securosys

Solution Brief

Keyfactor EJBCA / SignServer and Securosys Primus HSM

Post-Quantum ready PKI with REST API

Securosys and Keyfactor have collaborated to enhance PKI security by integrating Securosys Primus HSMs with Keyfactor's EJBCA and SignServer through REST API. This innovative approach removes the complexities associated with PKCS#11 in SaaS and PaaS environments, streamlining cryptographic operations for improved scalability and resilience. Built-in Post-Quantum Cryptography (PQC) support enables organizations to prepare for future cybersecurity challenges while ensuring the highest standards of key protection.

Challenge

Modern enterprises demand scalable, robust, and easy-to-integrate PKI solutions to manage digital certificates and cryptographic operations securely. Traditional HSM integrations using PKCS#11 are often cumbersome to configure and maintain. Moreover, evolving cryptographic standards necessitate infrastructure readiness for PQC algorithms to stay secure and future-proof.

Solution Benefits

Simplified Setup & Maintenance: REST API integration reduces deployment complexity by eliminating PKCS#11 dependencies.

PQC-Ready Security: Native support for postquantum algorithms ensures long-term cryptographic agility.

Secure Key Management: SKA policies enforce multi-party authorization and regulatory compliance.

Seamless Integration: Fully integrated with FortiGate for a streamlined setup and simplified management.

Flexible Deployment: Available on-premises or as a cloud-based service, enabling scalable deployment options.

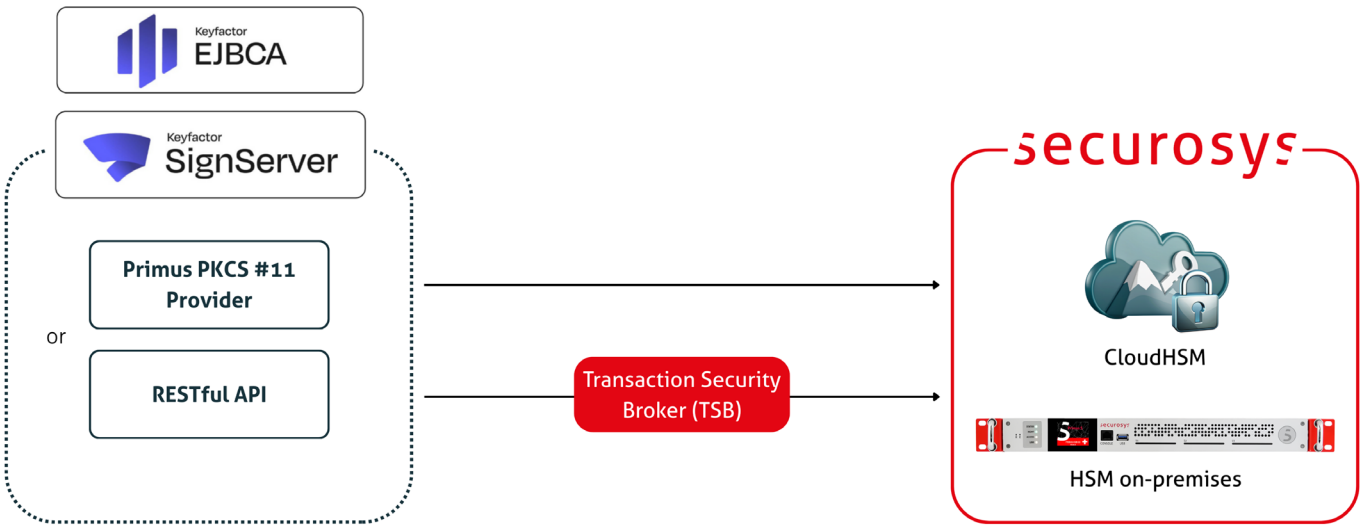
Get started

securosys

Solution Integration

By leveraging REST API integration, Keyfactor EJBCA and SignServer can establish direct, secure connections with Securosys Primus HSMs, eliminating the need for additional middleware or PKCS#11 configurations. This integration streamlines certificate issuance, validation, and encryption processes, all while ensuring hardware-backed protection of private keys.

Enterprises benefit from real-time cryptographic operations that optimize both performance and security without added complexity. The solution also includes built-in support for NIST-selected post-quantum cryptographic algorithms – such as ML-DSA, SLH-DSA, ML-KEM, HSS-LMS, and XMSS – allowing organizations to future-proof their PKI infrastructure. As a result, businesses can smoothly transition into the post-quantum era while staying resilient against evolving security threats.



HSM Deployment Options

Joint Use Cases

This integration provides organizations with a forward-looking solution by supporting Post-Quantum Cryptography (PQC) algorithms, ensuring resilience against emerging threats. Businesses can utilize hybrid signatures that combine classical and post-quantum cryptographic algorithms, enabling broad compatibility across legacy and modern systems.

The solution strengthens security for critical applications such as digital signing, document authentication, and identity verification. These capabilities help organizations meet stringent compliance requirements while maintaining the highest level of trust in digital transactions. By leveraging this integration, businesses can proactively adapt their cryptographic infrastructure to evolving security challenges without disruptive systems overhauls.

About Keyfactor

About Securosys

KEYFACTOR