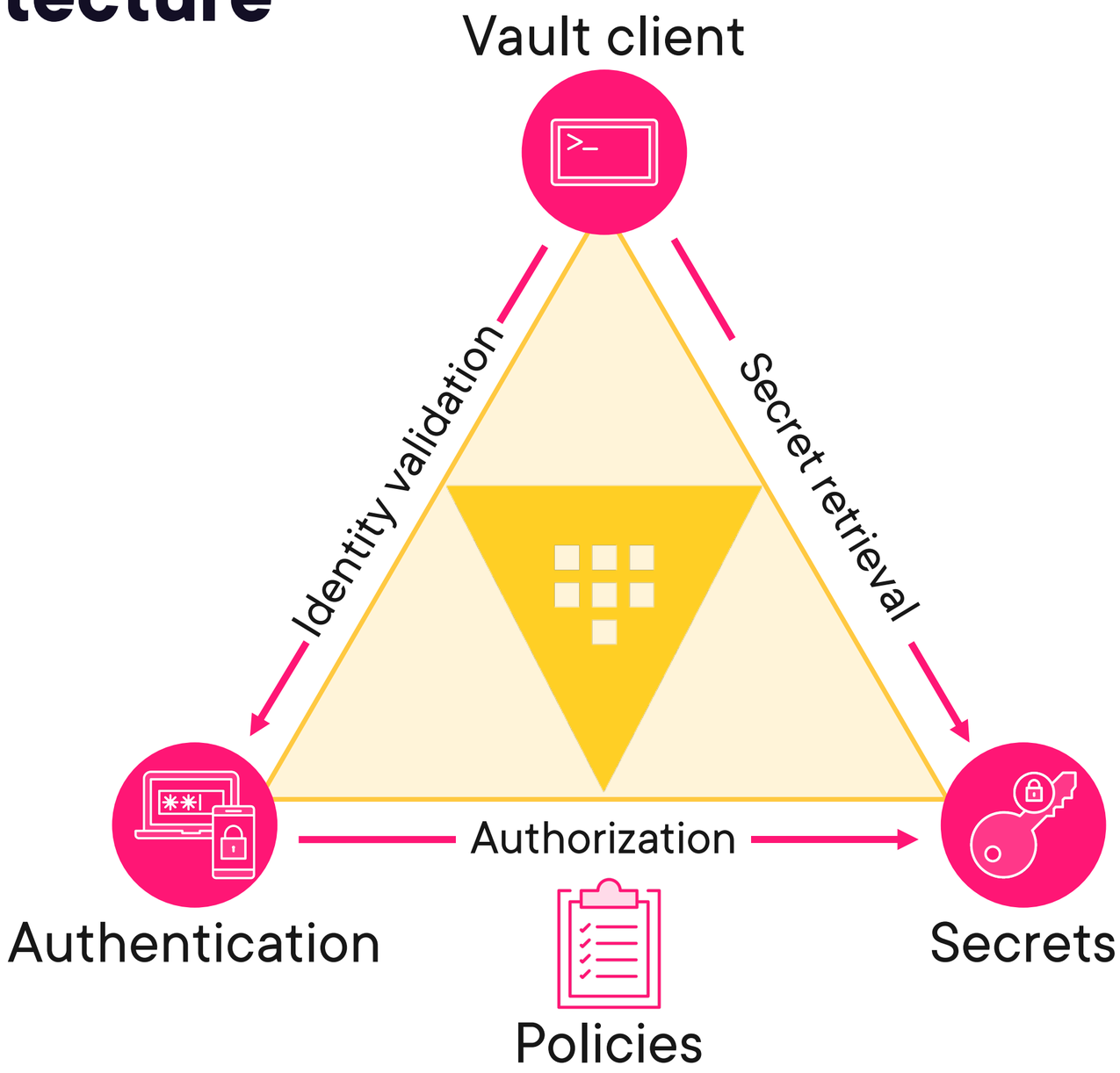
Secrets Engines for Vault Associate (003)

Secrets Engines Overview

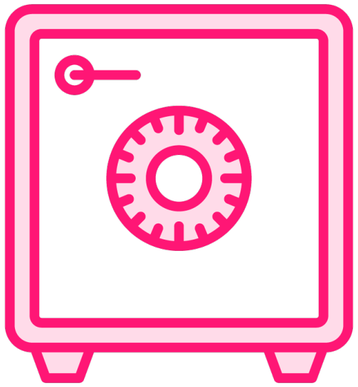
Ned Bellavance
HashiCorp Certified Instructor

