Security Biometric Clearing Network

SafeNet Security Hardware and Consulting Services for the Registered Traveler System

Security Biometric Clearing Network (SBCN) needed to secure their Root Certification Authority and Central Information Management System for the Transportation Security Administration's (TSA) Registered Traveler program. The program allows for certain government-identified low-risk passengers to voluntarily have their identities checked using biometric technology and the government threat database. Approved passengers, once identified, can take advantage of an expedited screening process at participating airports.

Business Challenge

SBCN required the highest level of security available to protect America's transportation system, as well as the identities of travelers participating in the Registered Traveler program. In order to protect SBNC's Central Information Management System (CIMS) and Root Certification Authority (CA), SafeNet was asked to provide a key management and cryptographic acceleration solution that would meet the strictest security standards and have the following features:

- **Government certifications** – provide the highest government security certifications including FIPS 140-2, Level 3, FIPS 201, and Common Criteria EAL4
- **Scalable performance** - deployment in a cluster configuration to provide failover capabilities for high-availability and scalable performance without having to modify the application
- **Role-based access control and role** separation - designed to make enforcement of role-based access control and multi-party consent easy and logical through two-factor authentication and multi-level access control
- **Protect the chain of custody** - maintain the confidentiality, integrity and non-repudiation of sensitive cryptographic keys
- **Ease of use** - seamlessly integrate with Microsoft Certificate Services and provide Java, C, and CAPI API's for custom application development
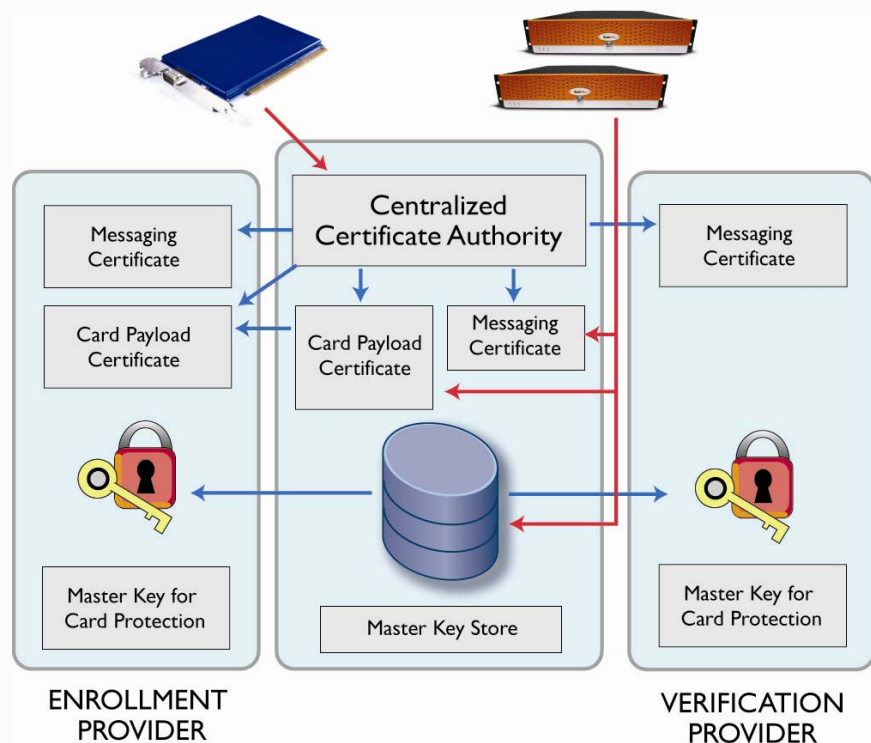
Solution

In order to provide the most robust security solution for SBCN, a combination of SafeNet hardware devices and Security Consulting Services were selected:

- A dedicated SafeNet Luna HSM to secure the highly sensitive CA.
- Two SafeNet Luna SAs were chosen to secure other critical cryptographic keys, including the Subordinate Certificate Authorities, XML, SSL encryption keys, and other application-specific keys.

The network-attached HSMs were configured in a cluster to provide high-availability to meet defined service level agreements and performance requirements. This architecture provides scalability for future performance needs as the system grows.

Complete HSM-based data security solution

- Luna SA HSM for root key protection and the ability to aggregate multiple HSM requirements in a network-shareable deployment scenario

- Luna CA3 HSM for root key protection and digital certificate issuance at the root certificate and registration authority

- Luna PCI HSM for smart card and digital ID key generation used for certificate issuance

- Luna SA HSM

Security Architecture of the Registered Traveler Program

Securing the Root Certification Authority- The SBCN CIMS architecture uses PKI certificates for authentication, digital signatures, non-repudiation, and data encryption. SafeNet HSMs and Security Consulting Services helped SBCN deploy a multi-tiered Certification Authority with Microsoft Certificate Services in less time than it would have taken to outsource it, and at a lower cost, all while meeting the strict security requirements imposed by the TSA.

Securing Sensitive Data- The CIMS architecture requires the use of SSL for securing data in motion. Both the initiator and the responder must verify each others identity when establishing this connection. Certificates are issued to each Service Provider for this purpose and are presented whenever attempting to establish a secure connection. SafeNet HSMs are used by CIMS to issue and store these SSL certificates securely in hardware. The CIMS security architecture requires that all sensitive data that is exchanged between system components be encrypted to prevent leakage of sensitive personal information. SafeNet HSMs are used by CIMS to issue and store XML encryption certificates, and to encrypt and decrypt the XML data fields.

Securing Cryptographic Keys- Government regulations for cryptographic key management require that cryptographic modules be certified under NIST's validation program, FIPS 140-2. NIST has certified SafeNet HSMs to FIPS 140-2, Level 3, which is approved for use in any federal key management system.

Issuing Digital Identities- SafeNet HSMs are used in the process of issuing digital identities in the SBCN RT system by accelerating the signing of biometric data for RT participant card issuance

CASE STUDY

SafeNet Security Consulting Services were retained to provide best practices, knowledge transfer, and documentation for the key management and cryptographic acceleration system.

- Key management and architecture deployment
- Staff training and knowledge
- Planning, installation, and configuration on SafeNet hardware
- Participation n he audited key generation ceremony
- General system review and planning
- Environment specific documentation including:
- Quick Start Guide
- Operations Guide (including disaster recovery procedures)

Conclusion

SafeNet helped SBCN meet their operations strict security requirements, and allowed the CIMS systems to become operational by the target date. Time from validation to deployment was decreased by providing expert knowledge to developers throughout the development process. SafeNet's Security Consulting Services helped to reduce future maintenance and administrative costs by documenting precise procedures for on-going system maintenance and disaster recovery. The scalable design of the solution will allow SBCN to easily upgrade capacity as demand increases without interrupting service.

About SafeNet

SafeNet is a global leader in information security. Founded 25 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. UBS, Nokia, Fujitsu, Hitachi, Bank of America, Adobe, Cisco Systems, Microsoft, Samsung, Texas Instruments, the U.S. Departments of Defense and Homeland Security, the U.S. Treasury and scores of other customers entrust their security needs to SafeNet. In 2007, SafeNet was taken private by Vector Capital. For more information, visit www.safenet-inc.com/HSM