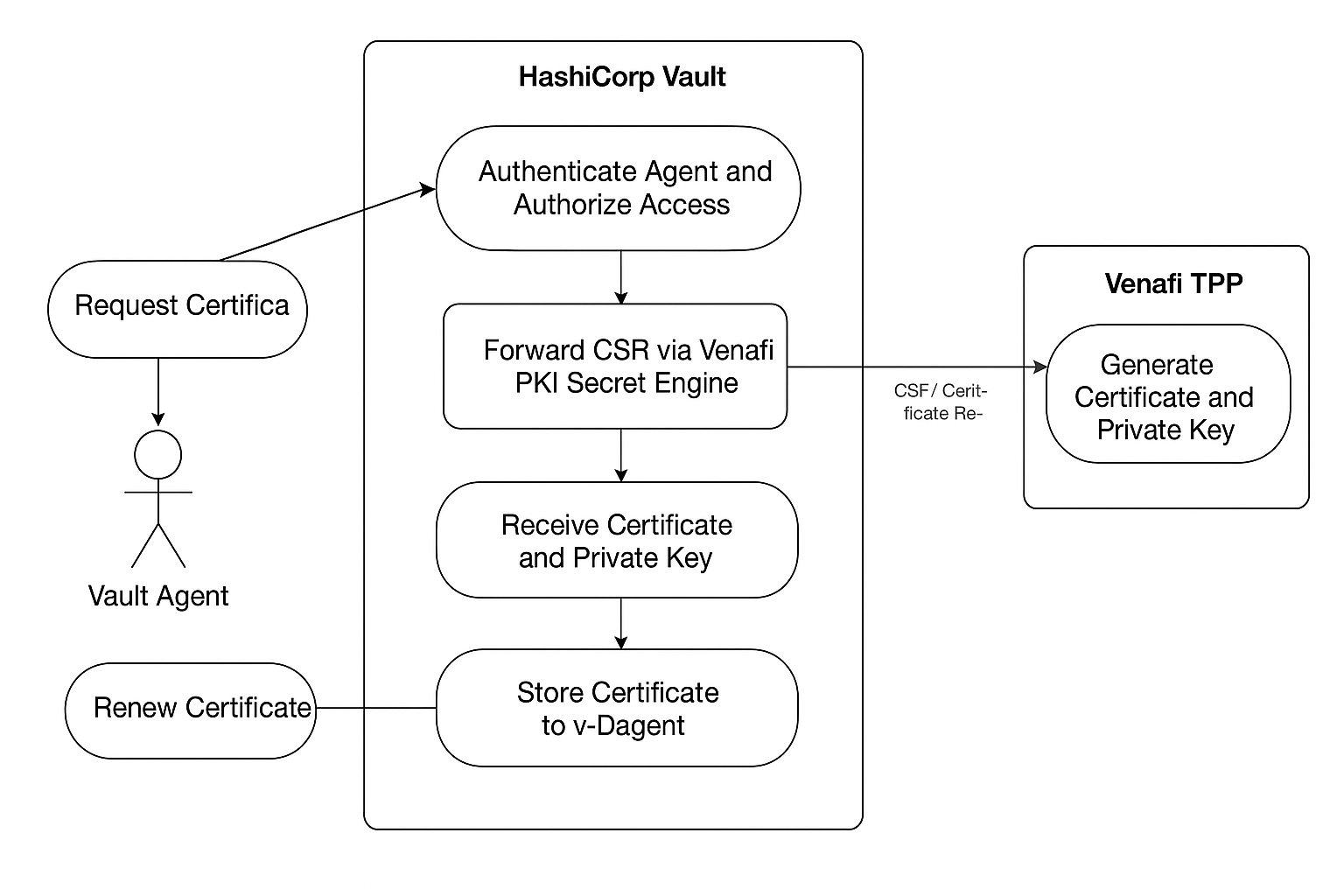
# Vault–Venafi PKI Integration: Use Case and Context View Documentation

## 1. Use Case Diagram

The following diagram represents the interaction between Vault Agent, HashiCorp Vault, Venafi PKI Secret Engine, and Venafi TPP for certificate management lifecycle. The Venafi PKI Secret Engine acts as a passthrough between Vault and Venafi TPP, while the Certificate Store ensures certificates and private keys are securely stored.