@nedinthecloud | nedinthecloud.com

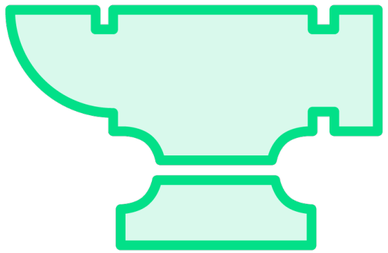
Vault Architecture



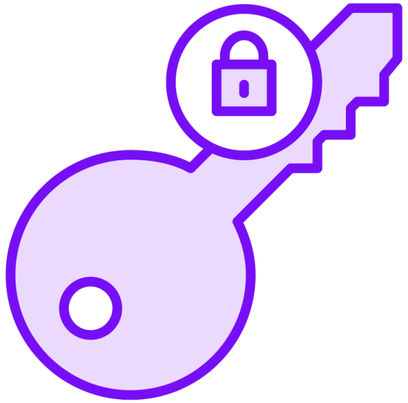
Secrets Engines



Store data



Generate data



Encrypt data

Secrets Engine Examples

Key Value – store arbitrary key value pairs

Database – create and manage database credentials

PKI – automate certificate enrollment

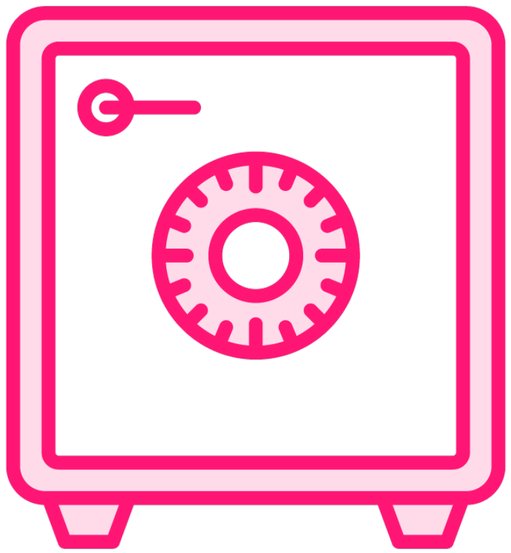
Transit – provide encryption as a service

