Giant Swarm

Introduction to HashiCorp's Vault

September 30, 2021



Christian Bianchi
SRE @ Giant Swarm

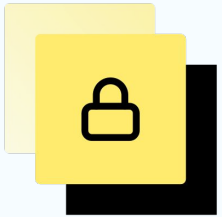
Agenda

- What is Vault
- Architecture
- Use cases
- How Giant Swarm uses Vault
- Questions

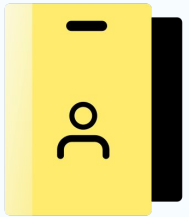

Giant Swarm
What is HashiCorp’s Vault?
KUBERNETES



Secrets Management



Data Encryption



Identity-Based Access



Secrets Management

Secret

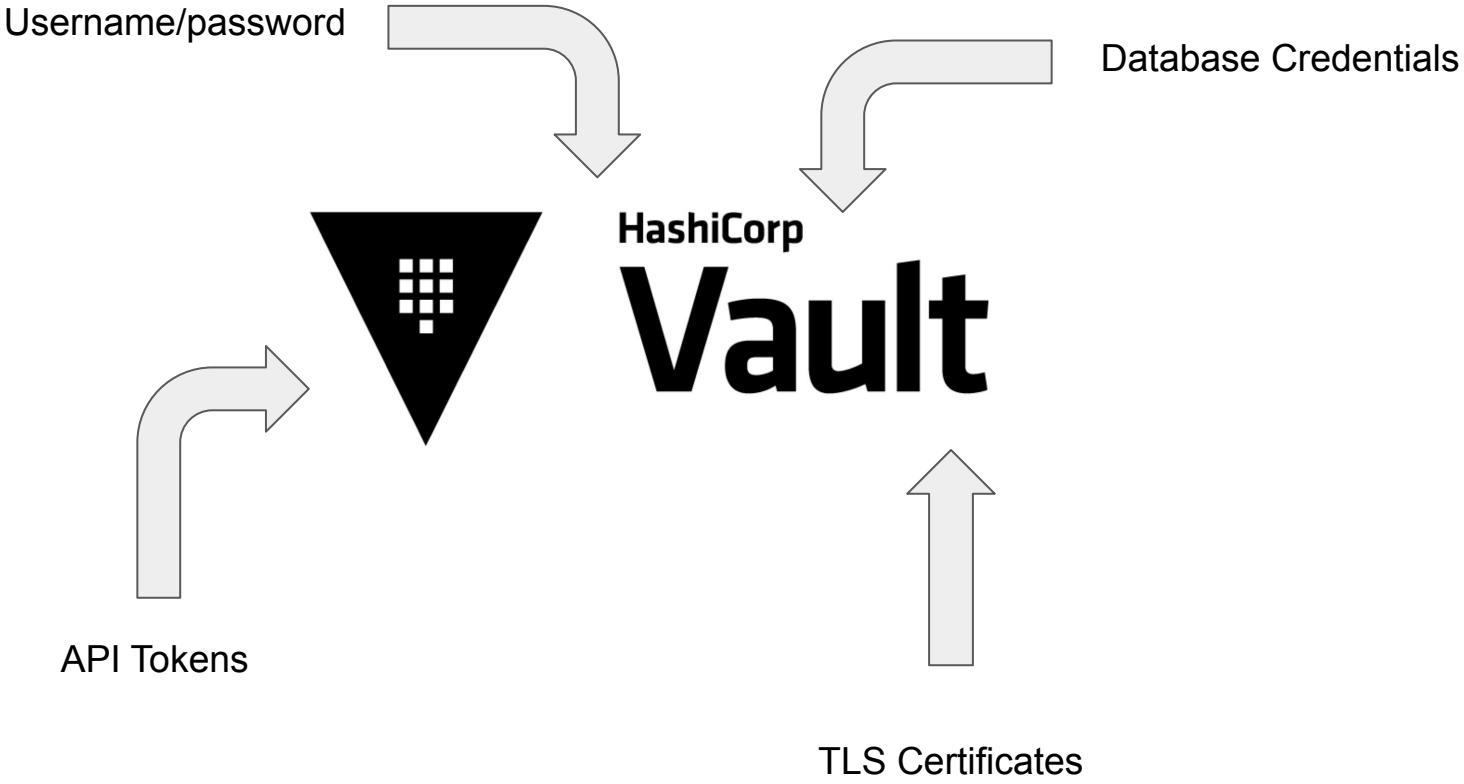
> Any data that can be used for authentication and authorization.
>
> *- Armon Dadgar, HashiCorp's co-founder and CTO*

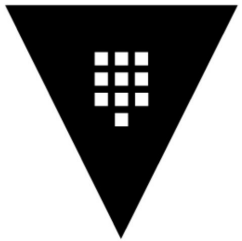


The Secrets Sprawl Problem

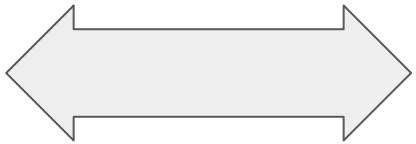
- Secrets are stored everywhere
  - Hard-coded in the applications source code
  - Config management
- They eventually end up in the VCS
- Available to everybody without access control

