

PKI in a Virtualized World: Seamless, Simple, Secure and Straightforward with PrimeKey EJBCA Software Appliance and Thales Luna HSMs



Leverage your virtualization environment with PrimeKey EJBCA® Software Appliance and Thales Luna HSMs

Make PKI Simpler, More Manageable and More Secure

- Expanded support for even more Public Key Infrastructure (PKI) use cases
- Easy and fast deployment; simplified provisioning and maintenance
- Encryption keys and certificates used by EJBCA® protected in an HSM Root of Trust
- Root of Trust support for both on-premises and cloud HSM use cases

The Problem: Every day, businesses face unexpected security events and threats to their data. At the core of enterprise IT, Public Key Infrastructure (PKI) is an essential platform to protect identities, data and secure connections across the organization. At the heart of the PKI is a certificate authority (CA) that ensures the trustworthiness of all certificates within the PKI. Because the CAs private key is the anchor to the trustworthiness of all certificates within a PKI, one must ensure the CAs root key is well protected. A compromise of the root key means that the network of trust inherent within a stable PKI collapses, and the PKI can no longer be trusted.

The Solution: PrimeKey EJBCA® brings transparency to PKI, issuing machine, device and personal certificates, and providing the performance, flexibility and automation required for business critical applications. In order to ensure the trustworthiness of keys and certificates generated and used by a CA, and meet compliance needs, EJBCA® Software Appliance has integrated with Thales Luna Hardware Security Modules (HSMs). Luna HSMs generate, manage and store encryption keys and certificates in a root of trust across on-premises, cloud and hybrid environments, ensuring they cannot be compromised. With increasing pressure on PKI to protect new use cases, such as cloud services, mobile, and remote workforces, the ability to support scale, availability, and assurance is even more critical.

Secure and Protect Enterprise Networks, IT Systems, and IoT Devices

PrimeKey EJBCA® Software Appliance is a pre-packaged solution that allows you to deploy and maintain your PKI solution utilizing your existing virtualization environment. The software appliance works with Thales Luna Network HSMs and Luna Cloud HSM Services from Thales Data Protection on Demand (DPoD), and is integrated for customers that need an easy to deploy PKI solution with either an HSM on-premises or as a Cloud HSM service.

The software appliance includes all of the required software and is distributed as an Open Virtual Appliance (OVA) package, making it easy to install and maintain. The software appliance comes with a complete software technology stack packaged in a virtual machine (VM) and easily deployed within minutes.

Luna HSMs are FIPS 140-2 Level 3 validated and add critical levels of security to the PKI solution with a strong architecture that includes side channel attack protection; audit logging; and multifactor authentication. Luna HSMs ensure the critical private keys and digital identities are always secure by generating, managing and storing them in a hardware root of trust to help meet compliance needs. The support for the on-premises Luna HSM or the cloud-based Luna Cloud HSM service adds the assurance that the critical private keys and digital identities are always secure regardless of environment.

Luna HSMs offer a broad range of authentication methods and adaptive access policies that evaluate risk conditions and validate users by enforcing the appropriate level of authentication where needed, ensuring the right people have access under the right conditions.

Depending on requirements, the EJBICA® Software Appliance is available in five different models ranging from an 'XS model' with limited functionality and up to 1K certificates to an 'XL model' that is suited for extremely large PKI deployments. All models include a complete Certificate Management System, with an unlimited number of Certification Authorities (CAs) and subordinate CAs, Registration Authorities (RA), and Validation Authorities (VA). The models in between offer variation in the number of certificates they can manage.

PrimeKey EJBICA® Software Appliance and Luna HSMs are the essential components needed to deploy and operate a fully-compliant PKI with success.

Easy to Deploy, Easy to Maintain

Easy, efficient installation and management are critical to a secure and reliable PKI deployment. Updates to the EJBICA® Software Appliance are delivered as a complete and tested software package for smooth operation and maintenance of a full-blown PKI. In addition, the backup and restore procedures are robust, and simplified to reduce manual errors. All installation, configuration, and maintenance tasks are performed from a user-friendly graphical user interface, and there is no need for configurations files updates or other "under the hood" adaptations.

The EJBICA® Software Appliance works out-of-the-box with Luna HSM solutions that provide flexibility for on-premises or cloud-based, hybrid/multi-cloud root of trust protection and management of critical encryption keys.