Secret Types

Static secrets

Dynamic secrets

Static Secrets



Long-lived and seldom change

No expiration date

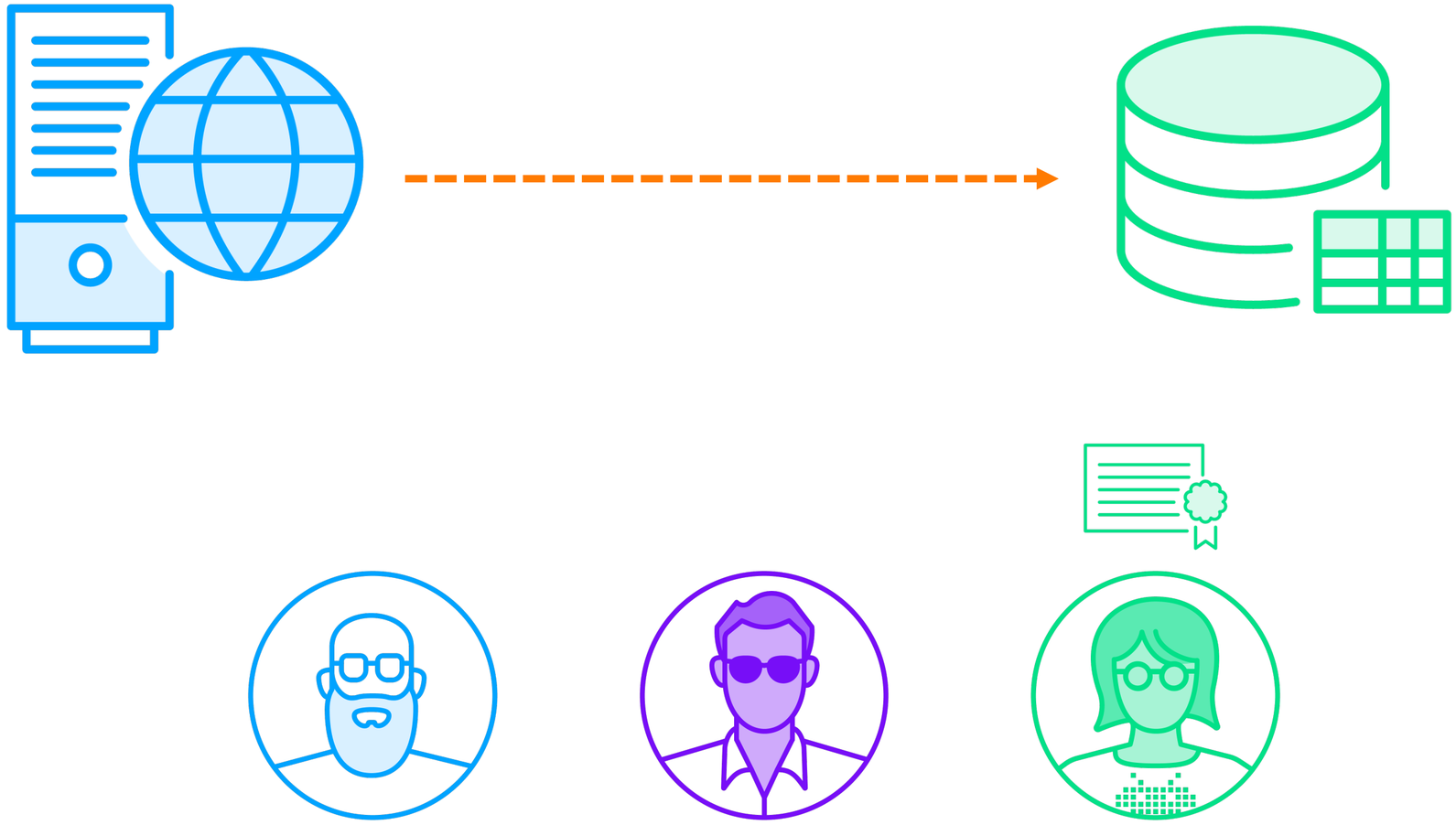