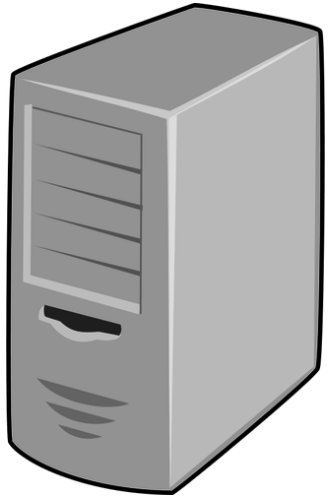


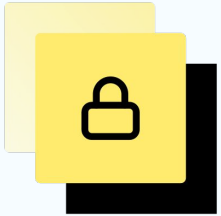

Username/password
Database Credentials
HashiCorp
Vault
API Tokens
TLS Certificates



HashiCorp
Vault

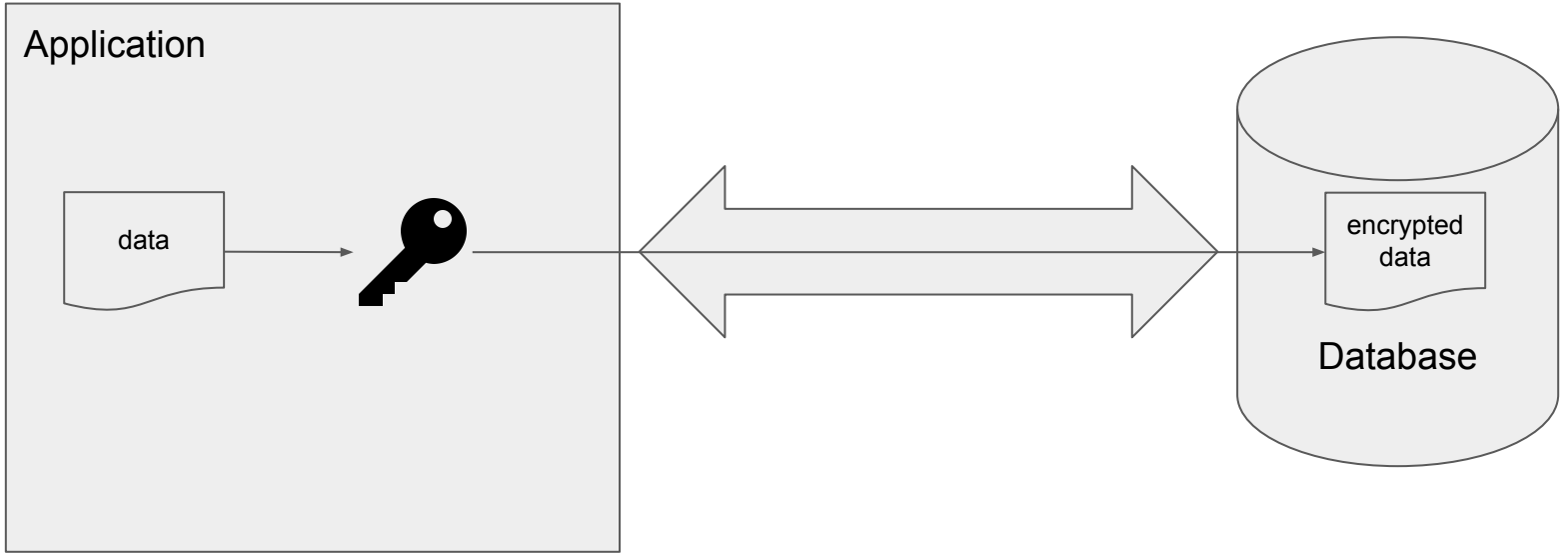




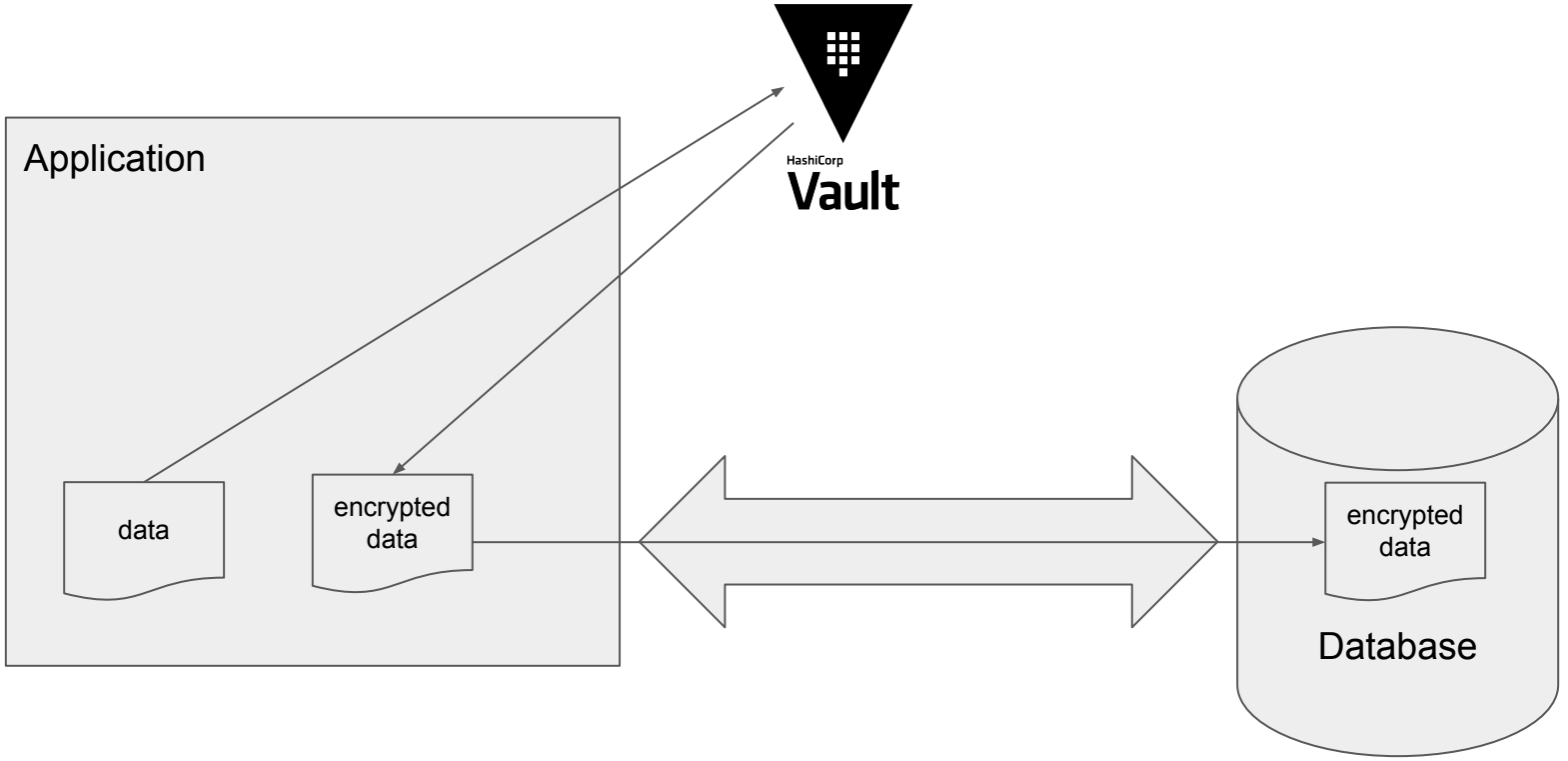


