

E-passport

Hardware Security Modules Deployed to Ensure Data Authenticity and Integrity for electronic passport projects



Overview

In the wake of terrorist acts occurring around the globe, it has become imperative for countries to increase the level of security at their borders. To assist in their efforts for stronger border security, countries worldwide have implemented an e-passport program.

The e-passport has a smart card chip embedded in the passport's back cover that contains a digital image of the traveler's face, their name, date and place of birth, gender, passport number, and dates of passport issuance and expiration. Since different passports are used daily worldwide, it is critical to have a standard system in place for the e-passport design and reader technology. For this reason, the International Civil Aviation Organization (ICAO), created a set of worldwide e-passport technical specifications to assist in the implementation process to ensure all e-passports work with other countries readers. Further, the e-passport holding biometric information is recognized as the new standard for Machine Readable Travel Documents (MRTD). The systems standardization has aided in the cooperation levels of countries that were once hesitant about how the e-passport implementation would affect international travel.

However, security and data protection continues to be an issue surrounding the e-passport implementation. Although e-passports have a built in anti-skimming device in the cover and smart card chips that cannot be read further

than ten centimeters away, the need for further data protection is essential.

Solution

To ensure data authenticity and integrity, the information in the chip has to be digitally signed by the respective issuing authority. When the electronic passport holder reaches a customs entry desk, the customs officer verifies the personal information and biometric identifier stored in the chip.

The trust of the digital signature is bound to the security of the corresponding digital signing key. Countries around the world are turning to SafeNet's HSM family of products as the solution for secure key generation and storage, cryptographic signing, encryption, and to encode the passport holder personal data to the smart card chip.

SafeNet's HSMs are purpose-built hardware appliances that protect the digital signing key, and deliver comprehensive and high-speed hardware-based cryptographic functionality for a myriad of digital identity applications. 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 hardware security module to prevent compromise. SafeNet's HSMs provide advanced features like direct hardware-

to-hardware backup, split user role administration, multi-person authentication, and trusted path authentication coupled with proven security and operational deployment

Today, SafeNet HSMs set the standard for CA key protection and are employed to protect some of the largest PKI installation in the world. SafeNet HSM's are FIPS 140 and Common Criteria certified, assuring the highest level of security available in the market today.

SafeNet HSM's are currently deployed in 14 countries around the world to support different e-passport initiatives. The strength of the product offering, combined with an established and large global presence are key factors resulting in the use of SafeNet technology upon which to base the trust and security of this scheme.

Products

The Luna SA and Luna SP are flexible, network-attached hardware security modules featuring powerful cryptographic processing and hardware key management for applications where security and performance are a priority.

Luna® CA³ Root Key Management System is a dedicated Hardware Security Module (HSM) designed to provide the highest levels of performance and protection for the cryptographic keys at the heart of today's PKI systems.

Protect Server Gold is a tamper-protected PCI Hardware Security Module that provides rich, high-performance secure cryptographic

processing in server systems, and allows for the highest degree of flexibility through its built-in capability to load and execute custom code inside the secure confines of the HSM.

For More Information

SafeNet (SFNT:Nasdaq) is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property and digital identities, and offers a full spectrum of products including hardware, software, and chips. ARM, Bank of America, Cisco Systems, the Departments of Defense, and Homeland Security, Microsoft, Samsung, Texas Instruments, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. For more information, visit www.safenet-inc.com.

Corporate Headquarters:

4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: +1 410.931.7500 or 800.533.3958
email: info@safenet-inc.com

Phone USA and Canada (800) 533-3958
Phone Other Countries (410) 931-7500
Fax (410) 931-7524
E-mail info@safenet-inc.com
Website www.safenet-inc.com

©2004 SafeNet, Inc. This document contains information that is proprietary to SafeNet, Inc. No part of this document may be reproduced in any form without prior written approval by SafeNet. SafeNet shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretation thereof. The opinions expressed herein are subject to change without notice.