Manual updates

Examples

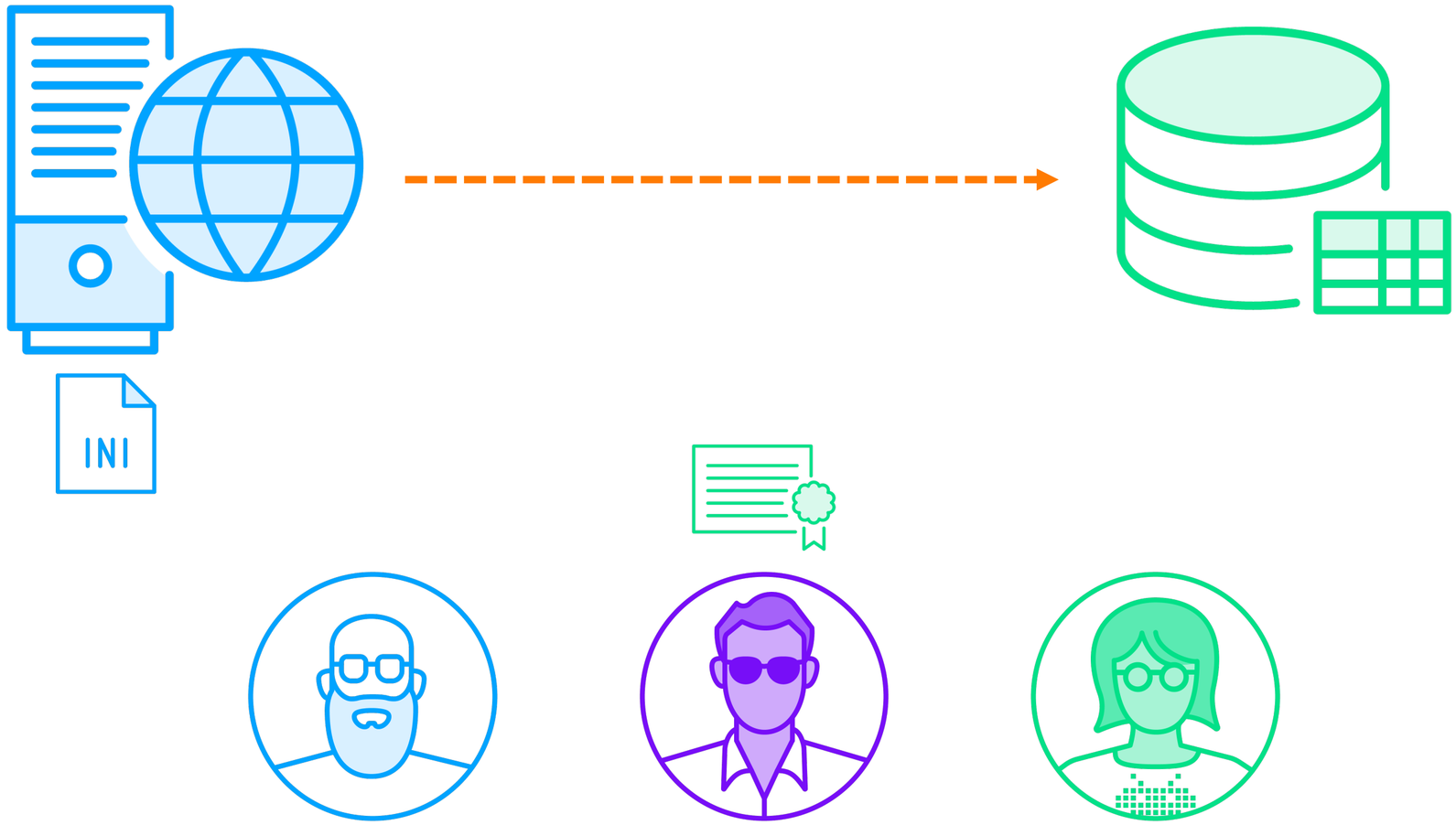
- API keys
- 3rd party tokens
- PGP keys
- Username/password

