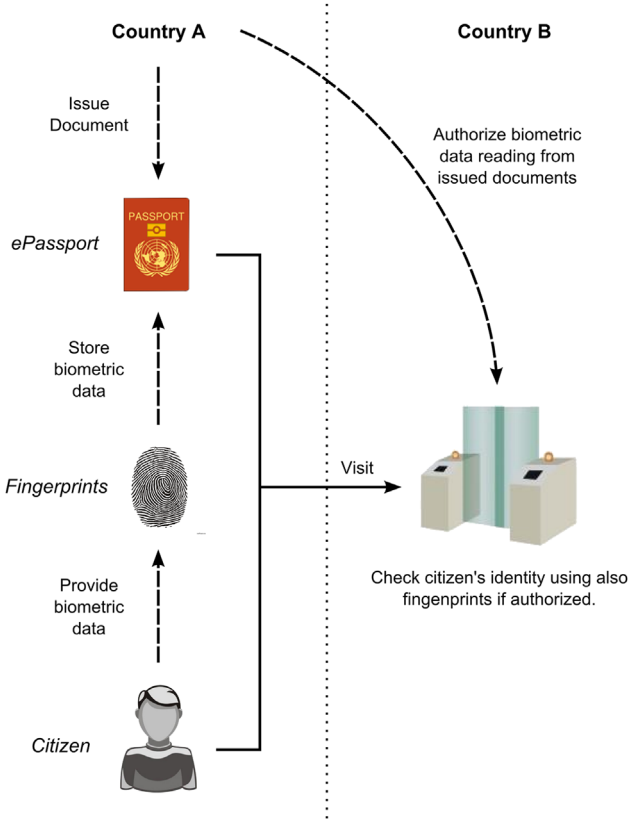


Fig. 1 – Identity and citizenship checking in a foreign country using an ePassport.

Table 1 – Access control of ePassport data groups containing document holder data.

DG	Data	Access control
DG1	Machine readable zone	BAC/PACE
DG2	Facial image	BAC/PACE
DG3	Fingerprints	BAC/PACE+EAC
DG4	Iris image	BAC/PACE+EAC

Passive authentication in introduced to guarantee that the chip contents have not been modified [14]. Essentially, each country owns a public-private key pair and uses the private key to sign the chip contents of all the machine readable travel documents that it issues. The associated public key is enclosed in a digital certificate made available to other countries, which is installed in their inspection systems. Each inspection system can verify that the chip data is genuine by checking the country signature on the certificate.

Verification of the authenticity of a travel document via passive authentication requires a directory system, or a repository, in which the root certificates (CSCA) and the document signing certificates (DS) of all the countries that issue travel documents can be stored and accessed when passive authentication based verification has to be executed. The repository must also contain certificate revocation lists that identify all the certificates that have been revoked. ICAO uses its public key directory (PKD) to provide an automated system for subscribers to download document signing certificates and certificate revocation lists. This simplifies the management of a local directory system because, in order to obtain the document signing certificates, subscribing countries only have to synchronize their local directories with the ICAO public key directory using the Lightweight Directory Access Protocol (LDAP).

wHowever, things are a bit different for CSCA certificates. ICAO does not provide the ability to download CSCA certificates directly. This is because exchanging, verifying the origin and trust of the root certificate for a country is not the responsibility of ICAO. Rather, it is recommended that this be done bilaterally via diplomatic means.

The ICAO public key directory does, however, offer the possibility to acquire CSCA certificates through master lists (MLs). The concept and the principle of use of a master list are described in [15]. A master list is essentially a list of CSCA certificates signed by a country that has obtained them in a trusted manner and guarantees their authenticity. The guarantee is based on a digital signature by the country that issues the master list. Master lists, currently produced by Germany, Switzerland and Australia, may be downloaded from the ICAO public key directory. Document signing certificates, certificate revocation lists and master lists are available from the ICAO public key directory to entities that do not subscribe to the service in the form of LDIF (Lightweight Directory Interchange Format) files. Of course, subscribing to the public key directory service and connecting to it via LDAP facilitate timely and reliable access to document signing certificates and certificate revocation lists, although there is a cost associated with this service.

3. Extended access control

This section describes the extended access control (EAC) mechanism used by an inspection system and machine readable travel document chip to authenticate each other and to manage inspection system rights. The public key infrastructure is presented, followed by the protocol that is executed by the inspection system and the machine readable travel document.

3.1. *Public key infrastructure*

The extended access control system is based on public key cryptography and digital certificates [4]. It is primarily intended to assign a certificate to each inspection system that specifies the access rights of the inspection system to biometric data stored in travel document chips with which it interacts (i.e., if the data can be read or not).

Each country that adheres to the extended access control scheme is required to set up the public key infrastructure shown in Fig. 2. The entities constituting the public key infrastructure are country verifying certification authorities (CVCAs), document verifiers (DVs) and inspection systems (ISs). Each entity has a public–private key pair along with a certificate that encloses the public key. Certificates have validity periods; certificates associated with document verifiers and inspection systems also specify their rights to biometric data.