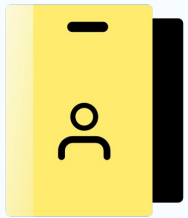
Data Encryption

Data Encryption - Without Vault

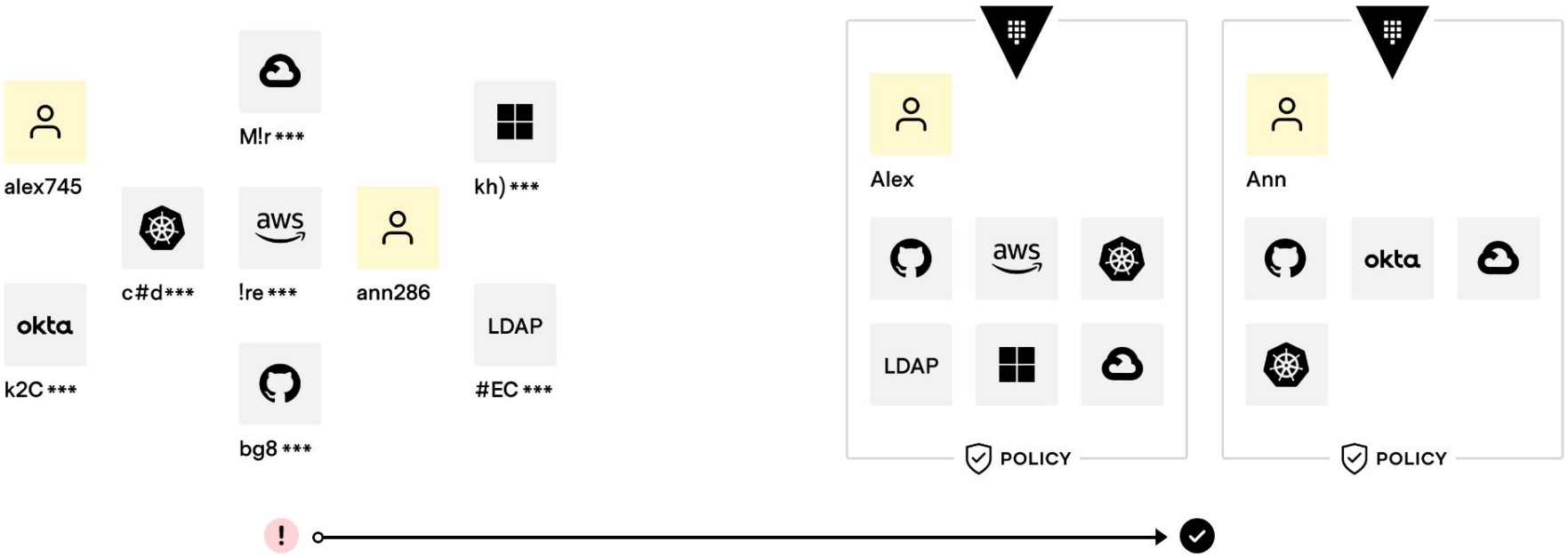


Data Encryption - With Vault

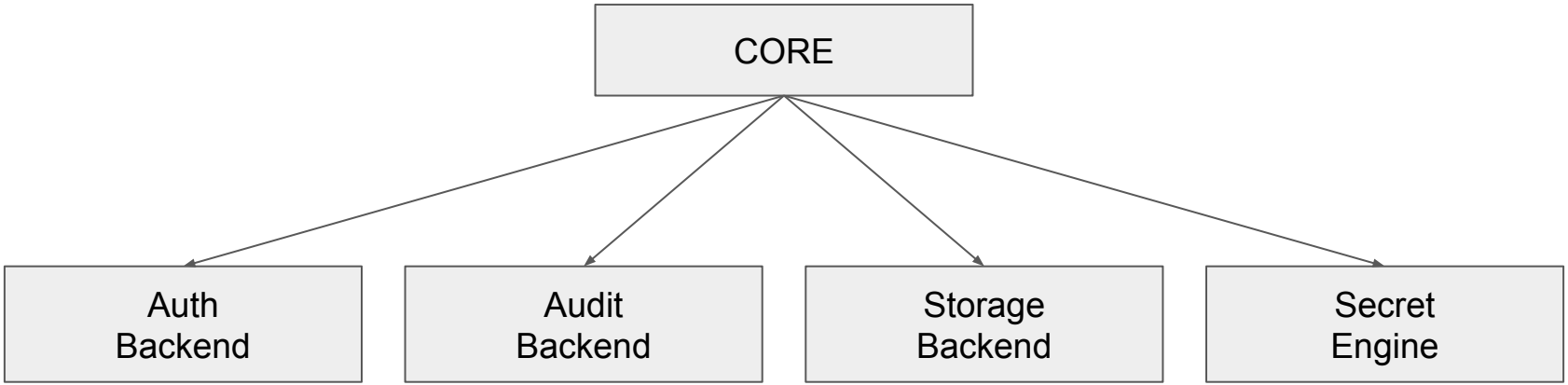




Identity-Based Access


alex745
okta
k2C***
c#d***
M!r***
aws
!re***
bg8***
ann286
kh)***
