SafeNet Security Offering for ePassport Systems

Enhancing the security of global travel

Overview

ePassports herald a global revolution in the issuance of travel documents and identity management. Passport and identity inspection systems used by airlines and border control authorities at airports, harbors, and roadside country borders will be able to more precisely match documents to people, authenticate data in the documents, and more efficiently process travelers at checkpoints. The ePassport also offers substantial benefits to the rightful holder by providing a more sophisticated means of confirming that the passport belongs to that person and that it is authentic, without jeopardizing privacy.

More than 45 states are currently issuing ePassports, which corresponds to more than 50% of all passports being issued worldwide. This represents a great enhancement in national and international security as (1) it improves the integrity of passports by the need to match the information contained in the chip to the one printed in the document and to the physical characteristics of the holders; and (2) enables machine-assisted verification of biometric and biographic information to confirm the identity of travelers.

ePassport Requirements

As mandated by the International Civil Aviation Organization (ICAO), the controlling body of ePassport standards, by April 1, 2010, participating states will be required to solely issue machine-readable passports.

From a security perspective, the 1st generation ePassport needs to support the following two security measures as a minimum:

- Passive Authentication – The data on the chip is digitally signed by the originating country. The reader at the border control point can verify the authenticity of the data on the chip.
- Basic Access Control – This authentication measure protects the basic identification data (including facial image) and personal data from access without the holder's consent. A shared key is derived from the data in the optical MRZ to open access to the microprocessor. The communications between reader and chip is encrypted. BAC is intended to prevent skimming and eavesdropping.

An ePassport solution that supports the minimum requirements is commonly known as 1st-generation or BAC ePassport.

Issuing states have the possibility to enhance mandated security by adding secondary biometrics, such as fingerprints and iris scan to the ePassport chip data. In fact, the European Commission (EC) regulation 2252/2204 calls for the use of fingerprints as a second biometric characteristic in its second phase, and was adopted by the EC on June 28, 2006. The deadline for compliance, applicable to EU countries participating in the Schengen agreement, is set for June 28, 2009.

Secondary biometrics, such as fingerprints, represent much more sensitive personal data than the face. Therefore, access to this data must be more restricted, which is also mandated in the technical specifications underlying the EC regulation.

One way to accomplish this is to use extended access control (EAC). Today EAC is not yet an ICAO standard, but mandatory in the EU and expected to be adopted by ICAO as an international standard.

Use of EAC in the EU scheme is based on the authorization of inspection systems by e-machine readable travel documents (eMRTD) issuers, proven via the possession of digital certificates and strong authentication employing private asymmetric keys.

From a technical security perspective, EAC extends BAC and consists of the following three phases:

- Basic Access Control – Encrypted communications to prevent skimming and eavesdropping
- Chip Authentication – Authenticates the ePassport (chip) with respect to the terminal. This allows for proof that the chip is genuine, and prevents cloning.
- Terminal Authentication – Authenticates the Terminal in order to prove to the ePassport (chip) that the terminal is authorized to access the chip data. Access is granted upon successful verification of a chain of certificates, with the root certificate belonging to the ePassport issuing country. This means that the issuing country determines who can access the ePassport chip data.

Benefits of SafeNet ePassport Offering:

Protects security and integrity of passports:
- *Thwarts forgery and identity theft*
- *Thwarts illegal immigration*
- *Thwarts trans-border crime*
- *Thwarts terrorism*

Globally interoperable
- *Conforms to global standards*
- *Leads to wider global participation*

Improves Airport and airline efficiencies
- *Automates passenger clearance*
- *Reduces time and resources*

Improves Citizen's/Passenger's Travel Experience
- *Faster, automated passenger flow through border posts*
- *Reduces wait time and stress*

SafeNet®

The Opportunity

As an ePassport represents a digital identity, whose main purpose is to attain trust in a person's identity by linking the identity card to the person (e.g., via a biometric counter-check), the use of Public Key Infrastructure (PKI) technology, along with the use of Hardware Security Modules (HSMs), is the logical choice to provide the trust and security framework for ePassports, both on the issuing and verification sides.

In the digital world, cryptography is the best technology to provide data confidentiality, message authentication and integrity, plus the establishment of identity and trust. However, cryptography relies on the use of keys—and failure to protect and manage these cryptographic keys risks shattering the entire layer of security.

HSMs deliver the highest level of physical and logical protection of cryptographic keys, preventing unauthorized access to highly sensitive key information. Tamper-resistant secure casing, trusted path authentication, secure key storage, and automatic cryptographic key erasure upon tamper detection ensure the maximum level of secrecy and integrity of keys and sensitive data. Certification to international evaluation schemes, such as FIPS 140-2 and Common Criteria, provide assurance of the effectiveness of the HSM technology.