The CVCA represents the trust point for each participating country. It is typically managed by a government entity, with the CVCA's certificate self-signed with the CVCA's private key. The CVCA signs and issues certificates for document verifiers, which specify the rights of each document verifier to the biometric data stored in travel documents issued by the corresponding country. A document verifier is an intermediate entity, introduced for organizational reasons, that manages a group of inspection systems. Each document verifier acts as a certification authority, signing and issuing a certificate for each inspection system in its jurisdiction and specifying its access rights.

As shown in Fig. 2, the CVCA can issue certificates to domestic document verifiers (located within the country) as well as to foreign document verifiers (located in other countries). This is a key aspect for authorizing the use of biometric data in travel document chips outside the issuing country. Specifically, if a document verifier intends to authorize its inspection systems to read biometric data stored in travel documents issued by another country, it has to apply for a document verifier certificate from the CVCA of that country. Thus, each document verifier would have certificates from a number of CVCAs.

A CVCA determines the rights of various domestic and foreign document verifiers according to internal policies. The document verifiers, in turn, assign their rights or a restricted set of rights (e.g., granting access to only a portion of the biometric data) to their inspection systems according to internal rules. The CVCA also determines the document verifier certificate validity, which is typically kept short to mitigate issues related to the loss or theft of inspection systems, which could be exploited by unauthorized entities to access sensitive data. The inspection system certificate validity is assigned by the issuing document verifier; it may reflect the validity period of the document verifier certificate or be a sub-interval of the validity period. Table 2 shows the certificate validity periods for various entities according to the Common Certificate Policy for EU member states [5].

Fig. 3 shows a certificate scheduling scheme for CVCAs, document verifiers and inspection systems. When a CVCA certificate is about to expire, the issuing country generates a

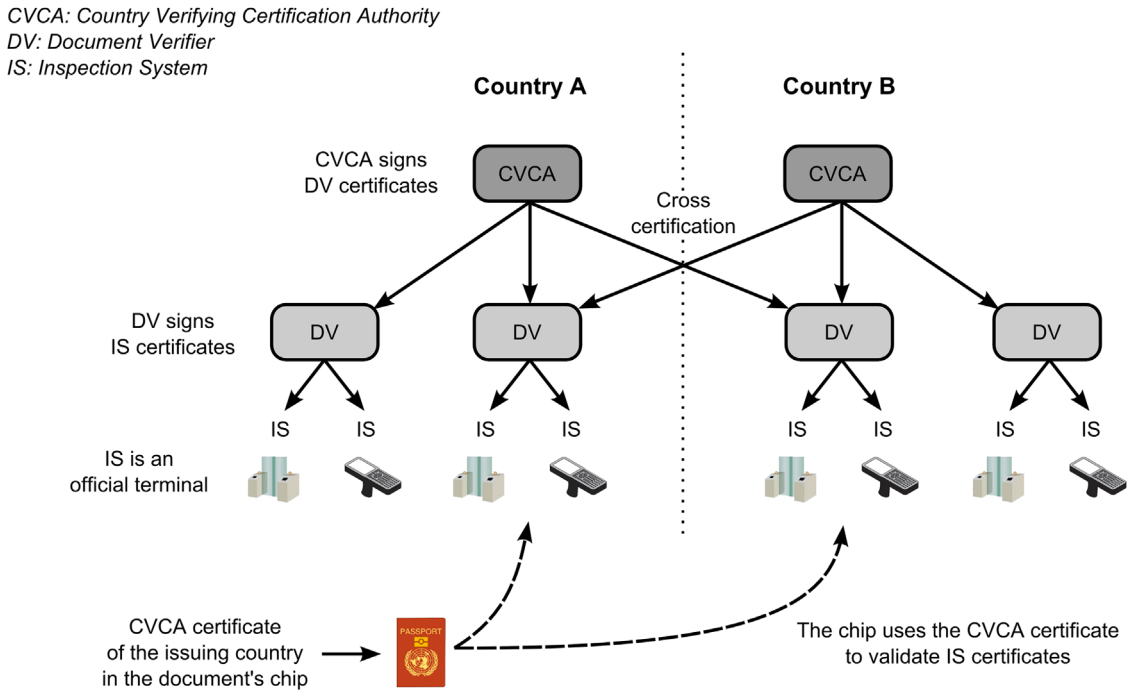


Fig. 2 – Public key infrastructure for extended access control (EAC).

new key pair and new certificate. Along with the new CVCA certificate, a link certificate is produced as well, which establishes a connection between the new and old CVCA certificates. The link certificate contains the public key of the new CVCA certificate. It has the same validity period as the new certificate and is signed with the private key of the old CVCA certificate [5]. Note that at most two valid CVCA certificates can coexist at the same time. After the new CVCA certificate and key pair are generated, they are used to issue new document verifier certificates that are, in turn, used to issue new inspection system certificates.