Stored in Key Value engine

Static Secret Example



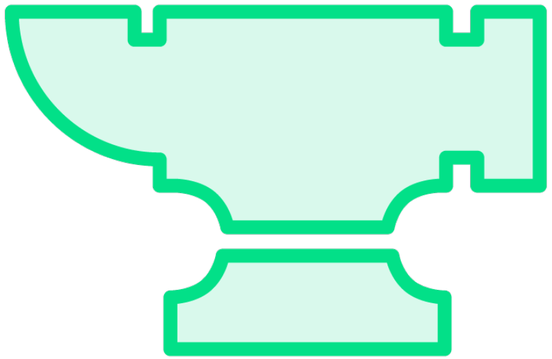
Static Secret Example



Pros and Cons

Static secrets	vs.	Dynamic secrets
Easy to manage		
Centralized storage		
Manual workflow		
Credential reuse		
Hard to trace		
Complex rotation		

Dynamic Secrets



Generated on-demand

Short lifetime with expiration

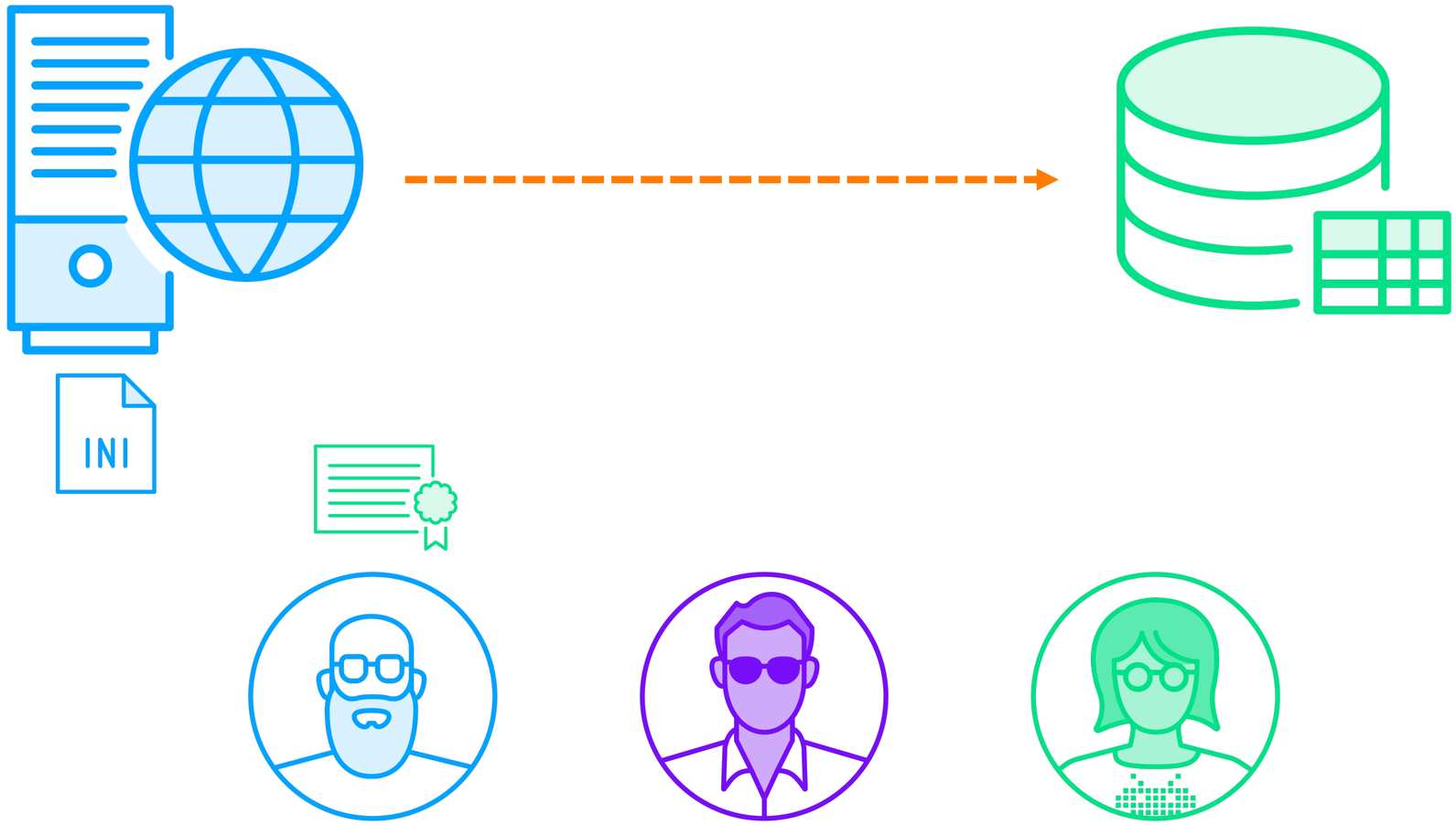
Automatic rotation

Examples

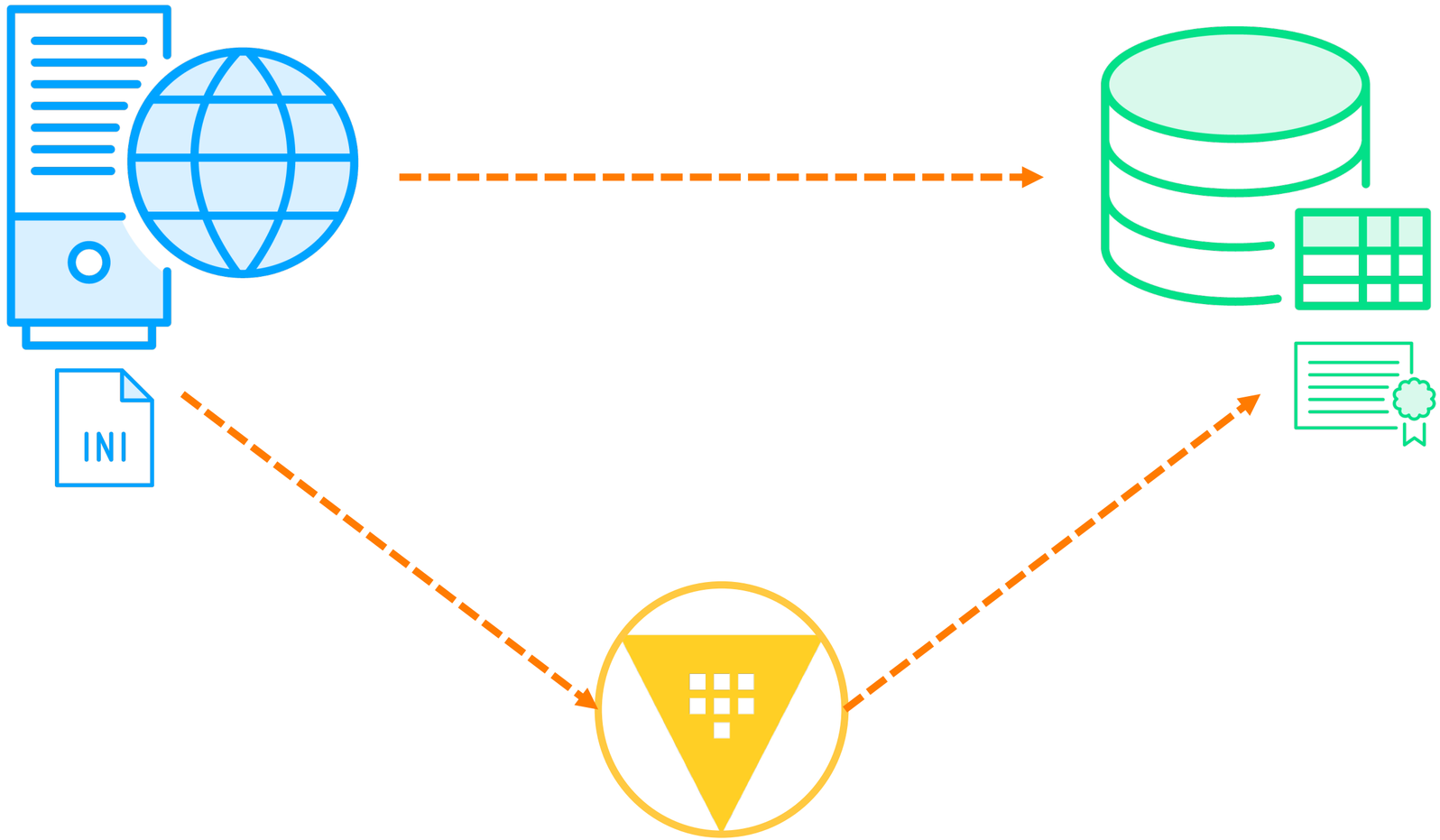