LDAP
#EC***
Alex
aws
LDAP
POLICY
Ann
okta
POLICY


Giant Swarm
Architecture
KUBERNETES



Username/Password
AWS
Azure
Token
GitHub
Kubernetes
...

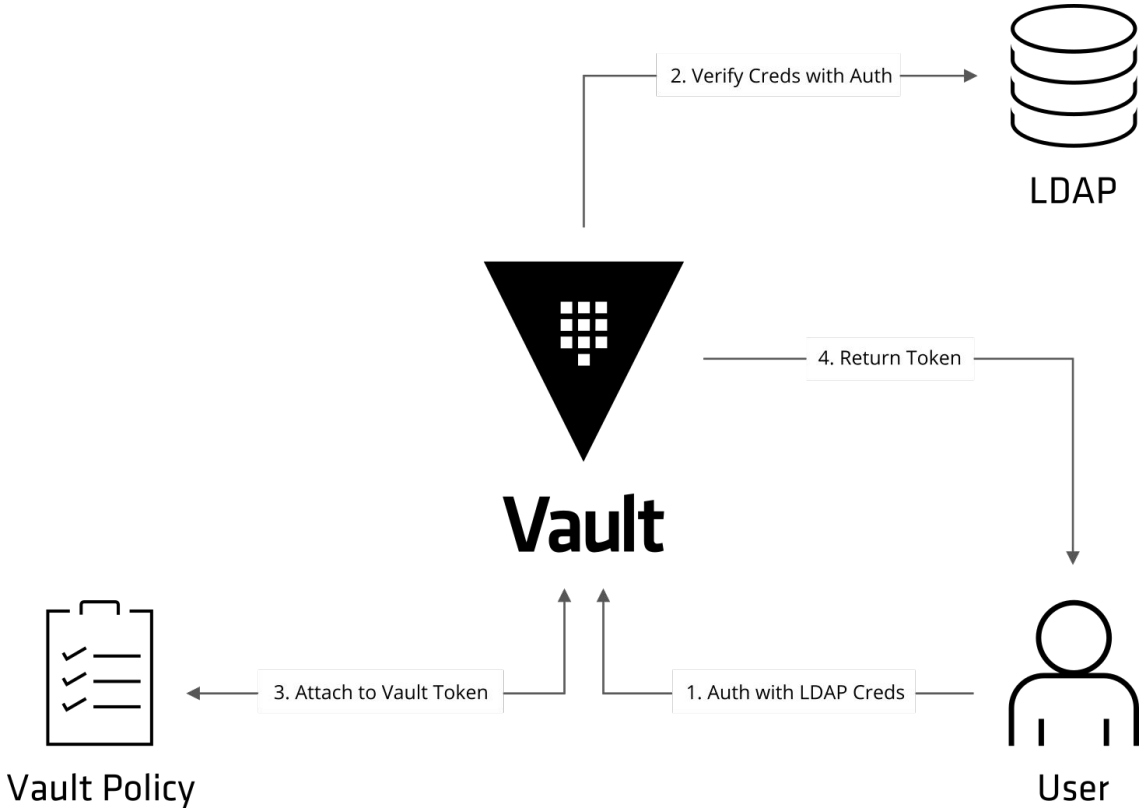
File
Syslog
...

Azure
ETCD
S3
PostgreSQL
MySQL
...

Azure
AWS
Databases
Key/Value
SSH
PKI
...