The card verifiable certificate (CVC) format is used for the certificates in the extended access control public key infrastructure. This format is particularly suitable when certificates have to be interpreted and used by resource-constrained devices such as machine readable travel document chips, which are basically contactless smartcards and have to perform computations on the certificates. In particular, during the extended access control (EAC) protocol, the chip has to validate the certificate received by the inspection system in order to authenticate it and check its rights.

A machine readable travel document chip stores the current valid CVCA certificate of its country (Fig. 2), which is used as the trust point by the chip. Indeed, when the document interacts with an inspection system, a certificate chain is established starting from the inspection system certificate up to the trust point of the chip – this is the concatenation of the inspection system certificate, document verifier certificate, CVCA certificate and, if appropriate, the link and other CVCA certificates up to the CVCA certificate that resides in chip memory. The trust point enables the chip to check the validity of the signatures along the entire length of the certificate chain. Note that the first inspection system, document verifier and CVCA certificates in the chain are the current valid certificates, while the remaining link and CVCA certificates, if present, are accepted by the chip even if they have expired. This mechanism guarantees that travel documents issued in the past can interact with inspection systems that have recent certificates.

Table 2 – Certificate validity periods for EU member states.

Entity	Minimum period	Maximum period
CVCA	6 months	3 years
Document verifier	2 weeks	3 months
Inspection system	1 day	1 month

At this time, a mechanism to update the trust point of a chip is foreseen, along with a solution to maintain an approximation of the current date on the chip, which would be used to check the validity period of certificates in the chain. In particular, since the initial current date reflects the date that the travel document was created, the chip would have to update it with the most recent date of the start of the validity period of a valid certificate received from a CVCA, document verifier or domestic inspection system located in the same country that issued the travel document. At the same time, when CVCA certificates still in their validity period and guaranteed by link certificates are received by a travel document, they are stored as new trust points in the chip; previous CVCA certificates that have expired are removed from the chip. Note that, at most two trust points would be stored in chip memory because no more than two CVCA certificates can be valid at the same time (see Fig. 3).

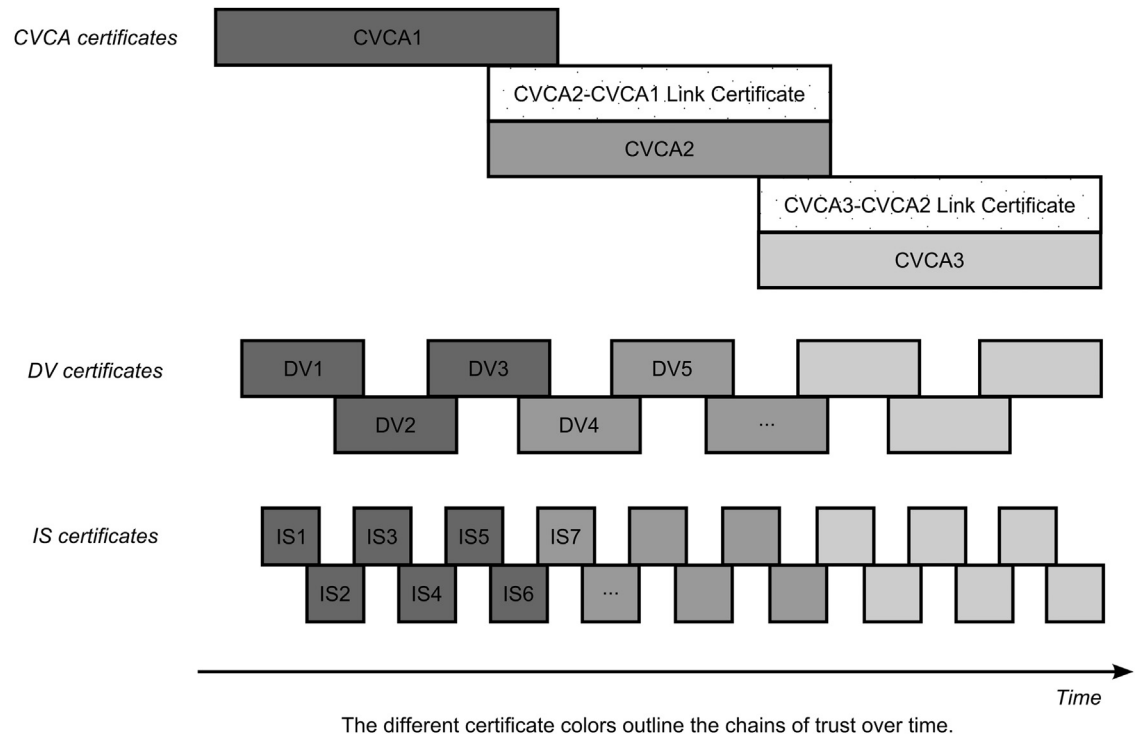


Fig. 3 – Scheduling of certificates in extended access control with relative chains of trust.

No certificate revocation lists are foreseen for the extended access control public key infrastructure because travel document chips could not access or download these lists in a simple manner. This provides additional motivation to keep the certificate validity period short as shown in Table 2 in order to mitigate the risk associated with compromised document verifiers and lost or stolen terminals.

