| Definition & Strategic Vision |
| --- |

Organizations face significant security and operational challenges within their technology estates due to continued reliance on legacy and fragmented management systems and processes. As technology environments become increasingly complex and dynamic, the speed and breadth of change is breaking historical control measures. Exposure to business risk is increasing because there are weak and inconsistent controls over the intent and scope of interactions between technology components.

An effective and fully realised Machine Identity and Trust (MIT) minimises human threats, secures autonomous hybrid-cloud setups, centralises dynamic access controls, and enhances auditing for improved compliance and risk management.

Objective pre-SKO

Demonstrating the value of automating the producer/consumer model for certificate management. The producer architecture will be consistent with our currently documented HashiCorp Validated Designs. This would include examples of an appropriate Vault architecture for integrating into existing CA’s / PKI infrastructure.

The initial consumer use case will be the integration of Vault PKI functionality into existing, or traditional, applications. How can these applications still benefit from a modern certificate management platform? We will use our existing Vault agent patterns to have the furthest reach.

Objective post-SKO

Demonstrating the consumer model for integration into modern Kubernetes services. How vault can leverage custom resource definitions (VSO) to automatically provide key material to dynamic, auto-scaling, or microservice architectures.

*[I suggest we do this K8s platform agnostic to reduce complexity. For instance, we should refrain from making unique demos for EKS, GKS, AKS, {{insert-other-k8s-here}}]*

| Customer Problem Statement |
| --- |

Modern organizations depend on a secure, resilient IT environment to safeguard sensitive data, maintain operational continuity, and drive business outcomes. However, outdated and fragmented PKI systems fail to meet the demands of today’s rapidly evolving technology landscape. This creates a cascade of challenges:

**Certificate Lifecycle Management:** Manual or poorly integrated processes for certificate renewal, issuance, and revocation lead to unexpected service outages and a lack of accountability.

**Lack of Visibility and Control:** Organizations lack a unified view of their certificate inventory, leaving them exposed to compliance failures, security vulnerabilities, and operational risks.

**Scaling Issues:** The rapid growth of digital assets, cloud adoption, and IoT devices has put a strain on legacy PKI systems, leading to performance bottlenecks, management inefficiencies, and rising costs.

**Operational and Business Risk:** Without automated, reliable PKI processes, businesses face an elevated risk of downtime, data breaches, and reputational damage, hindering their ability to innovate confidently.

Many organizations today rely on outdated or fragmented systems to manage their certificates and secure digital interactions. These systems weren’t built for the complexity and scale of modern IT environments, where technology changes rapidly, and security demands are higher than ever.

This often leads to:

* Unplanned Downtime and Disruptions: When certificates expire unexpectedly, critical business systems—like websites, applications, or customer portals—can go offline, costing time, money, and customer trust.
* Security Vulnerabilities: Without clear visibility and centralized control, certificates can become an entry point for cyberattacks, leaving your organization exposed to data breaches or compliance violations.
* Operational Inefficiency: Managing certificates manually or across disconnected tools wastes valuable IT resources, increasing costs and slowing down innovation.

The result is an elevated risk to your business operations, reputation, and bottom line. Organizations need a smarter, more scalable approach to managing PKI to keep pace with modern demands and stay ahead of risks.

**[Chris to add details on his view. Have a section for problem statements, and high level solution. Can you add a few lines around the Enterprise value prop as well?]**

| Sales Problem Statement |
| --- |

In collaboration with TFO, the Value Engineering team went through an effort to requalify the value obtained by our customers. This effort included building a new weighted scoring methodology for product use cases, plotting those scores against a quadrant ranging from low value/low stickiness to high value/high stickiness, and mapping our current customers against this new model. This effort clearly displayed a lack of differentiation between individual use cases and the holistic potential value proposition when multiple use cases are consumed to obtain a strategic outcome. This effort is to align multiple use cases from the HashiCorp Maturity Model into more consumable outcomes that align to our longterm strategic vision.

If customers are not realizing the value proposition and do not have many use cases consumed that align to our value pillars, risk of reduced, or churned, consumption is possible. Accounts will be scored and risk will be calculated for customers that are not realizing the value of the defined outcomes.

These following assets will be used to prepare the field for this technical motion.

**Tactical One Pager:** Define

**Discovery / Objection Handling:** Define

**2nd Call Deck:** Define

**Demo Creation & Recording:** Define

**Workshop Slides:** Define

**Validated Pattern:** Define

| Component |
| --- |

The following sub-usecases are applicable to realize the value provided by auto-renewed certs.

| Sub UseCase | References | Workshop | DDR |
| --- | --- | --- | --- |
| * Public Key Infrastructure | **HVD**  [PKI Secrets Engine](https://developer.hashicorp.com/validated-designs/vault-operating-guides-scaling/pki-secrets-engine) [Key lifecycle management](https://developer.hashicorp.com/validated-designs/vault-operating-guides-scaling/key-lifecycle-management) [Producer / Consumer - Overview](https://developer.hashicorp.com/validated-designs/vault-operating-guides-adoption/people-and-process#producers)  **Public** [PKI - Secrets Engines: Considerations](https://developer.hashicorp.com/vault/docs/secrets/pki/considerations)  [Managed Keys](https://developer.hashicorp.com/vault/docs/enterprise/managed-keys)  **Internal** [PKI design considerations](https://docs.google.com/document/d/1ZFE6DWxmzH2wLn85U4JVXhViAfhtQS035HEXhzF_Nsc/edit?tab=t.0#heading=h.gjdgxs) |  | [Guilherme Pamplona Santos](mailto:guilherme.pamplonasantos@hashicorp.com)[demo](https://github.com/hashicorp/demo-vault-auto-renewed-certs/tree/main) |
| * App modernization | [Connect Apps using Vault Templates](https://developer.hashicorp.com/validated-designs/vault-operating-guides-standardization/vault-agent-templates)  [Vault PKI Consumption Patterns](https://docs.google.com/presentation/d/1tdcRlk4c2T_x2akDZr7ljCg776kcD9iLkhCeX3jX5Mk/edit#slide=id.g1461e01e411_0_7017)  [Vault Quick Start Workshop](https://docs.google.com/presentation/d/1fMW4cWn3BMagEbKifRTE3lEoy5Ehiena9r30oWbte7A/edit#slide=id.g30c70b8241e_0_4263)  [Revolutionizing Certificate Management with ACME and Vault](https://docs.google.com/presentation/d/1COyhvjd2ZmIDUiBfeqK6onvHmOwhf62-q5ZYXtoQdlU/edit?usp=sharing) |  |  |
| * Trusted Identity Providers | [Authentication for people](https://developer.hashicorp.com/validated-designs/vault-operating-guides-adoption/authentication-for-people) [Authentication for applications](https://developer.hashicorp.com/validated-designs/vault-operating-guides-adoption/authentication-for-applications) |  |  |
| * Access controls | [Namespaces](https://developer.hashicorp.com/vault/docs/enterprise/namespaces)  [Control Groups](https://developer.hashicorp.com/vault/docs/enterprise/control-groups) |  |  |

Need to add links to existing content that can be used….