- **Luna Network HSMs:**

- Store, protect and manage sensitive cryptographic keys on-premises in FIPS 140-2 Level 3 validated and Common Criteria EAL4+ certified, tamper-resistant hardware appliances, providing high-assurance key protection within an organization's own IT infrastructure.
- Perform all cryptographic operations within the HSM in order to maintain integrity and security of the network and provide the highest degree of protection for the CA and the root keys.
- Benefit from strong separation of duties, MofN with multifactor authentication, and data encryption to prevent unauthorized access to the HSM

- **Luna Cloud HSM (DPoD):**

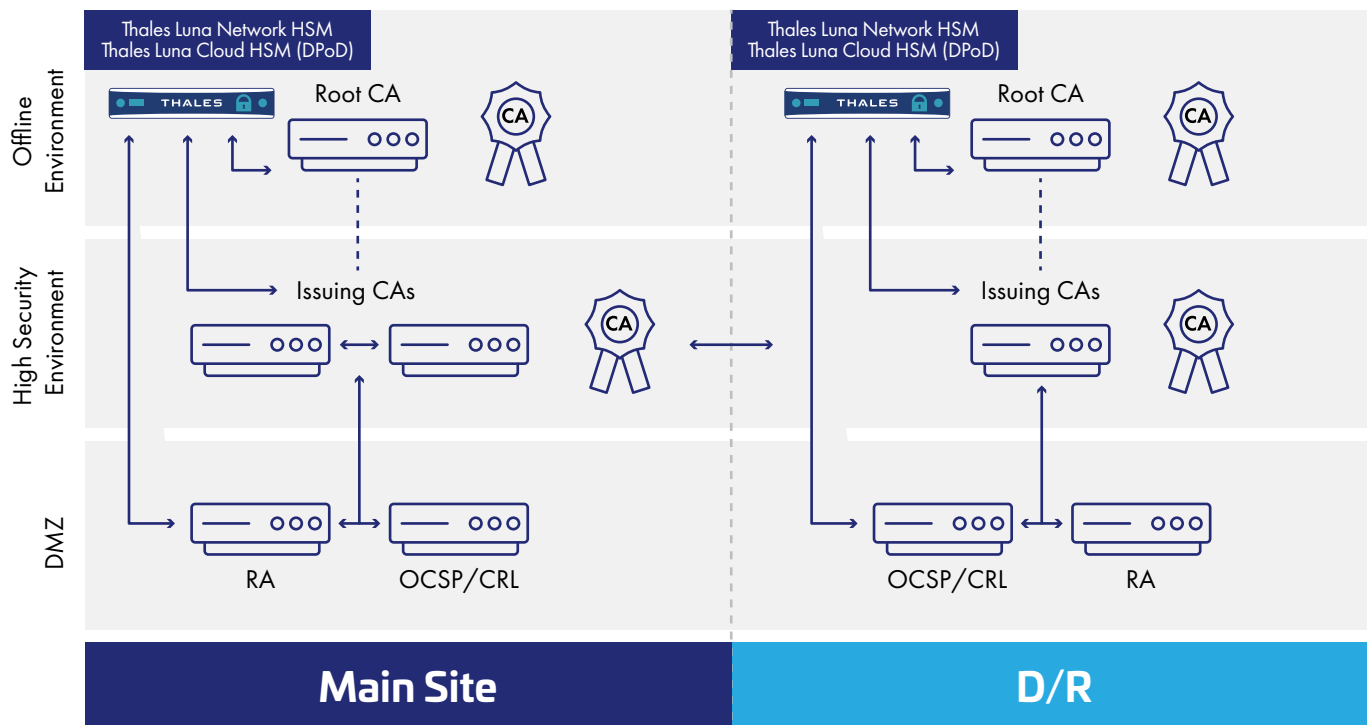
- FIPS 140-2 Level 3 validated Cloud HSM service that can be provisioned within minutes
- A fully Thales hosted and managed service (99.95% SLA) giving customers extremely easy and scalable access into HSM resources, yet only the end customer has access to the security critical PKI keys.
- Extensive set of automation and orchestration features included, enabling fast deployment of the HSM services even for users who do not have prior experience with HSMs.

- **PrimeKey EJBICA®:**

- Commonly referred to as a CA, EJBICA® PKI is an open-source, Common Criteria certified, IT-security software for Certificate Issuance, Certificate Management and Validation Authority (OCSP/CRL) services, used for secure communication in any environment.
- All EJBICA® upgrades are delivered as a complete and easy-to-install software package.
- System maintenance, backup, and restore tasks can be executed efficiently and straightforwardly.

With the EJBICA® Software Appliance, organizations can manage digital certificates and device/user enrollments to power strong authentication, encryption, and data integrity for a broad range of use cases. The inclusion of Luna Network HSMs or Luna Cloud HSMs makes it easy for organizations of all sizes to deploy PKI and adhere to best practices.

Deploying the EJBCA Appliance



Security and Simplicity in a Joint Solution

Organizations can implement strong security and best-in-class PKI management and key storage solutions from two security industry leaders. PrimeKey and Luna HSM solutions provide end-to-end key creation and management from certificate issuance to revocation. The seamless integration makes it easy for organizations to deploy PKI and adhere to best practices.

- Supports all your PKI and HSM needs and scales/aligns with your use cases
- Easier and faster with a self-contained unit and pre-installed software components
- Installation and configuration are performed entirely via the graphical user interface
- Lower costs with simplified management and maintenance
- Ensure the critical private keys and digital identities are always secure by generating, managing, and storing them in a root of trust to help meet compliance needs.

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 appliance, in a robust hardware appliance, in the Cloud/SaaS, or in a hybrid deployment adapted to your business needs. As of June 2021, PrimeKey is a part of Keyfactor. More information at www.primekey.com.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.