# PKI Automation and Integrated Secret Management with AppViewX and HashiCorp

## Pain Point

A critical part of the IT/DevOps teams' jobs involve 'secret management'. As part of this task, confidential material such as private keys, access codes, and database credentials must be stored, circulated, managed, and used with utmost caution, so as to prevent loss, or potential misuse. Often, these secrets are stored in a miscellaneous, scattered fashion, which not only increases their exposure to theft, but is also counter-intuitive to traditionally rapid, organized DevOps processes. These methods also lack industry - standard encryption, which compromises organizations' threat deterrence capabilities and compliance protocols even further. The use of secure vault software to store and circulate secrets adds an additional layer of security to tasks like key storage for SSL termination and use, or key imports. Additionally, there is a need for the PKI management system to be closely integrated with the secure vault, so as to facilitate simplified management, centralized control, and streamlined usage of secrets.

## AppViewX-HashiCorp Joint Solution

AppViewX and HashiCorp Vault integrate seamlessly to enable secure correspondence between various applications. The disjointed manual processes of key generation and Certificate Signing Requests can be skipped by means of automation, accelerating the process of issuance and installment. HashiCorp Vault provides secure storage, retrieval, and manipulation of PKI components, while AppViewX assumes the role of a registration authority, certificate management engine, and lifecycle automation tool via the API..

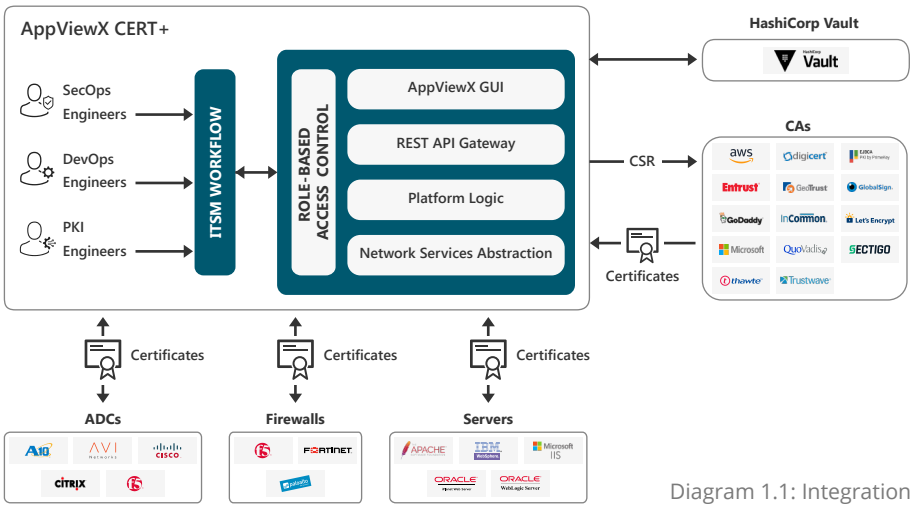


Diagram 1.1: Integration Overview

## Solution Benefits

- Based on the policy configured, admins can select a CA and rapidly get (internal/external) CA-signed certificates issued.
- Secure storage of certificates, keys, and CSRs within HashiCorp Vault.
- Full lifecycle management of certificates and keys via AppViewX's automation engine.
- Seamless integration with AppViewX via SDK.

# Solution Highlights

## Certificate Enrolment with AppViewX as (internal/external) CA

AppViewX provides a plugin that can be configured and installed into a live HashiCorp Vault environment. Here, AppViewX acts as a Registration Authority, via which certificate requests are routed by the Vault. Once the Vault requests a certificate, AppViewX automatically gets the certificate signed by the CA, and pushes it back to the vault for further usage.

Once the setup process is complete, users can request and enrol certificates from right within the Vault's PKI engine, with the certificates and private keys being stored inside it to enhance security and minimize latency.