## 2. Functional Requirements (FRs) and Non-Functional Requirements (NFRs)

### Functional Requirements (FRs)

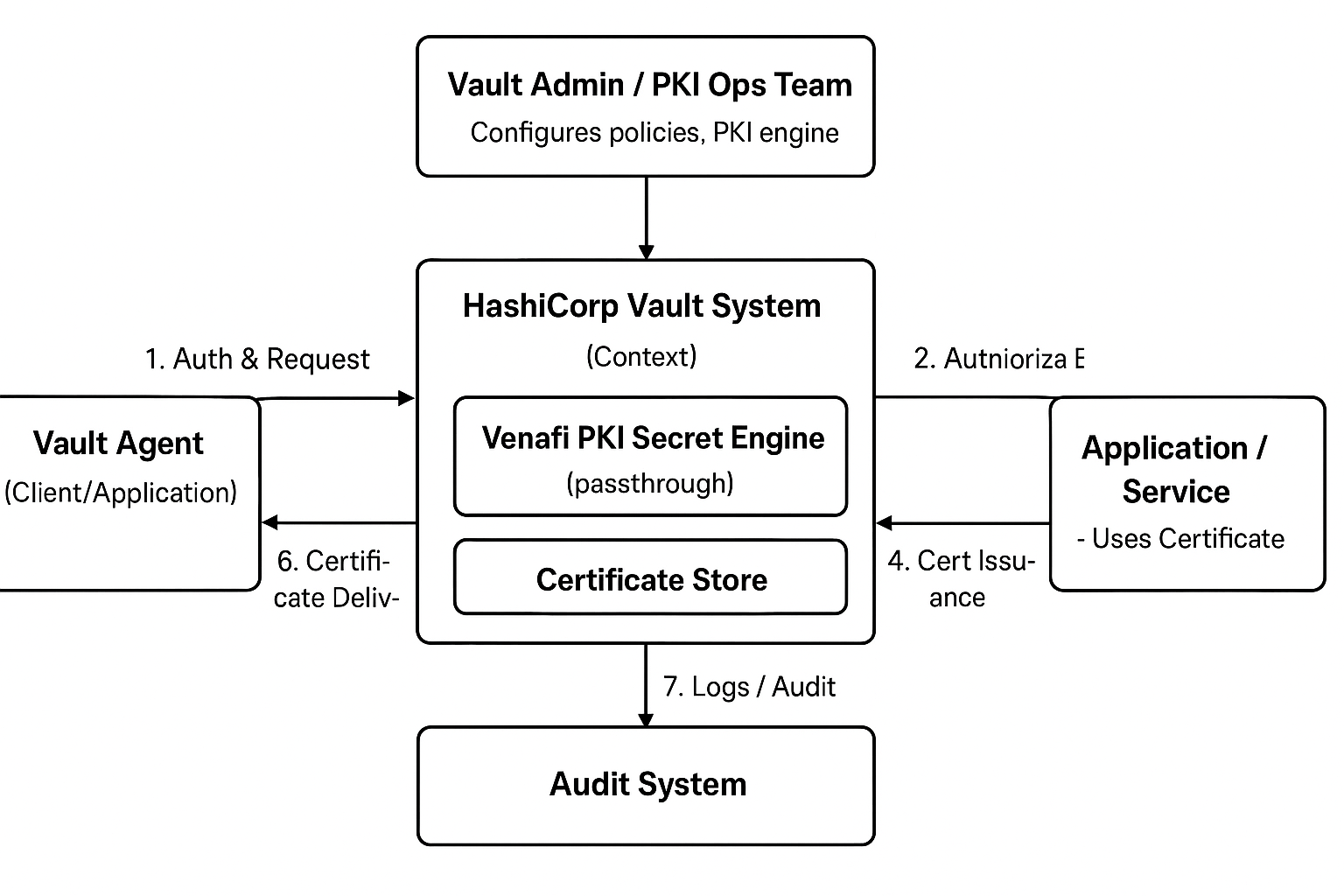
1. FR1: Vault Agent authenticates with Vault and requests or renews certificates.
2. FR2: Vault authenticates the agent and enforces access policies using Vault cert-auth method.
3. FR3: Vault forwards CSR via Venafi PKI Secret Engine to Venafi TPP.
4. FR4: Venafi TPP generates certificate and private key, returning them to Vault.
5. FR5: Vault stores certificate and key in its Certificate Store to avoid redundant issuance.
6. FR6: Vault Agent retrieves the certificate and key securely from Vault.
7. FR7: All operations are logged for audit and compliance.

### Non-Functional Requirements (NFRs)

|  |  |
| --- | --- |
| Category | Requirement |
| Performance | Certificate issuance should complete within 5 seconds under normal load. |
| Scalability | Support at least 100 concurrent certificate requests. |
| Availability | System uptime should be 99.9% or higher. |
| Security | All communications must use TLS 1.2+ with mutual authentication. |
| Confidentiality | Private keys never leave Vault or Venafi TPP unencrypted. |
| Auditability | All actions must be logged for traceability. |
| Maintainability | System configurations should be changeable without downtime. |
| Compliance | System must adhere to X.509, FIPS 140-2, and organizational PKI standards. |

## 3. Context View Diagram

The Context View Diagram represents the high-level interactions between external actors and the Vault system. It illustrates the main system boundaries, external entities, and the flow of data between them.



## 4. Context View Details

System: Vault-based Certificate Management System (HashiCorp Vault with Venafi PKI Secret Engine)  
  
Actors:  
 - Vault Agent: Requests and renews certificates.  
 - Venafi TPP: External PKI authority generating certificates and private keys.  
 - Application/Service: Consumes certificates from Vault Agent.  
 - Vault Admin / PKI Ops: Configures Vault PKI engine and policies.  
 - Audit System: Receives logs and compliance data.  
  
Key Interactions:  
 1. Vault Agent authenticates and requests certificates.  
 2. Vault authenticates and authorizes the agent.  
 3. CSR forwarded via Venafi PKI Engine to Venafi TPP.  
 4. Venafi TPP generates and returns certificate and key.  
 5. Vault stores certificate and key in Certificate Store.  
 6. Vault Agent retrieves the certificate.  
 7. Vault sends audit logs to the Audit System.