The requirement to use the highest level of security in the form of HSMs, as mandated by the various ePassport standards, opens up opportunities with the following parties who play a key role in the manufacture, issuance, use, and inspection cycle for both BAC and EAC ePassports:

- Country governments operating CSCA, CVCA and DVCA certification authorities
- Secure document printers
- PKI technology vendors
- Chip technology and smart card vendors
- Chip personalization hardware vendors
- ePassport reader manufacturers
- Providers of inspection system and border control solutions
- Systems integrators and security consultants

SafeNet HSMs for ePassport Systems

SafeNet's HSMs provide security for the following components of an ePassport system:

- Country Signing Certification Authority (CSCA) & Country Verifying Certificate Authority (CVCA): An HSM provides CA key protection and secure issuance of Document Signer (DS) and Document Verifier (DV) certificates.
- Document Signer (DS): An HSM provides key protection and secure, high-performance signing of BAC Document Security Objects (DSOs).
- Document Verifier (DV) sub-CA: An HSM provides sub-CA key protection and secure issuance of Inspection System (IS) certificates.
- ePassport Chip Personalization: An HSM ensures the secure loading of passport holder information, including biometrics, as well as issuing information, to the MRTD chip during the chip personalization process, using a unique, direct cryptographic channel between HSM and chip (secure messaging).
- ePassport Inspection System (IS)/Border Control System: An HSM provides key protection for private keys of Inspection Stations/Inspection Servers, and performs the cryptographic operations on the terminal side for terminal authentication and chip authentication. Additionally, an HSM may securely store CSCA, CVCA, DS, and DV certificates, and SSL private keys/certificates for communications with PKI infrastructure.

The following diagrams illustrate the role of SafeNet HSMs as security components in an ePassport system, in both a BAC and EAC architecture.

SafeNet – Where Added Value Lies

- Best and most widely deployed PKI and card issuance/personalization HSMs in the market
- Broadest HSM product portfolio
- Choice of form factors, performance options, and price points
- Widest choice of cryptographic algorithms and APIs, coupled with unsurpassed flexibility

Industry Leadership in Hardware-based Cryptographic Security

SafeNet's HSMs are purpose-built hardware appliances that protect the digital signing key and/or symmetric keys, and deliver comprehensive and high-speed, hardware-based cryptographic functionality for a myriad of digital identity applications.

Technical Specifications

SafeNet HSMs:

- *Luna CA4 (BAC and standard ECC support)*
- *Luna SA (full BAC/EAC and extended ECC support)*
- *Luna PCI (full BAC/EAC and extended ECC support)*
- *ProtectServer Gold (full BAC/EAC and extended ECC support)*
- *ProtectServer External ((full BAC/EAC and extended ECC support)*

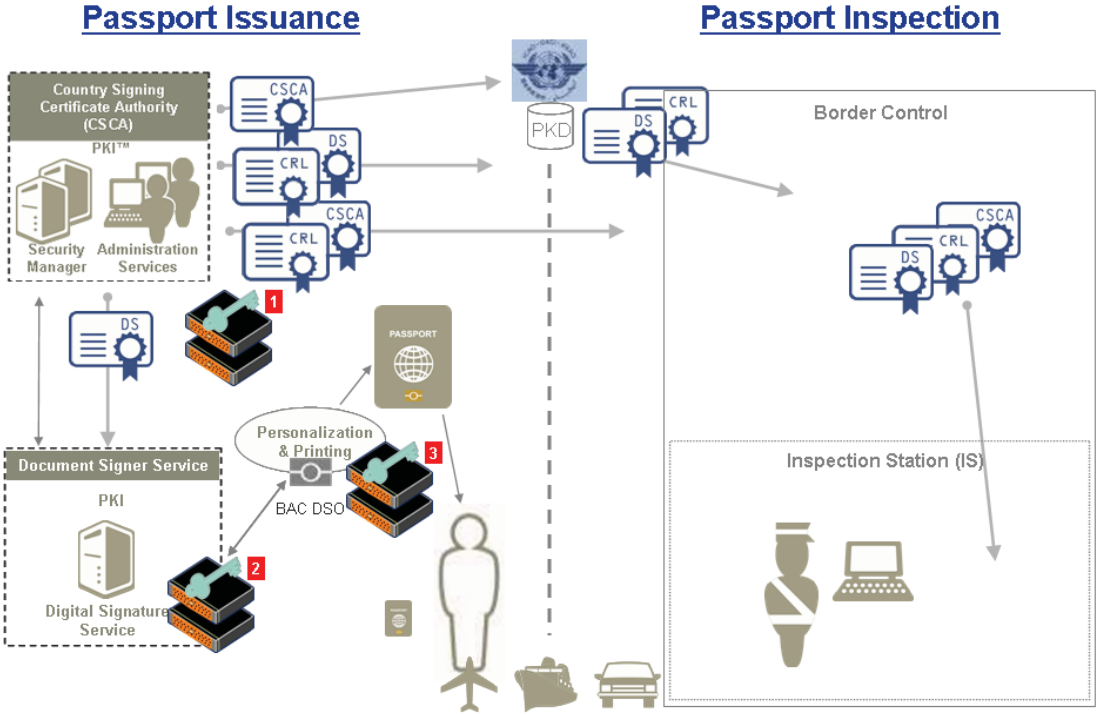
Cryptographic Support for ePassport:

- *RSA: RSA PSS, RSA PKCS_1.5, up to 4096 bit*
- *DSA, 1024 bit*
- *DH, up to 4096 bit*
- *ECDSA (X9.63, Brainpool), 190 – 521 bits*
- *ECDH (X9.62, Brainpool), 190 – 521 bits*
- *ECDSA and ECDH: additional support for user-defined Curve Domain Parameters*
- *ECDH1 Key Agreement and Key Derivation Functions (ICAO, 3DES KDF and many more)*
- *SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*
- *3DES*

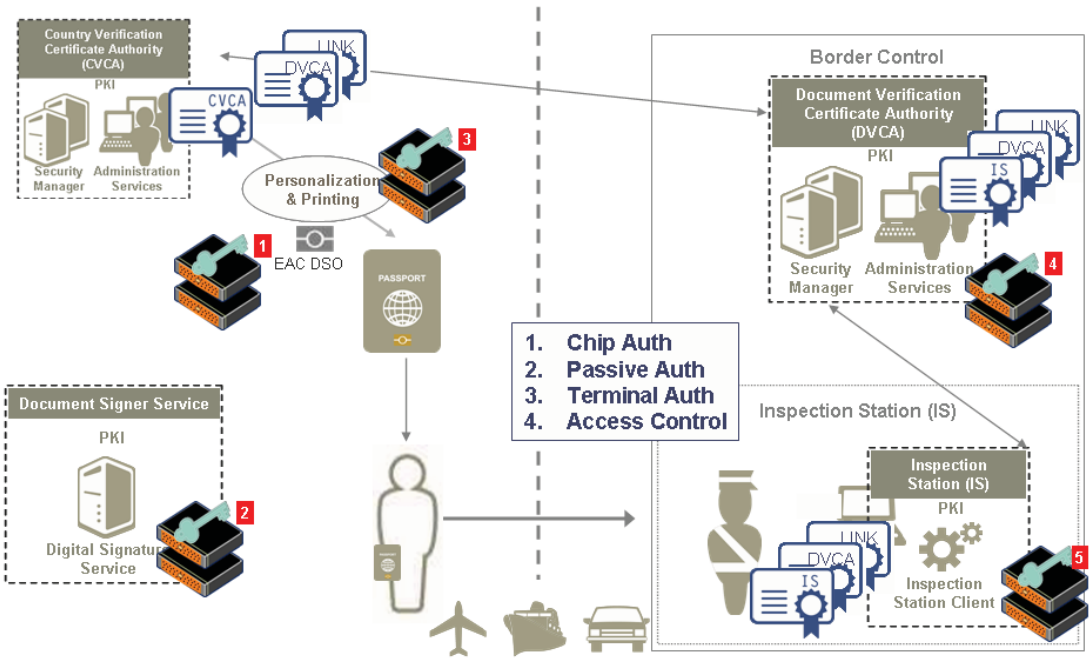
Certifications:

- *FIPS 140-2 level 3 (all SafeNet HSMs)*
- *CC EAL4+ (Luna PCI in Luna SA configuration – in process)*

Basic Access Control (BAC) ***PKI Trust Model***



Extended Access Control (EAC) ***PKI Trust Model***



SafeNet's HSM products feature true hardware key management to maintain the integrity of encryption keys. Sensitive keys are created, stored, and used exclusively within the secure confines of the HSM to prevent compromise.

SafeNet's HSM-based ePassport offering:

- Prevents compromise of stored information
- Authorizes access to protected document information
- Maintains citizens' trust

By implementing SafeNet HSMs for key protection and secure cryptographic processing, customers can begin with BAC and layer in new capabilities for EAC. The PKI and security capabilities of EAC as initially devised for ePassport deployment are perfectly suitable and can also be leveraged for other citizen identity documents, such as national ID cards, travel visas, electronic driver's licenses, and other security documents.

Proven Solutions for ePassports

SafeNet HSMs set the standard for CA key protection and hardware-based cryptographic processing, and protect some of the largest PKI installations in the world, including support of ePassport initiatives in more than 14 countries.

SafeNet would be pleased to share its knowledge and experience related to ePassport and citizen identification. Expertise in information security has been a hallmark of SafeNet since we began developing best-of-breed solutions more than 25 years ago, and we are proud of the solutions we provide to government customers across the world. To learn more, please contact us at: +44 (0) 1276 608004

SafeNet
The Foundation of Information Security

www.safenet-inc.com

Corporate Headquarters:
4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel.: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524,
Email: info@safenet-inc.com

EMEA Headquarters:
Tel.: + 44 (0) 1276 608 000, Email: info.emea@safenet-inc.com

APAC Headquarters:
Tel: +852 3157 7111, Email: info.apac@safenet-inc.com

For all office locations and contact information, please visit
www.safenet-inc.com/company/contact.asp

SB-ePassport-08.25.08