JSON/HTTP
HashiCorp
Vault

Access Control



Access Control - Example

Read Secret Version

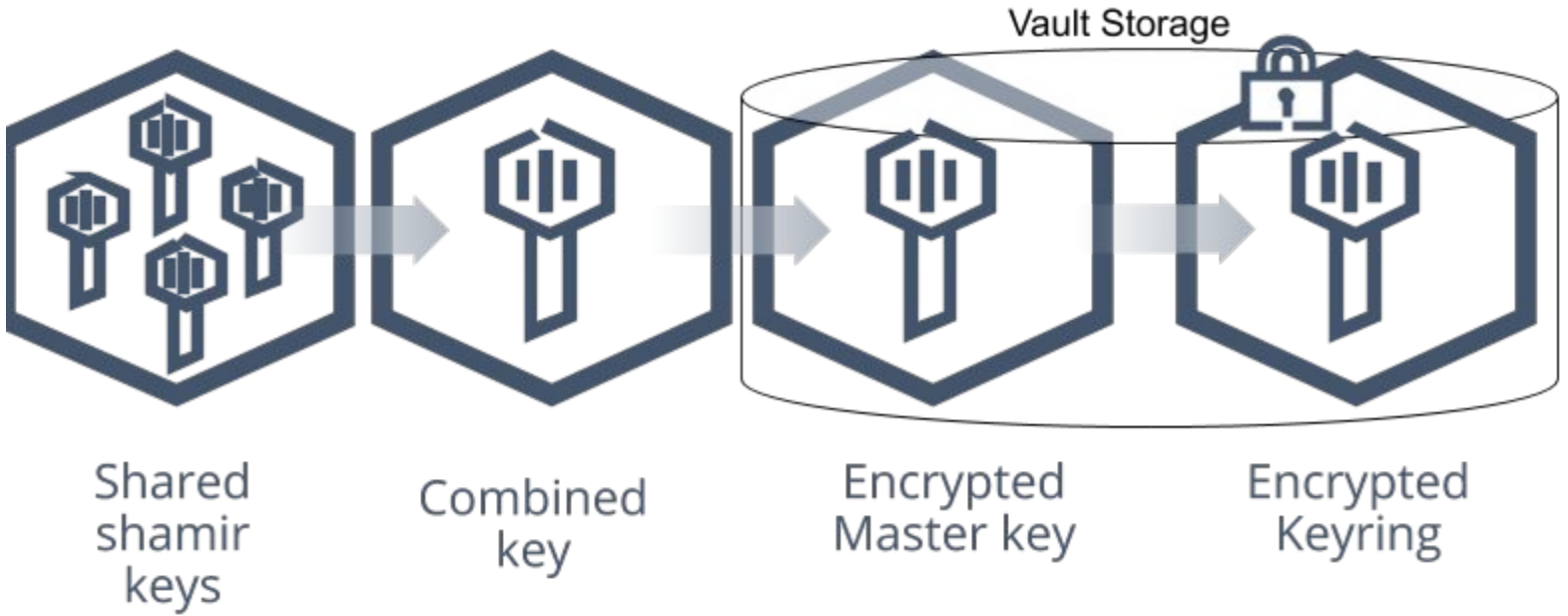
This endpoint retrieves the secret at the specified location.

Method	Path
`GET`	`/secret/data/:path?version=:version-number`

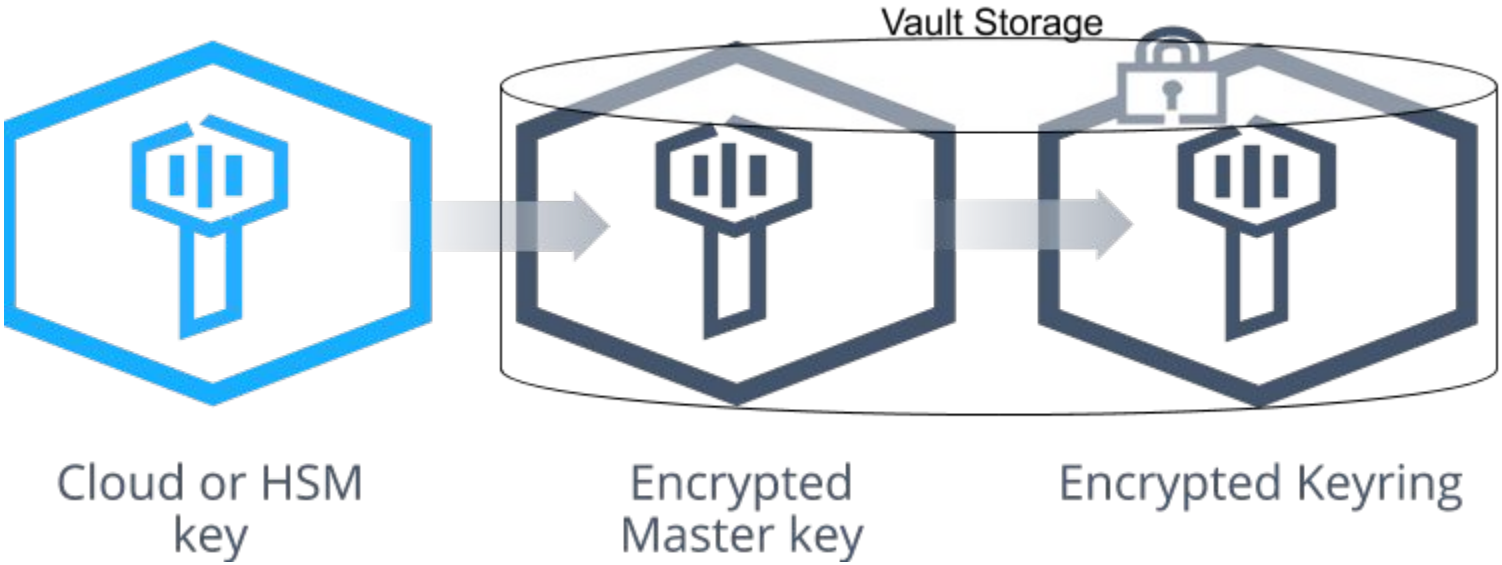
```
path "secret/data/*" {
  capabilities = ["read"]
}
```

