cpl.thalesgroup.com

THALES
Building a future we can all trust

Enabling IoT Security: PKI, Code-Signing and HSM Protected Keys

Creating Trust for Today's Connected World with Thales and PrimeKey

The Challenge

With new and constant threats to data emerging every day, Public Key Infrastructure (PKI) has become the increasingly prominent foundation of enterprise data security and risk management strategy. PKI is part and parcel of modern digital business, from secure communications to data transmission and beyond. Malware, hackers, and cyberattacks rank as one of the top costliest business issues and concerns globally. Today's business environment is also evolving, and organizations need to secure communication and access for their home-based employees, customers, partners, servers, and countless devices that maintain business continuity.

Implementing PKI within IoT is critical for businesses looking to fight back as it is the veritable security mechanism for guaranteeing that all communications are authentic, non-reputable and above-all, private.

In delivering end-to-end protection, today's PKI requires a robust platform for digital certificate and identity management, and Hardware Security Modules (HSM) are essential to securely generate, manage and store the private keys at the core of the PKI. Without an established root of trust (RoT) for the creation, management and secure storage of PKI private keys, the entire PKI solution is at risk. Without the proper expertise, operational management solutions and tools, PKI deployment and maintenance can be complex and time-consuming.

The Solution

A robust enterprise-class IoT security solution requires a combination of automated PKI certificate provisioning, firmware code signing, high-assurance key storage, and a powerful management system that simplifies certificate lifecycles while meeting data security and compliance requirements. PrimeKey and Thales bring together a proven PKI and key storage solution for both on-premise and cloud scenarios, combined with key lifecycle management systems to simplify certificate deployments that handle the large scale and widely dispersed needs of IoT.

PrimeKey EJBCA Enterprise brings the maturity and transparency required for any security-centric PKI solution. With EJBCA, 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 support for the (on-premise) Thales Luna HSM or the cloud-based Thales Luna Cloud HSM service adds the assurance that the critical private keys and digital identities are always secure regardless of location.

EJBCA enables flexible integration with most third-party and PKI dependent systems, combined with Luna HSMs. Managed through a web-based GUI combined with automated deployment possibilities, EJBCA's easy operation will simplify all aspects of PKI management.

- PrimeKey EJBCA and SignServer are multi-tenant and multi-use case solutions and leverage the Luna HSM to protect critical elements, e.g., CA, code, document, time-stamp, and e-passport keys.
- Luna HSMs store, protect and manage sensitive cryptographic keys on-premises in FIPS 140-2 Level 3 validated and Common Criterial EAL4+ certified, tamper-resistant hardware appliances, providing high-assurance key protection within an organization's own IT infrastructure.
- Luna Cloud HSM service is a cloud-based HSM as a service that can be provisioned within minutes and no need for specialized hardware or associated skills. (FIPS L3)
- PrimeKey EJBCA includes Certificate Authority (CA), Registration Authority (RA), and Validation Authority (VA) (OCSP and Certificate Revocation List) components along with issuance and complete lifecycle management of keys and certificates for people, machines, and things.
- Thales Trusted Access ensures secure identities and access to devices and applications with a broad range of authentication methods.

Key Features

- EJBCA and SignServer are available as an on-premises software appliance, in the AWS or Azure Cloud (IaaS) or combined.
- Built-in SLA, redundancy, high availability.
- Integrates via standard API and protocols: REST, ACME, EST, SCEP, WS, CMP, OAuth
- Multi-tenant - multiple CAs or signature use cases in one server installation.
- EJBCA is Common Criteria certified and installed at numerous eIDAS or WebTrust audited customers.

On-premises Luna HSMs + DPoD Luna Cloud HSM services work together for optimal flexibility and resilience

Hybrid Root of Trust

Migration from Luna HSM on-prem to Luna Cloud HSM and vice versa, with keys flowing back and forth between the two

Secure Backup

Both Luna HSMs (on-prem and cloud) used as a backup HSM with automatic key replication