3.2. Authentication protocols

The extended access control protocol is executed by an inspection system and a machine readable travel document in order for the inspection system to access the biometric data stored in the travel document chip. The protocol, presented in Fig. 4, is divided into two parts that are performed in succession. The first part involves chip authentication and the second involves terminal authentication [2].

Chip authentication involves the execution of the Diffie–Hellman key agreement protocol between the inspection system and the travel document; this enables the two parties to have a shared secret and for the inspection system to implicitly authenticate the travel document chip. The chip stores a static public–private key pair $PuK_{Passport}$, $PrK_{Passport}$. $PrK_{Passport}$ is inaccessible and used only internally by the chip, whereas $PuK_{Passport}$ is read by the inspection system. The inspection system generates an ephemeral key pair PuK'_{IS}, PrK'_{IS} and returns the relative public key PuK'_{IS} to the chip. This key exchange enables the inspection system and the travel document to execute the Diffie–Hellman protocol and to agree on a common secret used for encrypting and authenticating subsequent communications.

This mechanism also enables the travel document chip to be implicitly authenticated. The key $PuK_{Passport}$ is digitally signed by the country that issued the travel document; it is a part of the data involved in the passive authentication mechanism and the signature is checked by the inspection system immediately after chip authentication, thereby verifying that it is genuine. Thus, only a chip that knows the relative $PrK_{Passport}$ can run the correct Diffie–Hellman protocol and then successfully engage in encrypted communications with the inspection system. This prevents the chip cloning because, even if $PuK_{Passport}$ and the country signature are copied to another chip, the relative private key is not known.

Terminal authentication involves the execution of a challenge-response protocol that enables the chip to verify that the inspection system is authentic. As mentioned above, the inspection system is equipped with a key pair PuK_{IS}, PrK_{IS} and an inspection system certificate that encloses the relative public key, while the travel document chip has the CVCA certificate from its issuing country. The protocol begins by the inspection system sending the certificate chain starting from its inspection system certificate up to the CVCA certificate stored in the travel document chip. The travel document chip checks the validity periods of the certificates using its internal notion of current date and verifies their signatures relying on its trust point, eventually extracting PuK_{IS} from the inspection system certificate. Note that the internal current date and trust points could be updated on the basis of the received certificates. Next, a random challenge is generated and sent to the inspection system, which, in turn, returns the challenge signed with its private key PrK_{IS}. The travel document verifies the signature and, if the check is successful, grants access to the biometric data according to the rights specified in the inspection system certificate.

The protocol described above is called Chip and Terminal Authentication Version 1 and is required by EU ePassports [11]. Another version, Chip and Terminal Authentication Version 2, has been defined [3]. This version performs the chip and terminal authentications in reverse order (i.e., the inspection system is authenticated before the travel

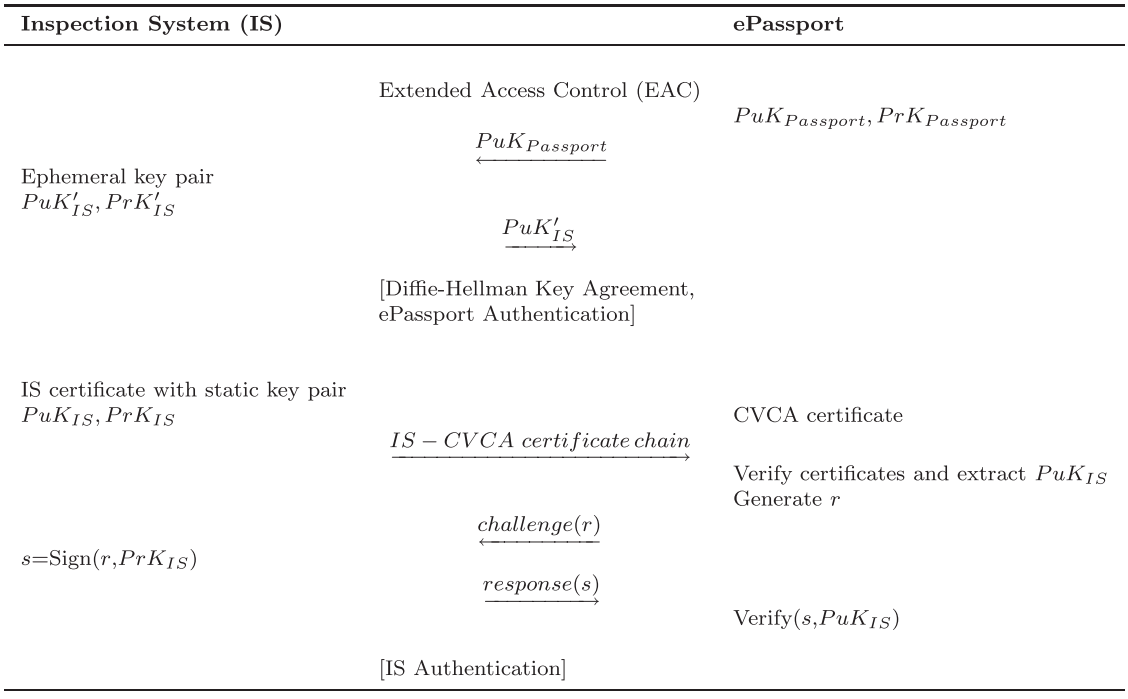


Fig. 4 – Extended access control (EAC) protocol.

document chip is authenticated). The document [3] also notes that the version may be adopted by inspection systems and machine readable travel document chips.