Capability	**HTTP method**
create	POST/PUT
read	GET
update	POST/PUT
delete	DELETE
list	LIST
deny, sudo	

Sealing

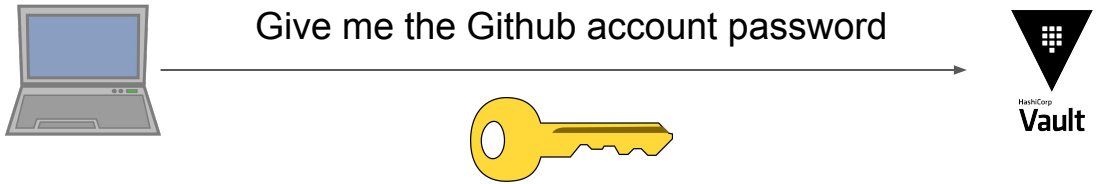

Vault Storage
Shared shamir keys
Combined key
Encrypted Master key
Encrypted Keyring

Auto Unseal


Vault Storage
Cloud or HSM key
Encrypted Master key
Encrypted Keyring


Giant Swarm
Use cases
KUBERNETES

Shared Employee Credentials

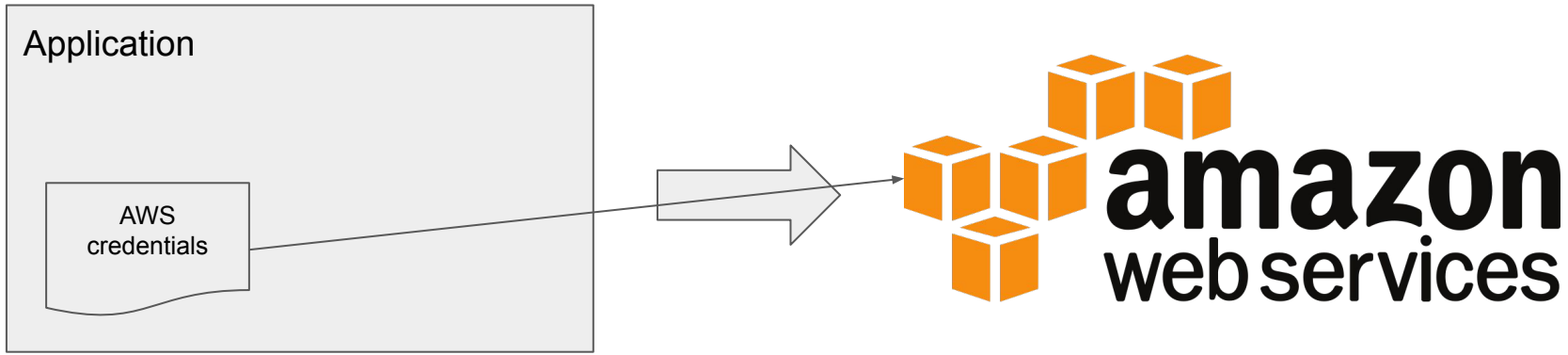


Dynamic Secrets

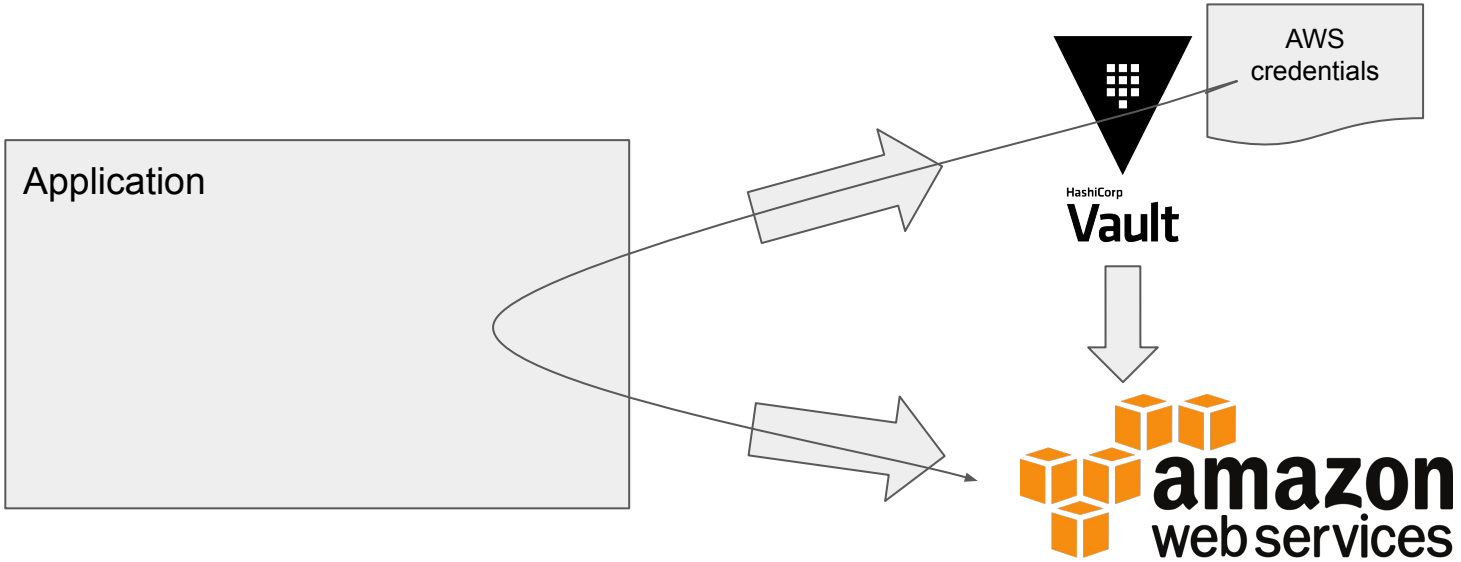
