Keyfactor and Thales TCT's solutions, designed specifically for Federal agencies, combine to deliver seamless migration to post-quantum cryptography.

RESOURCES

EJBCA and Luna SA HSM Integration
carah.io/ejbca-and-luna-integration

EJBCA Enterprise
carah.io/keyfactor-ejbca-enterprise

SignServer Enterprise
carah.io/keyfactor-signserver-entp

Thales TCT Luna Hardware Security Modules
carah.io/thales-hardware-security

CONTACT US

keyfactor@carahsoft.com

(888) 662-2724

https://www.carahsoft.com/keyfactor

Better Together: Keyfactor and Thales Deliver Post-Quantum PKI for Federal Agencies

Product Overview

As Federal agencies prepare for the quantum computing threat and navigate stringent compliance timelines under the Commercial National Security Algorithm (CNSA 2.0) and National Security Agency (NSA) guidelines, the need for quantum-resistant Public Key Infrastructure (PKI) has never been more critical.

Keyfactor's EJBCA Enterprise, integrated with Thales Trusted Cyber Technologies (TCT) Luna T-Series Network Hardware Security Module (HSM), delivers a comprehensive PKI solution specifically designed to meet Federal security requirements while ensuring seamless migration to post-quantum cryptography.

This native integration combines proven certificate authority (CA) capabilities with hardware-based cryptographic protection, offering agencies a trusted foundation for digital identity management across national security systems.

EJBCA Enterprise provides the maturity and transparency essential for security-focused Government applications. The solution allows for flexible integration with existing Federal infrastructure while maintaining the highest levels of cryptographic assurance through Luna T-Series HSMs, which are designed, developed, manufactured and supported entirely within the U.S. by security-cleared personnel.

How it Works

This integrated solution functions through Keyfactor's comprehensive PKI, signing and certificate lifecycle management platforms, which include EJBCA for CA operations, Command for CA-agnostic certificate lifecycle management and SignServer for large-scale, secure digital signing. All components are post-quantum ready today, allowing agencies to start implementing quantum-resistant certificates and signatures immediately.

The Luna T-Series HSM acts as the hardware root of trust, generating and safely storing all critical cryptographic keys within a Federal Information Processing Standard (FIPS) 140-3 Level 3 certified appliance that never exposes private keys to external threats.

Integration between EJBCA and the Luna T-Series HSM occurs through a streamlined "Crypto Token" configuration that eliminates the traditional friction points associated with HSM deployment. This native integration ensures that certificate signing keys, audit log signing keys and other critical cryptographic material remain protected within the hardened HSM environment. The system supports both parallel PKI infrastructure deployment for gradual migration and in-place firmware upgrades that enable seamless transitions from conventional to post-quantum algorithms without hardware replacement.

For agencies with existing PKI infrastructure, the solution supports two deployment approaches: building parallel post-quantum infrastructure alongside existing systems or migrating existing certificate lifecycles through crypto-agile processes. The platform's scalability handles millions to billions of certificate operations, with Luna T-Series HSMs optimized specifically for Government-mandated algorithms and key lengths.

KEYFACTOR | **THALES** | **carahsoft**

Real-time monitoring capabilities, enhanced through Keyfactor's recent acquisitions of InfoSec Global and Cypher Insights, provide comprehensive visibility into cryptographic assets and endpoint capabilities throughout the migration process.

The solution addresses the complex ecosystem requirements of post-quantum migration by ensuring all components—from cryptographic engines to Transport Layer Security (TLS) stacks—work seamlessly together despite larger certificate sizes and different protocol overheads. Advanced performance optimization continues to improve as post-quantum protocols mature, while the deep partnership between Keyfactor and Thales TCT ensures coordinated product development and unified customer support.

KEY BENEFITS:

Keyfactor EJBCA Enterprise Advantages

- Complete certificate lifecycle management for people, machines and devices
- Common Criteria certified and North Atlantic Treaty Organization (NATO) approved for high-security Government applications
- Post-quantum ready across all components, including underlying cryptographic engines
- Supports multiple parallel PKI hierarchies within a single deployment
- Web-based management interface simplifies complex PKI operations

Thales Luna T-Series HSM Protection

- FIPS 140-3 Level 3 certification and approval from the Committee on National Security (CNSS)
- Designed, developed and manufactured entirely within the U.S.
- All personnel are U.S. citizens with security clearances
- Industry-leading cryptographic performance optimized for NIST-standardized PQC algorithms
- High availability configurations for mission-critical operations
- Multiple form factors, including USB-attached models for offline root CAs

Integrated Partnership Value

- Pre-validated turnkey solution eliminates integration risks and deployment complexity
- Native "Crypto Token" integration removes traditional HSM bootstrapping friction
- Executive-level partnership ensures coordinated roadmaps and unified support
- Decades of combined Federal sector experience across both organizations
- Joint problem-solving prevents vendor disputes during critical operations
- Continuous optimization as post-quantum standards evolve

Operational Excellence Through Collaboration

- Industry cooperation is essential for successful post-quantum migration
- Comprehensive ecosystem visibility through combined discovery and monitoring capabilities
- Joint development ensures coordinated performance and security enhancements
- Unified solution evolution eliminates compatibility issues between vendors
- Proactive challenge resolution before impact to Federal customers

CONTACT US   keyfactor@carahsoft.com • (888) 662-2724 • https://www.carahsoft.com/keyfactor

KEYFACTOR | THALES | carahsoft.