thalestct.com

THALES

Enhancing Security and Trust in Your Public Key Infrastructure

PrimeKey

The Challenge

Built on open standards and an open source platform, PrimeKey EJBCA Enterprise brings the maturity and transparency required for any security-focused Public Key Infrastructure (PKI) solution. Proven in high security government applications, EJBCA provides a multipurpose PKI solution that is highly scalable and enables management of several parallel PKI hierarchies within the same deployment.

All security environments have different demands, different requirements for structure, and will need to adhere to different sets of organizational policies. For this reason, EJBCA enables flexible integration with most third party and PKI dependent systems, and will fit in to any PKI environment, regardless of the level of customization. Managed through a web-based graphical user interface, EJBCA's easy operation will simplify all aspects of PKI management.

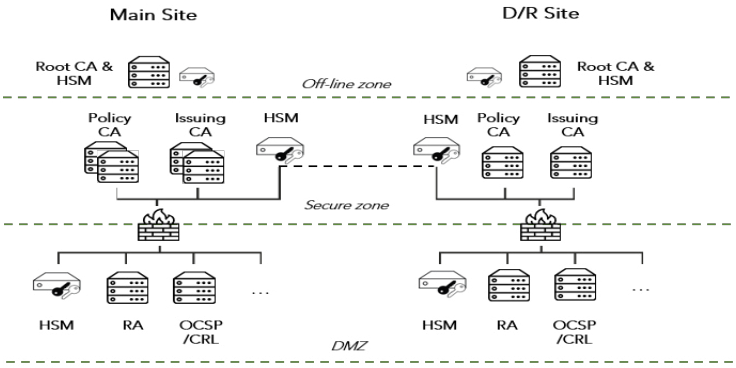
Paramount to the security of a PKI is the protection of the private keys belonging to the Certificate Authorities (CAs) and Validation Authorities (VAs) within the PKI. Secure generation and storage of the private keys must be assured.

The Solution

Hardware Security Modules (HSMs) are dedicated, hardened cryptographic devices that provide this protection for private keys. By using Thales Trusted Cyber Technologies (TCT) Luna Network HSM, federal agencies can be assured the most critical keys in their PKI are generated and stored in a trusted, FIPS 140-2 Level 3 certified* HSM designed and built in the United States.

Once generated by the HSM, the private keys never leave the hardened appliance and are utilized by EJBCA components via cryptographically secured communication links. At no time are these critical keys exposed to threats that exist in the external operating environment.

With a focus on security, EJBCA offers a powerful approval system and signed audit logs. It can utilize the Luna Network



Physical Architecture

HSM for all critical keys in the system, including not CA private keys and private keys used for Transport Layer Security (TLS), Online Certificate Status Protocol (OCSP), and audit log signing.

By integrating EJBCA Enterprise and Luna Network HSM, federal agencies will have a PKI that was designed from ground up with best security practices in mind.

Ease of Integration

EJBCA Enterprise's integration with the TCT HSM is seamless and straightforward. By utilizing the concept of a "Crypto Token," the HSM is easily configured as the crypto provider for the EJBCA component. Once the token is created, keys for various functions, like certificate signing and log signing, are also easily created on the HSM and associated with that token.

EJBCA Enterprise Key Benefits

EJBCA PKI by PrimeKey

- Includes Certificate Authority, Registration Authority, and Validation Authority (OCSP and Certificate Revocation List) components
- Issuance and complete lifecycle management of keys and certificates for people, machines and things
- Serves both small-scale environments and large implementations with millions of users
- Supports all major PKI enrollment protocols and integration interfaces
- Manages billions of certificates under high transaction loads
- Common Criteria certified and proven in practice for multiple national e-ID installations

Luna Network HSM HSM Key Benefits

- Provides centralized lifecycle management of cryptographic keys in a purpose-built, FIPS 140-2 Level 2 or 3 certified appliance
- Offloads and accelerates cryptographic operations to a dedicated cryptographic processor
- Available in multiple form-factors, including a USB-attached model ideal for offline root CAs
- Can be grouped together to provide high availability for critical PKI applications
- Developed, manufactured, and supported solely within the boundaries of the U.S., thus providing a completely trusted U.S. based source

About PrimeKey

PrimeKey is one of the world's leading companies for PKI and digital signing solutions. With our EJBCA Enterprise, SignServer Enterprise and the PrimeKey SEE products, we deliver the capability to implement an enterprise grade PKI system ready to support solutions such as IoT, e-ID, e-Passports, code signing, digital identities and electronic signatures; all solutions where digital certificates would be a main enabler. Choose to deploy your solution as flexible software, in a robust Appliance, in the Cloud, or in a hybrid deployment adapted to your business needs. More information at www.primekey.com.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com

*FIPS Validation Pending

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com