Note that the extended access control protocol is by no means a single cryptographic solution. Indeed, a suite of algorithms and protocols is specified (e.g., DH and ECDH for key agreement, and RSA and ECDSA for digital signatures). Interested readers are referred to [4] for more details.

4. Single point of contact

The various entities in the extended access control public key infrastructure have to communicate in order to renew their digital certificates over time (e.g., document verifiers have to periodically request new certificates from CVCAs). As discussed in the previous section, certificate validity tends to be short, so an automatic system for certificate renewal is needed. Internal communications for certificate distribution within each EU member state are left to the relevant member state authority, and no specifications are provided regarding the issuance of certificates from a CVCA to its domestic document verifiers. However, a system for certificate exchange between countries has been formally defined [7]. Its main purpose is to support periodic document verifier certificate requests directed at foreign CVCAs.

Fig. 5 presents the architecture for inter-country communications. Each country sets up a single point of contact (SPOC) system, essentially an interface between the country and other countries. All inter-country communications are conducted through their SPOCs, which are connected to the Internet. A SPOC collects certificate requests from each domestic document verifier, sends them to the SPOCs of the destination countries, which, in turn, forward the requests to their CVCAs. A certificate generated by a CVCA (or a failure notification) is returned along the same path, in reverse order, up to the document verifier that originated the request. Thus, a SPOC, on one hand, collects and forwards internal document verifier requests directed at foreign CVCAs and, on the other, collects and forwards foreign requests addressed to its domestic CVCA.

4.1. *Public key infrastructure*

Inter-country SPOC communications are offered as web services. The URL of each SPOC, and its system description and functionality are published. Communications between SPOCs are secured using the public key infrastructure shown in Fig. 6. Each SPOC has a root certificate authority that signs two SPOC certificates, a client certificate used by the SPOC to authenticate itself to foreign SPOCs and a server certificate used to authenticate the SPOC as a web service provider to other countries. Note that an intermediate certificate authority may be positioned between the root certificate authority and the SPOC client/server certificates. SPOCs rely on these certificates to establish TLS connections with other SPOCs after mutual authentication.

Table 3 presents the validity periods for SPOC public key infrastructure elements. As in the case of CVCA certificates, SPOC root certificate authority certificates are renewed and link certificates are generated as needed.

Note that a suite of algorithms and protocols is specified for SPOC communications (RSA or ECDSA may be used for authentication). Certificates are based on the X.509 format [7].

4.2. *Operational aspects*

To support activities in the architecture described above, countries must initially register using an out-of-band communications channel [5]. In particular, each country must provide registration data to the European Commission through secure diplomatic means. This includes the country SPOC root

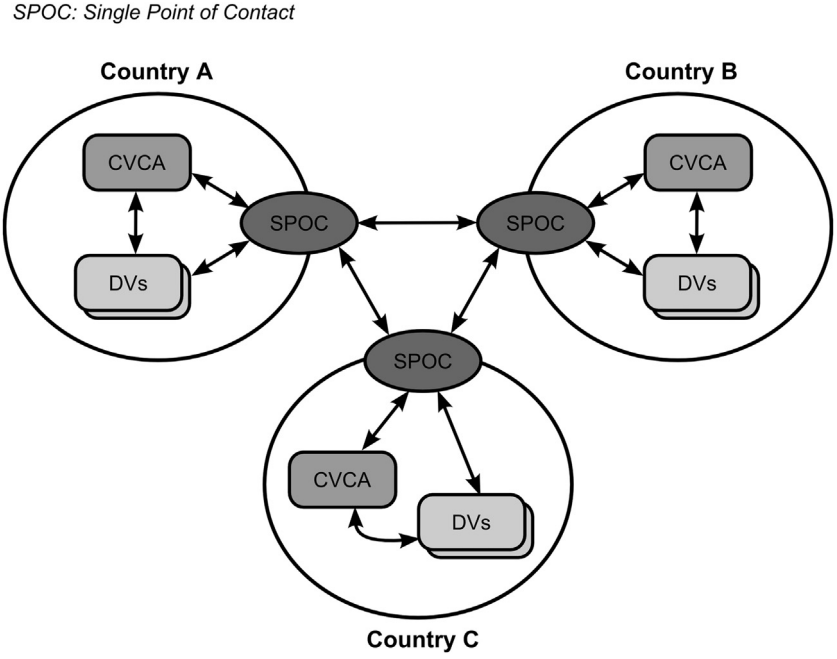


Fig. 5 – SPOC architecture for extended access control key management.

certificate authority, SPOC URL and CVCA certificate, along with other data. The European Commission makes this data available to other countries, which have to insert the registration information in their systems. The registration information may be exchanged bilaterally between countries, but the European Commission must also receive the registration information. After the initial registration has taken place, subsequent CVCA and SPOC root certificate authority certificate updates of a country, along with the associated link certificates, are distributed using the SPOC architecture; all that the recipients have to do is to check the validity of the certificates.

