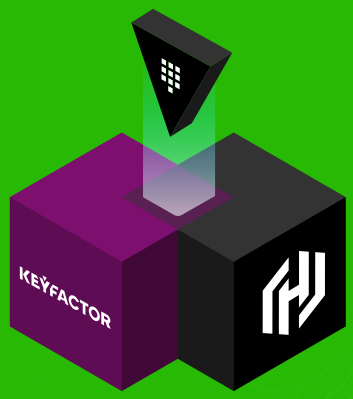
KEYFACTOR

Keyfactor Secrets Engine for HashiCorp Vault

Enable services with seamless access to trusted X.509 certificates, while security teams retain full visibility and control over backend PKI operations.

REQUEST A DEMO



HashiCorp Vault's built-in PKI allows DevOps teams to generate X.509 certificates they need to protect sensitive data and authenticate access to platforms and applications. However, as security teams demand more visibility and control over PKI and certificate issuance processes, finding a balance between speed and security is a serious challenge.

HashiCorp Vault + Keyfactor

Keyfactor acts as a secure PKI backend for HashiCorp Vault to ensure that every certificate is trusted and compliant with enterprise security requirements, without slowing down developers.

IMPROVE SECURITY

Give your security teams the ability to actively inventory and monitor certificates issued across all Vault instances and enforce consistent policies and approval workflows.

SIMPLIFY PKI

Make it easy for DevOps teams to request internal and publicly trusted certificates from any CA configured in the Keyfactor platform via native HashiCorp Vault APIs and workflows.

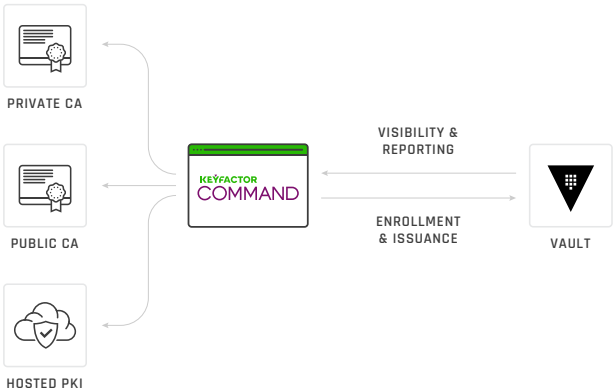
ACCELERATE DEVOPS

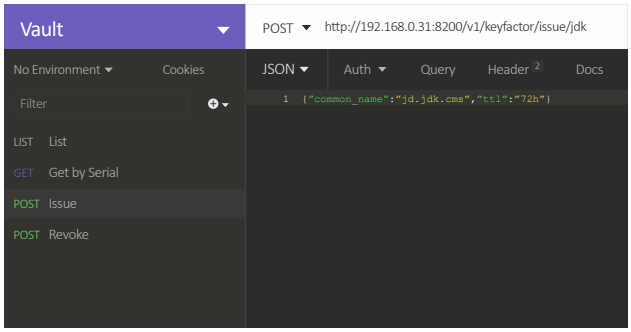
Eliminate manual, time-consuming certificate request processes by using developer-friendly APIs and identity-based access provided by HashiCorp Vault.

A Secure & Scalable PKI Backend for HashiCorp Vault

The Keyfactor secrets engine is implemented using Vault's plugin architecture to provide developers and security teams with exactly what they need.

- Connects Vault with any public or private certificate authority (CA) or Keyfactor's PKI as-a-Service
- Ensures all certificates are compliant with enterprise policy and audit controls
- Enables developers to issue certificates from any certificate provider via native Vault workflows
- Performs thousands of certificate operations per second at high scale with low latency