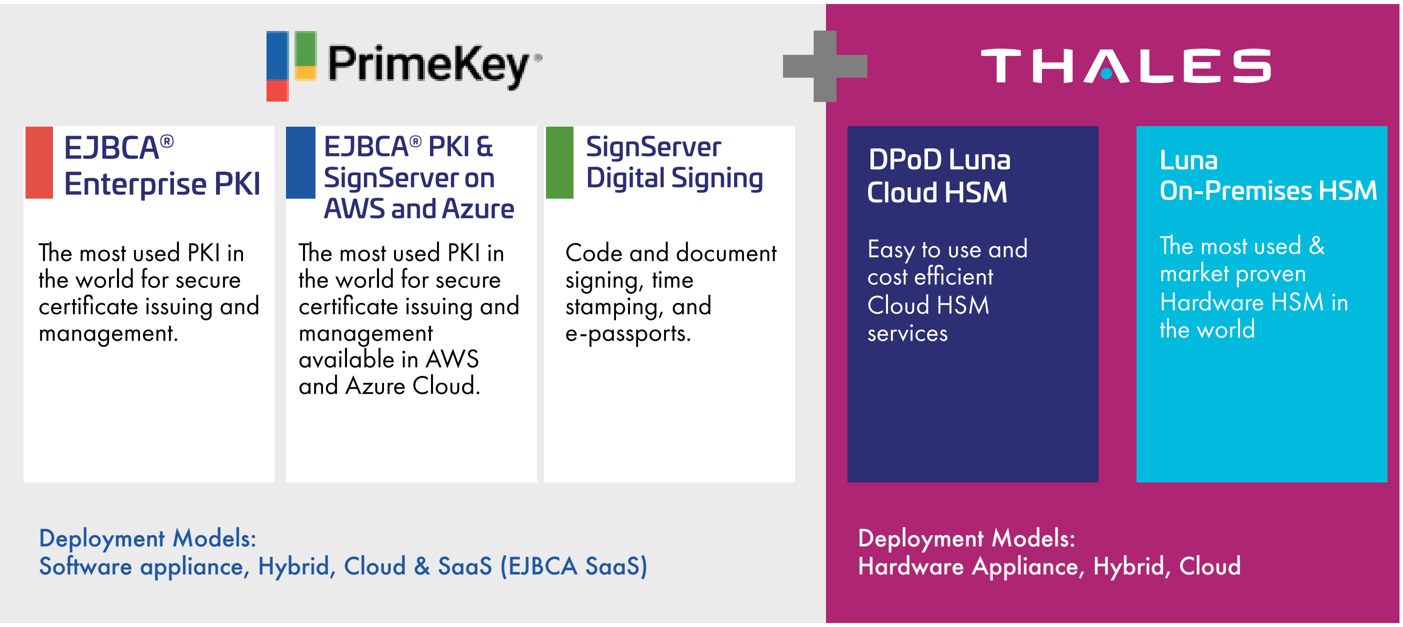
Reliability

Both Luna HSMs (on-prem and cloud) used as a standby in case one HSM becomes unavailable, optimizing performance and maintaining SLAs

Scalability

Both Luna HSMs (on-prem and cloud) used for bursting to help with peak performance requirements

- Works out-of-the-box with Luna HSM solutions that provide flexibility for cloud-based, hybrid/multi-cloud, or on-premises root of trust protection and management of encryption keys.



EJBCA® Enterprise PKI

The most used PKI in the world for secure certificate issuing and management.

EJBCA® PKI & SignServer on AWS and Azure

The most used PKI in the world for secure certificate issuing and management available in AWS and Azure Cloud.

SignServer Digital Signing

Code and document signing, time stamping, and e-passports.

Deployment Models:
Software appliance, Hybrid, Cloud & SaaS (EJBCA SaaS)

DPoD Luna Cloud HSM

Easy to use and cost efficient Cloud HSM services

Luna On-Premises HSM

The most used & market proven Hardware HSM in the world

Deployment Models:
Hardware Appliance, Hybrid, Cloud

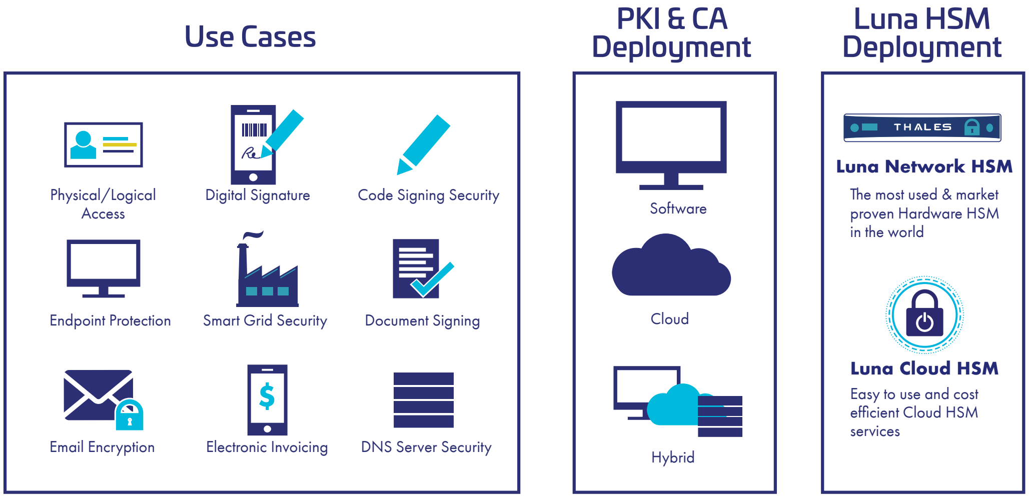
Solution Benefits

Today, many enterprises need the functionality of IoT with automated PKI capability and comprehensive certificate lifecycle management to meet the IoT security operation requirements of their deployments.

The combination of PrimeKey PKI with Luna HSMs provide:

- Flexible HSM key protection solutions offer cloud, hybrid/multi-cloud, and on-premise support that fit all deployments and meets the "high availability" required for an IoT production and operational environment
- Commonly referred to as a CA, EJBCA PKI is an open-source, Common Criteria certified, IT-security software for Certificate Issuance and Certificate Management, used for secure communication in any environment.
- EJBCA Enterprise also includes both RA and VA functionality to enable security through certificates properly.
- EJBCA Enterprise is highly flexible to most imaginable PKI use cases and scenarios. The solution can be found in face-to-face issuing workflows and highly automated processes via standard protocols and interfaces.
- Luna HSMs offer a broad range of authentication methods and adaptive access policies that evaluate risk conditions and validates users by enforcing the appropriate level of authentication where needed, ensuring the right people have access under the right conditions.
- 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.

PKI for Everything and Every Organization



In Summary

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.

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

PrimeKey

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.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us