Keyfactor +
Utimaco SecurityServer

End-to-end certificate lifecycle management backed by secure key generation and protection with Utimaco SecurityServer.

KEYFACTOR

utimaco®

Application
Utimaco SecurityServer HSM

Works with
Keyfactor EJBCA

Integration
PKCS#11

Use case
Certificate Authority and
Public Key Infrastructure (PKI)

Data is the critical digital asset of any company. To protect this data along with the identities of individuals and communication across the organization, Public Key Infrastructure (PKI) is a needed solution. The trustworthiness of PKI is entirely dependent on the Certificate Authority (CA), as the CA issues the certificates within PKI. CA utilizes the private key for issuing the certificates, so it is essential to protect the key. Unauthorized access to the private key reduces the trustworthiness of the PKI system.

Solution overview

Keyfactor and Utimaco combine the benefits of certificate lifecycle management with secure key management in SecurityServer. While Keyfactor EJBCA provides complete registration, issuance, and management for certificates' lifecycle, SecurityServer ensures secure generation, storage, and signing with CA (Certificate Authority) private keys. The combined solution gives teams the flexibility to securely issue and manage millions of certificates, with the PKI hosted in the cloud, on-premises, or a combination of both.

Flexible and scalable

Open standards and compliance

Protect CA private keys

EJBCA supports various PKI use cases, scenarios, and integrations into application ecosystems and is proven in large deployments worldwide. Deploy EJBCA and SecurityServer to suit your needs — either as a turn-key software or hardware appliance, in the cloud, or as a full-blown eIDAS compliant PKI.

Built on open standards, a Common Criteria certified platform, and numerous high security and audited reference customers, Keyfactor EJBCA and Utimaco SecurityServer ensure best practices and commitment for a long-term security solution.

A Hardware Security Module (HSM) is required to provide the highest degree of protection for the CA and the root keys in a PKI. EJBCA can host multiple Certificate Authorities and PKIs within one single server installation and integrates smoothly with SecurityServer using the FIPS 140-2 Level 3 certified or Common Criteria approved Utimaco HSM on-premises or in the cloud.

How it works

Keyfactor EJBCA issues and manages certificates via standard enroll-ment protocols, REST integrations, or manual procedures. The platform leverages SecurityServer to protect the CA private keys ensuring secure cryptographic operations when signing human, server, or device certificates. PKCS #11 is the required cryptographic interface for this integration.
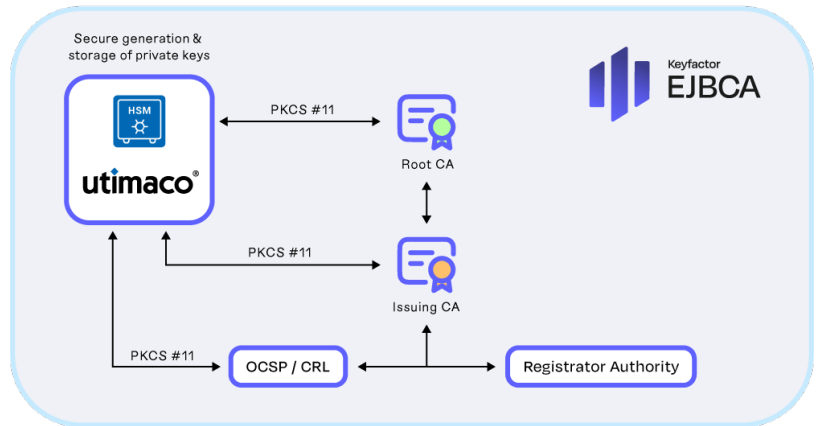
Key features

Excellent Price-Performance ratio

SecurityServer provides high performance of up to 10,000 RSA or 6,000 ECDSA signing operations for an attractive price and includes all necessary features and crypto algorithms.

Private key protection

Complete control of private keys in Utimaco's SecurityServer provides the most robust security.

DevOps-ready

EJBCA's extensible RESTful APIs and support for standard protocols such as EST, ACME, SCEP, and CMP, make it easy for developers to integrate security into applications.

Distributed architecture

EJBCA and SecurityServer can offer a highly scalable and distributed architecture that supports millions of certificates per customer

Flexible deployment

Keyfactor and Utimaco offer the flexibility to deploy as a service (SaaS), on-premises, or in cloud architecture.

Lifecycle automation

By adding the product Keyfactor Command, certificate discovery and certificate lifecycle automation can be extended and made more flexible.

---

utimaco®

UTIMACO is a global platform provider of trusted Cybersecurity and Compliance solutions and services with headquarters in Aachen (Germany) and Campbell, CA (USA).

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human.

KEYFACTOR