In the certificate request process (for inspection system requests directed at a document verifier and for document verifier requests directed at a CVCA), the applicant generates a new key pair and signs the request (which encloses the new public key) with the private key corresponding to the valid certificate. The entity receiving the request checks its validity and issues a new certificate, if appropriate. In the case of a document verifier request to a foreign CVCA, the initial certificate request of the document verifier is signed by the CVCA private key of its country, and subsequent requests directed at the same foreign CVCA are signed using the document verifier private key corresponding to the last certificate issued by the foreign entity.

The SPOC system implements four messages:

- *Request Certificate:* This message is used by a SPOC to forward a certificate request from one of its document verifiers to a foreign CVCA.
- *Send Certificate:* This message is used by a SPOC to send a certificate to a requesting SPOC.
- *Get CA Certificate:* This message is sent by a SPOC to a foreign SPOC to receive valid CVCA certificates (link and self-signed certificates) from the foreign country.
- *General Message:* This message is used to transmit SPOC–SPOC generic messages in a human-readable format.

The messages may be synchronous or asynchronous. In particular, when a RequestCertificate message is sent, the response may or may not contain the requested certificate. In the first case, the certificate is simply attached to the message response. Otherwise, the response is simply used to acknowledge message receipt, with the certificate sent later via a SendCertificate message.

5. Discussion

Implementing the infrastructure required to read the secondary biometric traits in machine readable travel documents can be a complex task. In conferences and technical meetings, some developers have expressed a general feeling that the SPOC specifications are too complex and should be improved, for instance with regard to the definition of the initial pairing between two SPOCs and in relation to error handling. Other suggestions for improvement include defining a semantics for the free-text content of general messages in order to use the SPOC protocol to securely exchange CSCA/document verifier certificates.

Some confusion about the concept, role, scope and functioning of SPOCs exists. One example is the concern that a SPOC would somehow be associated with or facilitate fingerprint exchange. This is far from the truth, as has been explained in Section 4: the SPOC protocol only provides a mechanism to securely exchange extended access control related certification requests between two countries that are mutually authorized to access the secure areas of each other's travel document chips.

It is true, however, that bilateral set-ups would complicate the process as the number of participating countries increases

Table 3 – Validity periods for SPOC public key infrastructure elements.

PKI element	Validity period
SPOC root CA certificate	Maximum 13 years
SPOC root CA private key usage	Maximum 3.5 years
SPOC client/server certificate	6–18 months

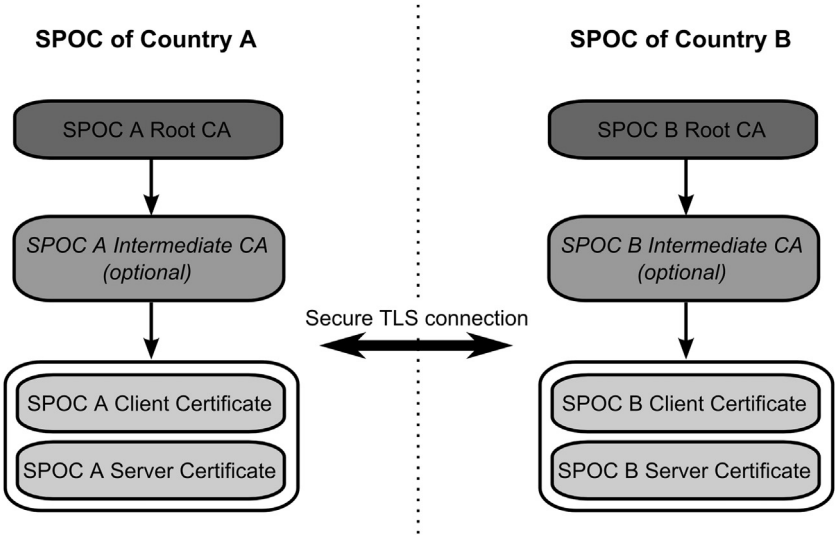


Fig. 6 – Public key infrastructure for secure SPOC communications.

and the appropriate infrastructure needs to be put in place. Special attention needs to focus on setting-up automated border crossing systems, where travelers could position their passports near optical contactless readers, face the camera to have their pictures taken to be matched with facial images stored in their passport chips, and place their fingers on fingerprint readers for fingerprint verification. These automated systems, often called "e-gates," may require online connections for the extended access control, whereas the passive authentication component (i.e., CSCA and document signature checks) could also work efficiently with offline daily updates of the databases. Similar considerations would apply to mobile devices that could be used to read travel documents; these devices would have to execute passive authentication as well as extended access control.