Fast, Easy Access for Developers

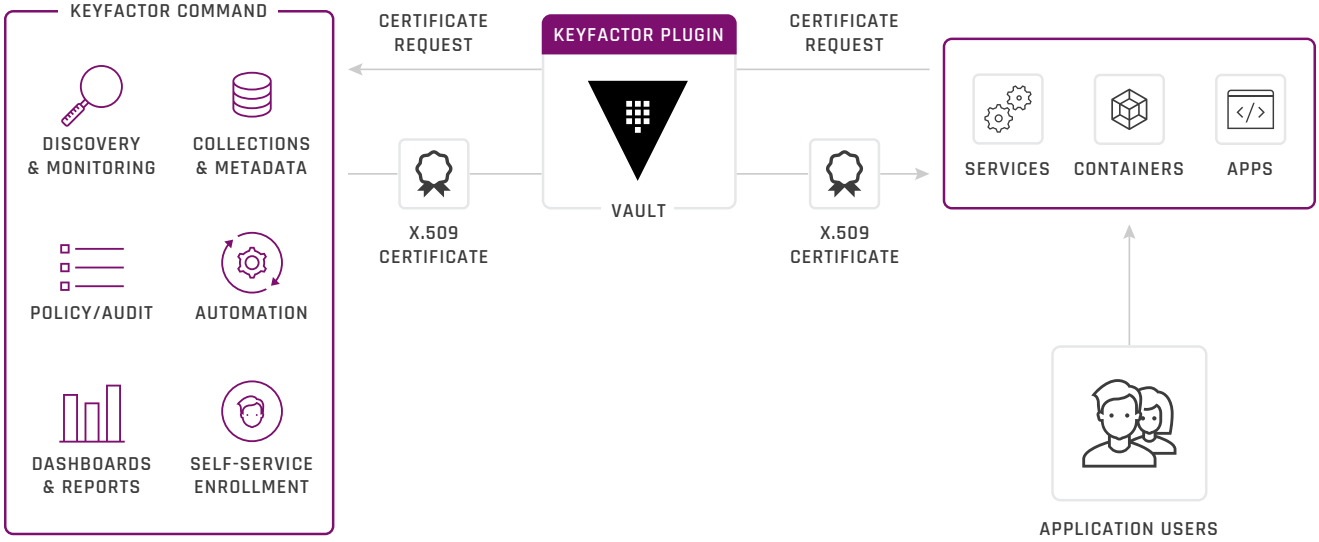
DevOps teams use the Vault-native API, CLI or UI to generate X.509 certificates and requests are rapidly fulfilled in the backend by Keyfactor Command.

This allows developers to move fast while ensuring that every certificate is issued from a trusted CA and compliant with policies defined by the security and PKI teams.

Watch Demo →

How it Works

Instead of using the Vault-native PKI secrets engine, the Keyfactor secrets engine is configured in the Vault plugin directory to route certificates requests to Keyfactor Command and deliver signed certificates back to Vault.



EASY DEPLOYMENT

The Keyfactor secrets engine uses the same Vault API as the built-in PKI secrets engine, so developer workflows remain unchanged.

COMPLETE VISIBILITY

Gain complete visibility of every key and certificate issued across all Vault instances and manage them from a single, easy to use dashboard.

POLICY CONTROL

Enforce certificate policies, use custom metadata to define granular rules, and easily search and revoke rogue or non-compliant certificates.

REAL-TIME REPORTING

Monitor the status of certificates, generate reports, set automated alerts, and automate the renewal of certificates with extended lifespans.

Using Keyfactor with HashiCorp Vault

Keyfactor Command makes it easy to discover, automate and protect certificates across multi-cloud deployments, and eliminates the complexity of setting up and running your own PKI for Vault.

	WITHOUT KEYFACTOR Vault-Native PKI Secrets Engine	WITH KEYFACTOR Keyfactor Secrets Engine for Vault + PKIaaS
DYNAMIC X.509 CERTIFICATES Allows users to dynamically generate short-lived X.509 certificates on demand.	✓	✓
API-DRIVEN WORKFLOWS Developers can use the Vault-native UI, CLI or HTTP API to get certificates.	✓	✓
ACCESS CONTROLS Enforces access controls via Vault identity-based access & authentication.	✓	✓
ANY CA AGILITY Allows Vault to issue certificates from any internal or publicly trusted CA for use in production environments.		✓
VISIBILITY & POLICY CONTROL Brings all certificates issued by Vault and other CAs into a single dashboard.		✓
LIFECYCLE AUTOMATION Enables one-click renewal, replacement and revocation of issued certificates.		✓
CLOUD-HOSTED PKI AS-A-SERVICE Delivers a dedicated, privately-rooted and highly available PKI in the cloud.		✓
SECURE ROOT OF TRUST Highly secure facilities & built-in HSMs protect your Root & Issuing CAs.		✓
24/7 PKI OPERATIONS It's your PKI, built and operated to industry best practices by our expert team.		✓

Related Integrations:

KEYFACTOR ANYGATEWAY

Use the built-in Vault PKI secrets engine and synchronize inventory in real-time with Keyfactor to provide security teams with visibility of all certificates issued across Vault instances along with one-click revocation or replacement.

KEYFACTOR SECRETS

Provide the Keyfactor platform with automated access to privileged credentials in Vault required for sensitive certificate provisioning, renewal and rekey operations.

KEYFACTOR

Keyfactor empowers enterprises of all sizes to escape the impact that breaches, outages and failed audits from mismanaged digital certificates and keys have on brand loyalty and the bottom line. Powered by an award-winning PKI as-a-service platform for certificate lifecycle automation and IoT device security, IT and InfoSec teams can easily manage digital certificates and keys. And product teams can build IoT devices with crypto-agility and at massive scale. Exceptional products and a white-glove customer experience for its 500+ global customers have earned Keyfactor a 98.5% retention rate and a 99% support satisfaction rate.

▶ www.keyfactor.com
▶ +1.216.785.2990