digicert® | HashiCorp

DigiCert Vault Plugin: Seamless CA Gateway Integration

SOLUTION BRIEF

Digicert Vault Plugin: Seamless CA Gateway Integration

Problem statement

In dynamic infrastructures, there is a growing need for a reliable and manageable source of identity that complies with regulatory standards. Centralizing secrets management across an organization ensures consistent policy enforcement while facilitating compliance and audit efforts. However, this approach may lack the capability to generate certificate-based identities that meet the stringent security demands of highly regulated industries. Even if a compliant PKI environment is in place, it may not be integrated with the secrets management system. Often, secrets are scattered and stored inconsistently, increasing the risk of theft and conflicting with well-structured DevOps practices. This highlights the importance of integrating PKI management systems with vault solutions to enable centralized control and efficient handling of secrets.

Product integration

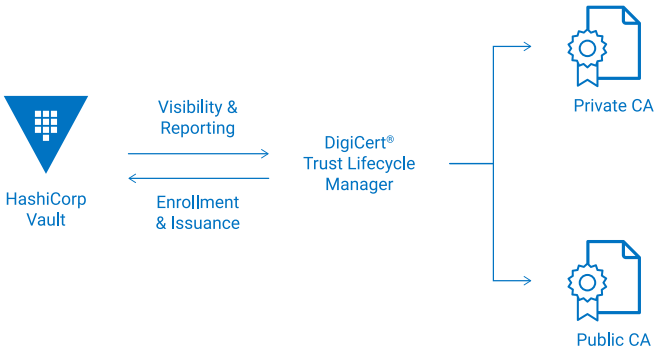
Digicert functions as a secure PKI backend for HashiCorp Vault, ensuring that all certificates are reliable and meet enterprise security requirements, without hindering developer workflows.

The DigiCert HashiCorp Vault integration offers an efficient solution for managing the enrolment, retrieval, and revocation of TLS/SSL certificates through DigiCert® Trust Lifecycle Manager. Delivered as a custom DigiCert Vault PKI plugin, this integration enables Vault to remain a centralized hub for certificate distribution and access, enhancing DevOps automation capabilities.

Key features include:

- Generating and signing Certificate Signing Requests (CSRs)
- Storing and tracking the status of issued certificates within Vault

This integration supports both the creation and storage of new TLS/SSL certificates in Vault, with various certificate types available based on configuration.

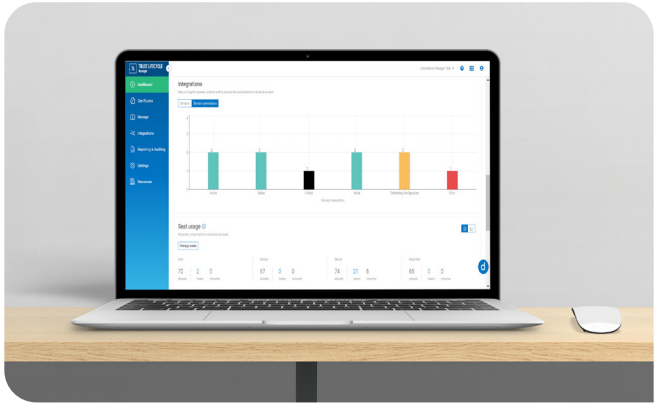


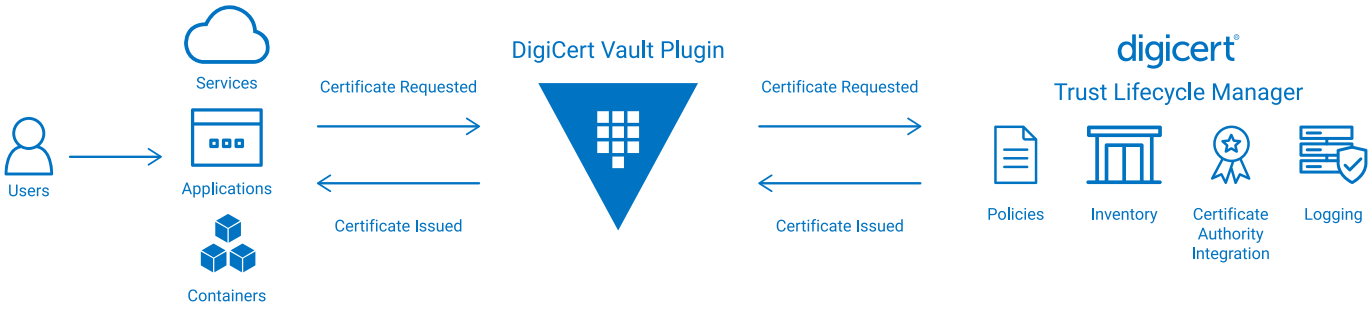
How it works

The DigiCert Vault PKI plugin acts as a bridge between Vault and your Certificate Authorities (CAs), bypassing Vault's native PKI secrets engine. Instead, the plugin, installed in Vault's plugin directory, routes certificate requests to the DigiCert ® Trust Lifecycle Manager and returns signed certificates to Vault. Built using Vault's plugin architecture, the DigiCert Vault PKI plugin provides security teams and developers with:

- Connectivity to any** public or private CA supported by DigiCert® Trust Lifecycle Manager
- Assurance that all certificates comply with organizational policies and audit standards
- The ability to issue certificates from any provider using Vault's native workflows

** - Vault plugin will support all the CAs that are supported by DigiCert® Trust Lifecycle Manager through API enrolment.





Value

Use Case	Description	Data Points
Automated Certificate Management	Automates the entire lifecycle of certificates, including issuance, and revocation, reducing manual work and human error.	Reduces administrative overhead and ensures certificates are always valid and compliant.
Seamless Integration with Vault	Fully integrates with HashiCorp Vault, streamlining certificate management within existing security workflows.	Supports multi-cloud, container, and hybrid environments.
Fine-Grained Access Control	Role-based access control (RBAC) policies ensure only authorized users and services can access sensitive certificates.	Helps meet security compliance for regulations.
Enhanced Visibility & Auditing	Centralized logging and audit trails for certificate usage and actions within Vault, improving oversight and compliance.	Complete audit logs for tracking certificates, detecting anomalies, and ensuring regulatory compliance.
Scalable Solution	Supports large-scale environments with dynamic certificate management capabilities, optimizing operational efficiency.	Scales to handle enterprise-level workloads across global, hybrid, and cloud environments.

About DigiCert, Inc.

DigiCert is the world's leading provider of digital trust, enabling individuals and businesses to engage online with the confidence that their footprint in the digital world is secure. DigiCert® ONE, the platform for digital trust, provides organizations with centralized visibility and control over a broad range of public and private trust needs, securing websites, enterprise access and communication, software, identity, content and devices. DigiCert pairs its award-winning software with its industry leadership in standards, support and operations, and is the digital trust provider of choice for leading companies around the world. For more information, visit digicert.com or follow @digicert.