- Database credentials
- Cloud credentials
- TLS certificate

Multiple secrets engines

Dynamic Secret Example



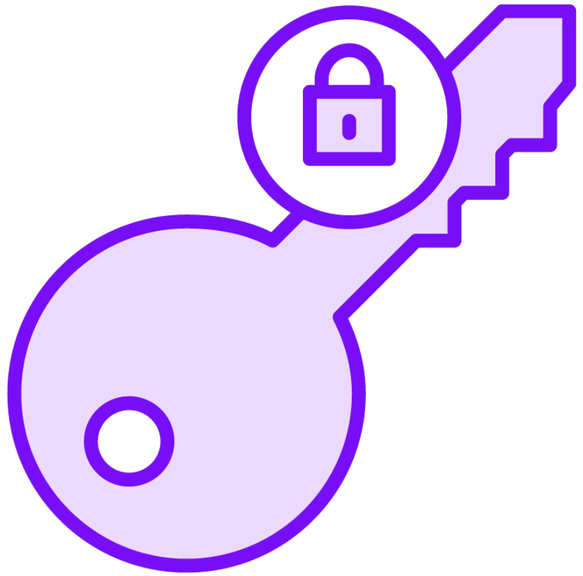
Dynamic Secret Example



Pros and Cons

Static secrets	vs.	Dynamic secrets
Easy to manage		More complex to setup
Centralized storage		Credential not stored
Manual workflow		Automated workflow
Credential reuse		Unique credentials
Hard to trace		Simplified tracing
Complex rotation		Automated rotation