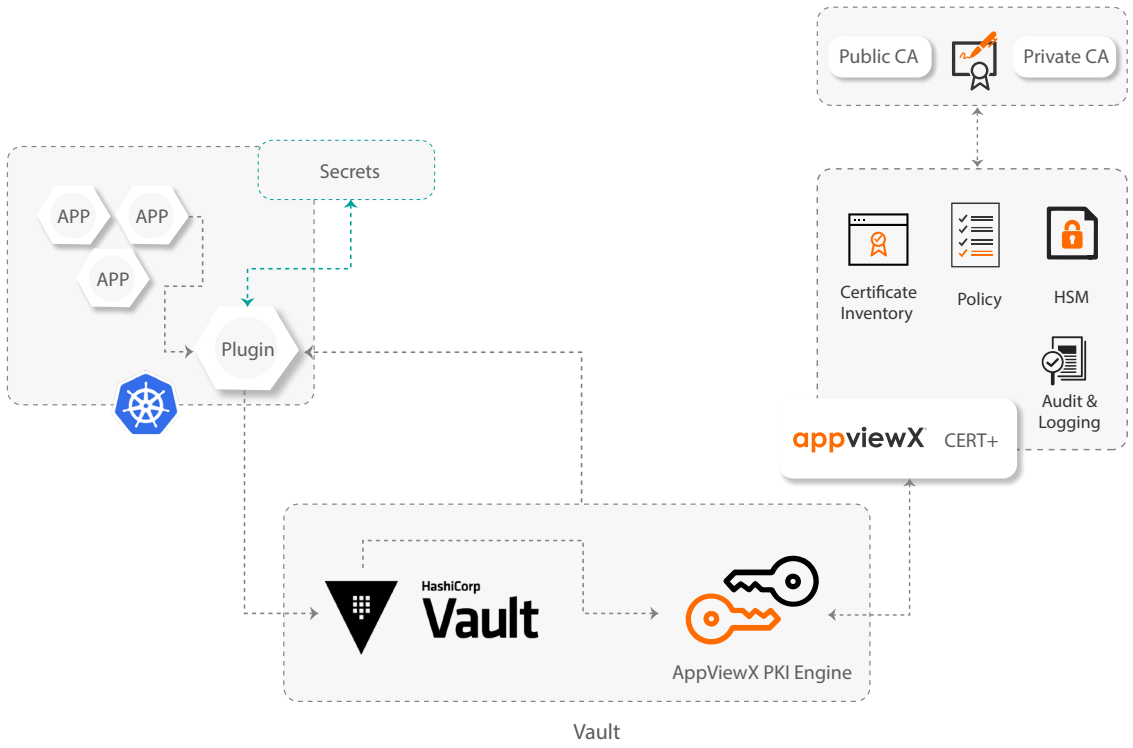


Diagram 1.2: Certificate Auto-enrolment with Dynamic Secrets Creation

## Single-pane-of-glass Issuance and Secure Key Storage

HashiCorp Vault's PKI engine is capable of securing, encrypting, storing, and controlling access to certificates, keys, and CSRs. The AppViewX-Vault integration makes it possible for users to obtain certificates from an enterprise/public CA without having to manually generate private keys and CSRs, submitting them to a CA, and getting them verified and signed before they can be deployed. AppViewX single-pane-of-glass functionality makes this possible without the user having to switch between interfaces to do so. HashiCorp Vault features built-in authentication and authorization functionality, enabling verification to be completed internally – this accelerating and securing the transaction end-to-end.

## Summary

The AppViewX-HashiCorp Vault integration solves a critical business problem – the enforcement of complete security and privacy of communications, while also easing issuance and enrolment cycles via Vault's PKI backend. Enterprises can take advantage of the joint solution to obtain greater visibility into their PKI infrastructures and accelerate traditionally slow certificate and key processes in order to better navigate DevOps pipelines.

## Next Steps

To learn more about AppViewX CERT+ or HashiCorp Vault, visit appviewx.com/products/cert or hashicorp.com/products/vault/

## About HashiCorp

HashiCorp is the leader in multi-cloud infrastructure automation software. The HashiCorp software suite enables organizations to adopt consistent workflows to provision, secure, connect, and run any infrastructure for any application. HashiCorp's open source tools Vagrant™, Packer™, Terraform, Vault, Consul, and Nomad are downloaded tens of millions of times each year and are broadly adopted by the Global 2000. Enterprise versions of these products enhance the open source tools with features that promote collaboration, operations, governance, and multi-data center functionality. The company is headquartered in San Francisco, though 85 percent of HashiCorp employees work remotely, strategically distributed around the globe. HashiCorp is backed by Bessemer Venture Partners, Franklin Templeton, Geodesic Capital, GGV Capital, IVP, Mayfield, Redpoint Ventures, T. Rowe Price funds and accounts, and True Ventures. For more information, visit https://www.hashicorp.com or follow HashiCorp on Twitter @HashiCorp.

**About AppViewX**

AppViewX is revolutionizing the way DevSecOps and NetOps teams deliver services to enterprise IT. The AppViewX platform is a modular, low-code software application that enables the automation and orchestration of enterprise network infrastructure and certificate management using an intuitive, context-aware visual workflow. It is built to rapidly enable users to implement cryptto-agility, enforce compliance, eliminate errors, and reduce cost. AppViewX is headquartered in New York City with additional offices in the US, UK, and India.
To know more, visit **www.appviewx.com** or **info@appviewx.com**

© 2020 AppViewX, Inc. All Rights Reserved.