The challenge posed by the SPOC concept is not merely to specify a few issues in detail or to publish a technical note or guideline describing the implementation requirements or cipher parameter set-ups. Rather, as in the case of all large infrastructure projects that are of an organizational and process nature, SPOC is also affected by the organizational set-up of the implementing country. Viewed in this light, the Common Certificate Policy [5], which is mandatory for all EU member states, provides useful and important indications in addition to the mandatory requirements.

5.1. *Operational aspects*

As discussed in the earlier sections of this paper, implementing extended access control and the associated SPOCs requires setting-up a complex infrastructure, which has technical, organizational and process implications. Difficulties also arise as a result of different organizations or authorities being responsible for the infrastructure and its operation, and for the verification of travel documents. However, these aspects are obviously outside the scope of any international standard because they deal with the implementation within a country rather than the communications and exchange of information between countries. For this reason, only guidelines or technical reports could be provided about implementing the internal infrastructure necessary for extended access control and SPOC. Substantial assistance regarding the harmonization of measures – other than technical and extended access control/SPOC oriented issues – comes from the Common Certificate Policy [5], which mandates the minimum measures that must be taken at the national level to guarantee adequate, common and minimum levels of security.

In addition to drawing attention to [5], it is worth mentioning that guidelines for the local implementation of an extended access control public key infrastructure is provided by a BSI technical report [6], which specifies a SOAP-based protocol for national certificate management and a public key infrastructure. This technical report also provides guidelines on public key infrastructure related communications between terminals, travel documents and the portion of the internal infrastructure that handles certificates. These guidelines are directed at entities who wish to build inspection systems that support extended access control.

In [6], an inspection system (also called a terminal in [6]) comprises a reader (i.e., a contactless reading device that establishes a radio communications channel with the machine readable travel document chip) and software that manages the information exchange and security protocols. Several readers can be associated with a single inspection system, facilitating the management of the private keys used for extended access control at the terminal level and not at the single reader level, as well as the efficient storage of the keys in a hardware security module. This also means that the terminal, even if associated with more than one reader, has a unique identity for the responsible document verifier.

The BSI report [6] also proposes that distributed terminals be coordinated by a terminal control center (TCC) and that all readers in a terminal should have a permanent secured online connection with the terminal control center; the actual security measures in place for securing such a connection would, of course, depend on the local environment. The protocol covers the management of CSCA certificates and master lists as well as extended access control certificate management. This technical guideline, although not part of the required standards, could provide useful guidance for implementing the internal portion of the extended access control public key infrastructure.

Other considerations related to operational aspects include the need to secure Internet access to SPOCs and, in particular, protect the links between SPOCs and the CVCA. In fact, it is advisable that the SPOC–CVCA link not be automated, but instead involve by manual intervention in a highly-secure environment. Finally, other obvious measures such as high availability, regular security audits, separation of trusted roles, two-person principles, which are also required by the certificate policy, should be implemented.

5.2. *Testing and interoperability*

Interoperability, the ability of two systems to exchange information and to interpret and use the exchanged information, is a central concept in order to use machine readable travel documents efficiently. Interoperability has a variety of aspects ranging from protocols to cryptosystems. Testing interoperability is not a straightforward process. In fact, it is common to test devices and software implementations for conformity to standards and then organize test interoperability events in which different inspection systems and machine readable travel document implementations from different vendors are tested against each other.

Interoperability testing is necessary because it may happen that two implementations, while conforming to the standards and passing conformity tests, are still unable to interoperate. Issues that could affect system interoperability include ambiguous definitions of options in the standards, different interpretations of options as well as implementation flaws. Different vendors and different organizational structures with different operational processes also play a role.

ICAO has organized a series of interoperability test events for machine readable travel documents (e.g., Canberra in 2004 and Berlin in 2006); the European Union has also organized an event in Prague in 2008. These events helped identify problems, which were subsequently corrected by vendors. In particular, extended access control testing was performed at the last major interoperability event held in Prague in 2008 [8]; however, SPOC operations were not tested. Document

verifier and CVCA certificates were exchanged in advance and loaded manually into the software that executes chip authentication and terminal authentication between machine readable travel documents and inspection systems.

In addition, although test suites for machine readable travel document conformity tests are defined at the ICAO and EU levels (for first and second generation passports, respectively), no formal test suite exists for the SPOC protocol. However, as said before, conformity does not guarantee interoperability and, indeed, interoperability can be tested independently of conformity tests. Because SPOC-to-SPOC communications are managed at the bilateral level, the same can be done for interoperability testing. Testing against a reference implementation, similar to the reference inspection system implementation used in the interoperability test events, would be very useful in the context of interoperability.

wIn the absence of a test specification, an interoperability testing plan for SPOCs could be devised. Such a plan could include

- Successful registration of a foreign SPOC at both ends.
- Successful establishment of a TLS secure channel between two SPOCs using the full range of supported cryptographic algorithms and protocols.
- Successful exchange of SPOC message handling (synchronous and asynchronous request-response) for all SPOC messages (i.e., RequestCertificate, SendCertificate, GetCA-Certificate and GeneralMessage).
- Proper handling of error messages and error situations (e.g., response not received, unsuccessful decoding of the message content, unsupported features or algorithms, incorrect use of parameters, etc.).
- Successful execution of extended access control and the reading of secondary biometrics in DG3.