Transit Engine



Encryption as a service

Vault performs operations

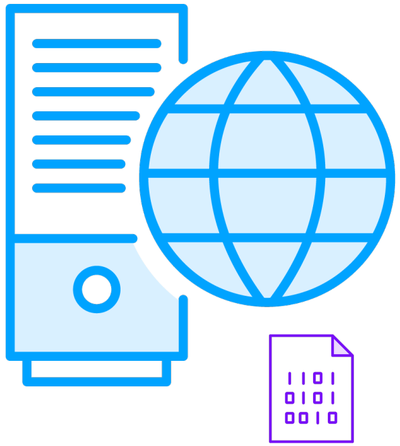
Data is not stored in Vault

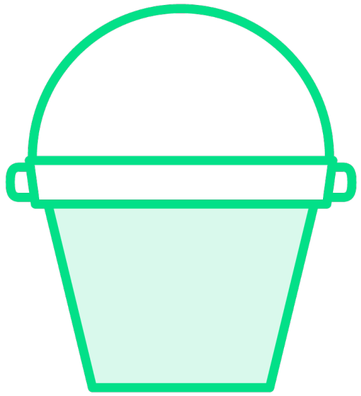
Multiple cryptographic operations

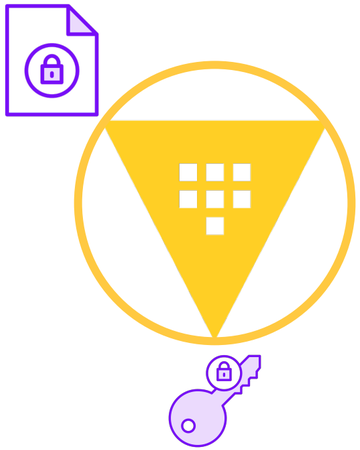
Vault manages the keys

Multiple key types supported

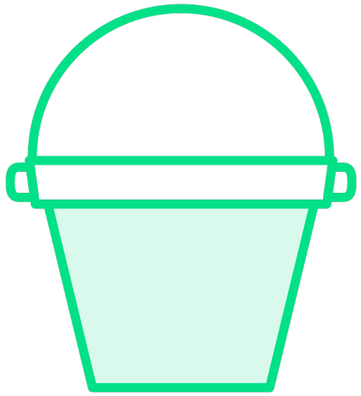
Transit Engine Example

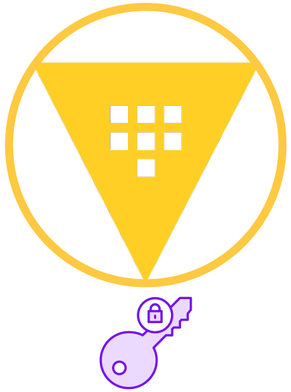






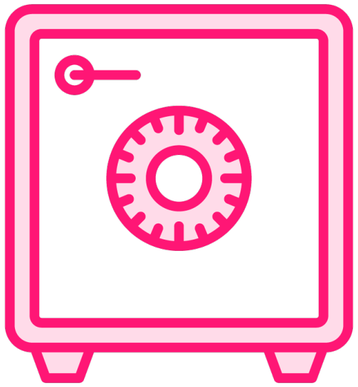
Transit Engine Example



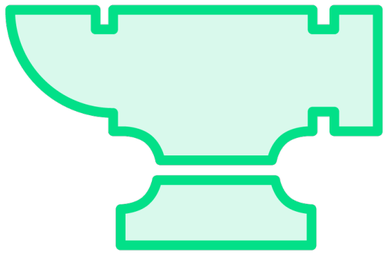


Choosing a Secrets Engine

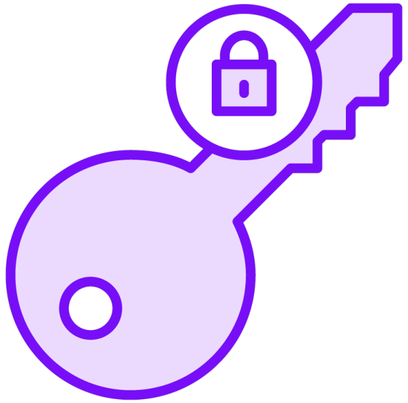
Secrets Engines



Store data



Generate data



Encrypt data

Secrets Engine Categories

Cloud

Database

HashiCorp

Internal

Identity

Certificate

Scenario One

Requirements

- Supply MySQL services
- Receive credentials on-demand
- Automatic credential management

Solution

- Database secrets engine with MySQL plugin
- AppRole authentication

Scenario Two

Requirements

- Store API keys for microservices
- Versioned and retrieved by multiple sources
- Generated by developers

Solution

- Version 2 of the KV engine
- AWS auth for application
- GitHub auth for developers

Scenario Three

Requirements

- Storing customer PII in blob storage
- Encrypt data before storing

Solution

- Transit secrets engine
- Azure auth method