Such a test plan should cover the exchange of all the SPOC protocol messages and verify that the receiving end successfully processes correctly-formatted as well as incorrectly-formatted messages. The test results should document unexpected behavior and error handling in situations that are not explicitly defined in the SPOC standard.

6. Conclusions

Machine readable travel documents or ePassports were introduced in the European Union in 2004, and are rapidly being rolled out in countries around the world. Obviously, the security of ePassports and the ePassport processing infrastructure are vital issues. The ePassport processing infrastructure relies on certificate management to guarantee the authenticity, access control and privacy of machine readable travel documents issued by European Union member states. This paper is the first to provide insights into the extended access control public key infrastructure and the SPOC protocol that provide the foundation for ePassport processing in the European Union. It is hoped that the discussion of the major issues associated with the interoperability and the operational aspects of the associated infrastructure will stimulate renewed research in the area and contribute to the development of secure, reliable and efficient implementations.

REFERENCES

[1] E. Bogari, P. Zavarsky, D. Lindskog, R. Ruhl, An analysis of security weaknesses in the evolution of RFID enabled passports, in: Proceedings of the World Congress on Internet Security, 2012, pp. 158–166.

[2] Bundesamt fur Sicherheit in der Informationstechnik (BSI), Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1: eMRTDs with BAC/PACEv2 and EACv1, Ver. 2.10, Technical Guideline TR-03110-1, Bonn, Germany, 2012.

[3] Bundesamt fur Sicherheit in der Informationstechnik (BSI), Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2: Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE) and Restricted Identification (RI), Ver. 2.10, Technical Guideline TR-03110-2, Bonn, Germany, 2012.

[4] Bundesamt fur Sicherheit in der Informationstechnik (BSI), Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3: Common Specifications, Ver. 2.10, Technical Guideline TR-03110-3, Bonn, Germany, 2012.

[5] Bundesamt fur Sicherheit in der Informationstechnik (BSI), Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents Issued by EU Member States, Ver. 2.1, Technical Guideline TR-03139, Bonn, Germany, 2013.

[6] Bundesamt fur Sicherheit in der Informationstechnik (BSI), PKIs for Machine Readable Travel Documents – Protocols for the Management of Certificates and CRLs – National Protocols for ePassport Application, Ver. 1.1, Technical Guideline TR-03129-2, Bonn, Germany, 2014.

[7] Ceska Technica Norma (CSN), CSN 36 9791 ed.A: Information Technology – Country Verifying Certification Authority Key Management Protocol for SPOC, Prague, Czech Republic, 2009.

[8] ePassports EAC Conformity and Interoperability Tests, ePassports 2008, Prague, Czech Republic (www.e-passports 2008.org),2008.

[9] European Commission, Commission Decision C(2005) 409 of 28 February 2005 Establishing the Technical Specifications on the Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States, Brussels, Belgium, 2005.

[10] European Commission, Commission Decision C(2006) 2909 of 28 June 2006 Establishing the Technical Specifications on the Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States, Brussels, Belgium, 2006.

[11] European Commission, Commission Implementing Decision C(2013) 6181 of 30 September 2013 Amending Commission Decision C(2006) 2909 Final Laying Down the Technical Specifications on the Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States and Commission Decision C(2008) 8657 Laying Down a Certificate Policy as Required in the Technical Specifications on the Standards for Security Features and Biometrics in Passports and Travel Documents issued by Member States and Updating the Normative Reference Documents, Brussels, Belgium, 2013.

[12] European Council, Council Regulation (EC) No 2252/2004 of 13 December 2004 on Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States, Brussels, Belgium, 2004.

[13] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Part 1, vol. 1, Sixth Edition, Doc 9303, Montreal, Canada, 2006.

[14] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Part 1, vol. 2, Sixth Edition, Doc 9303, Montreal, Canada, 2006.

[15] International Civil Aviation Organization (ICAO), CSCA Countersigning and Master List Issuance, Ver. 1.0, Technical Report, Montreal, Canada, 2009.
[16] International Civil Aviation Organization (ICAO), Supplemental Access Control for Machine Readable Travel Documents, Ver. 1.01, Technical Report, Montreal, Canada, 2010.
[17] A. Juels, D. Molnar, D. Wagner, Security and privacy issues in e-passports, in: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005, pp. 74–88.
[18] A. Sinha, A survey of system security in contactless electronic passports, Int. J. Crit. Infrastruct. Prot. 4 (3–4) (2011) 154–164.