- Cloud provider APIs
- Databases



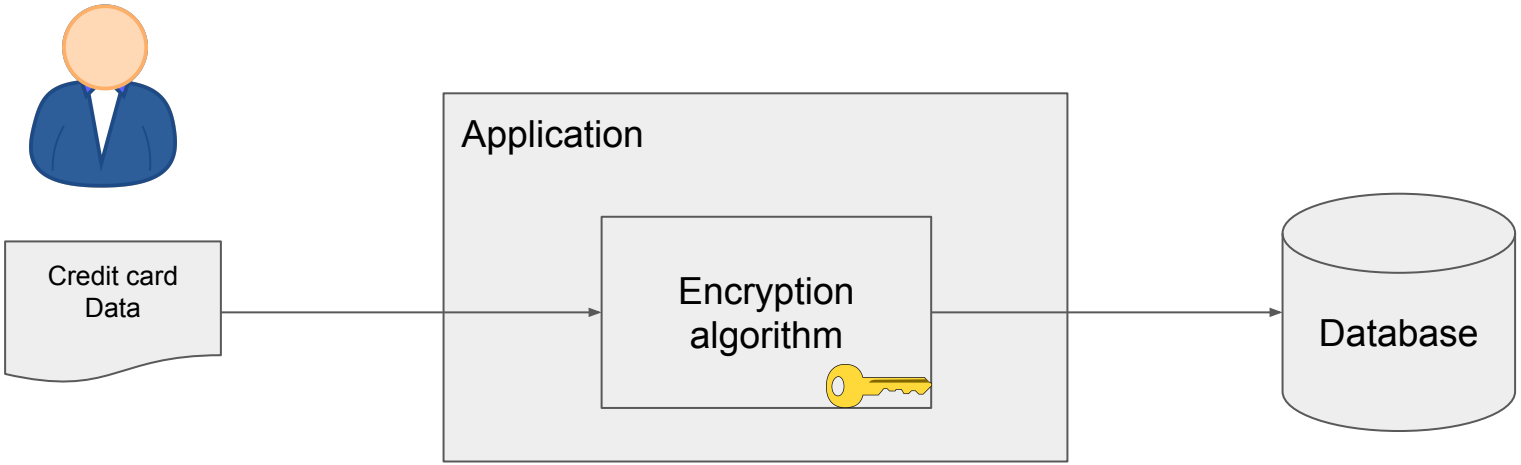
Dynamic Secrets - Without Vault



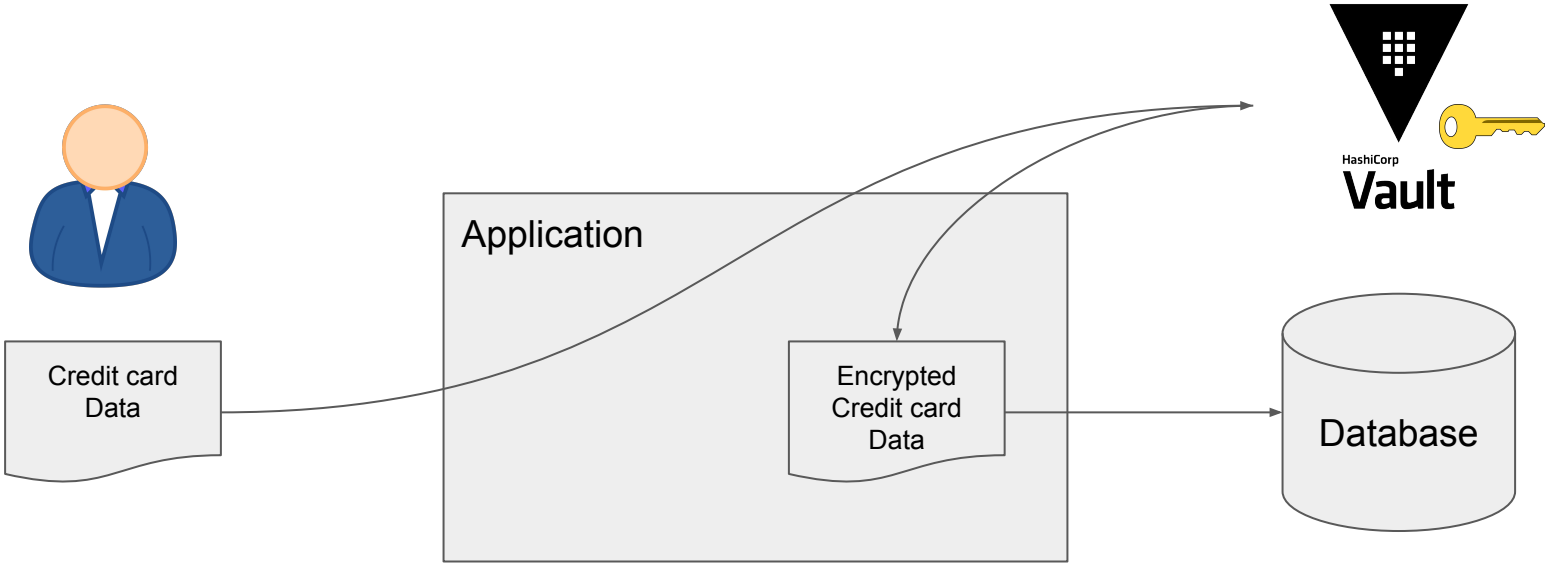
Dynamic Secrets - With Vault



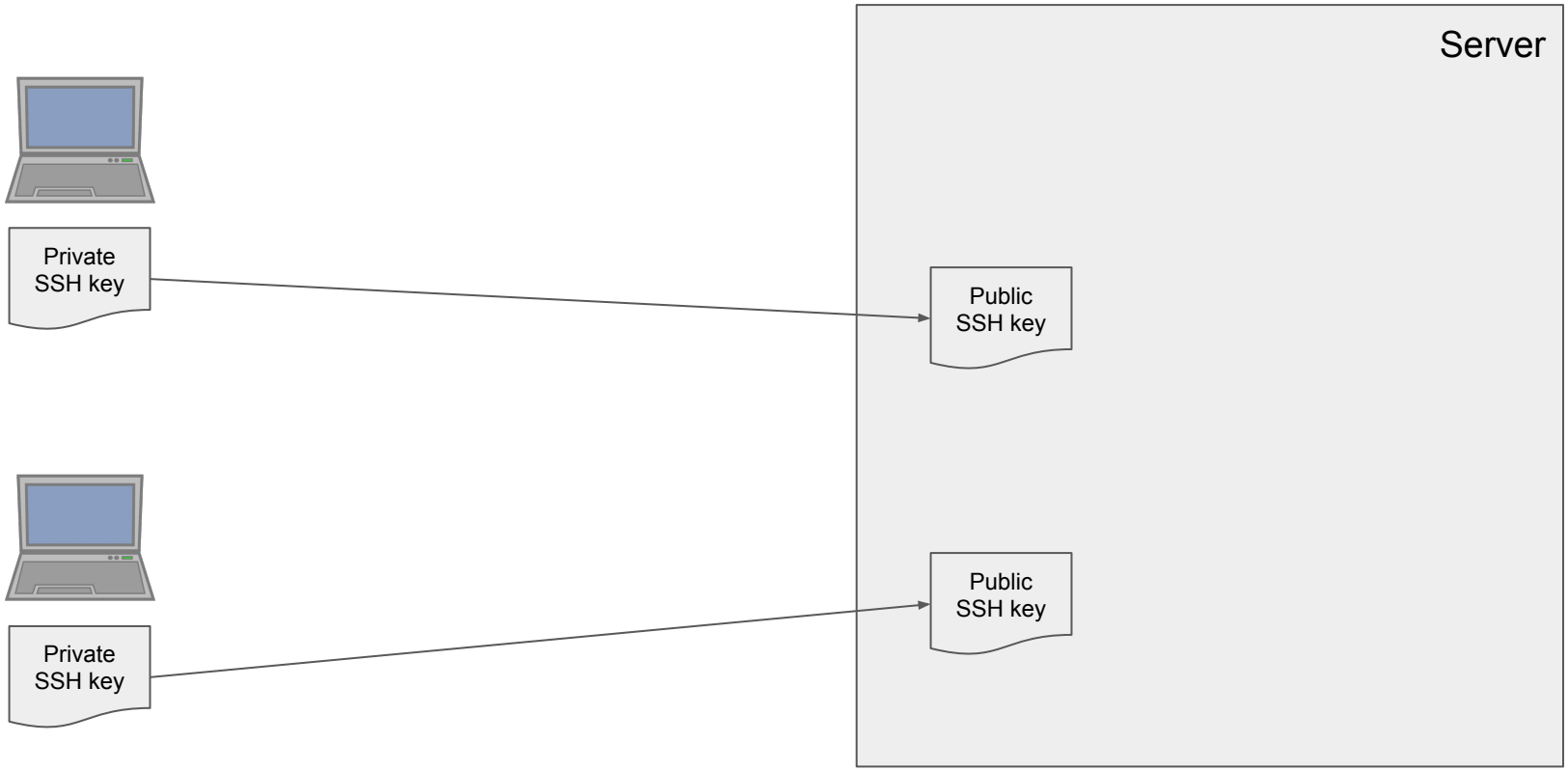
Data Encryption - Without Vault



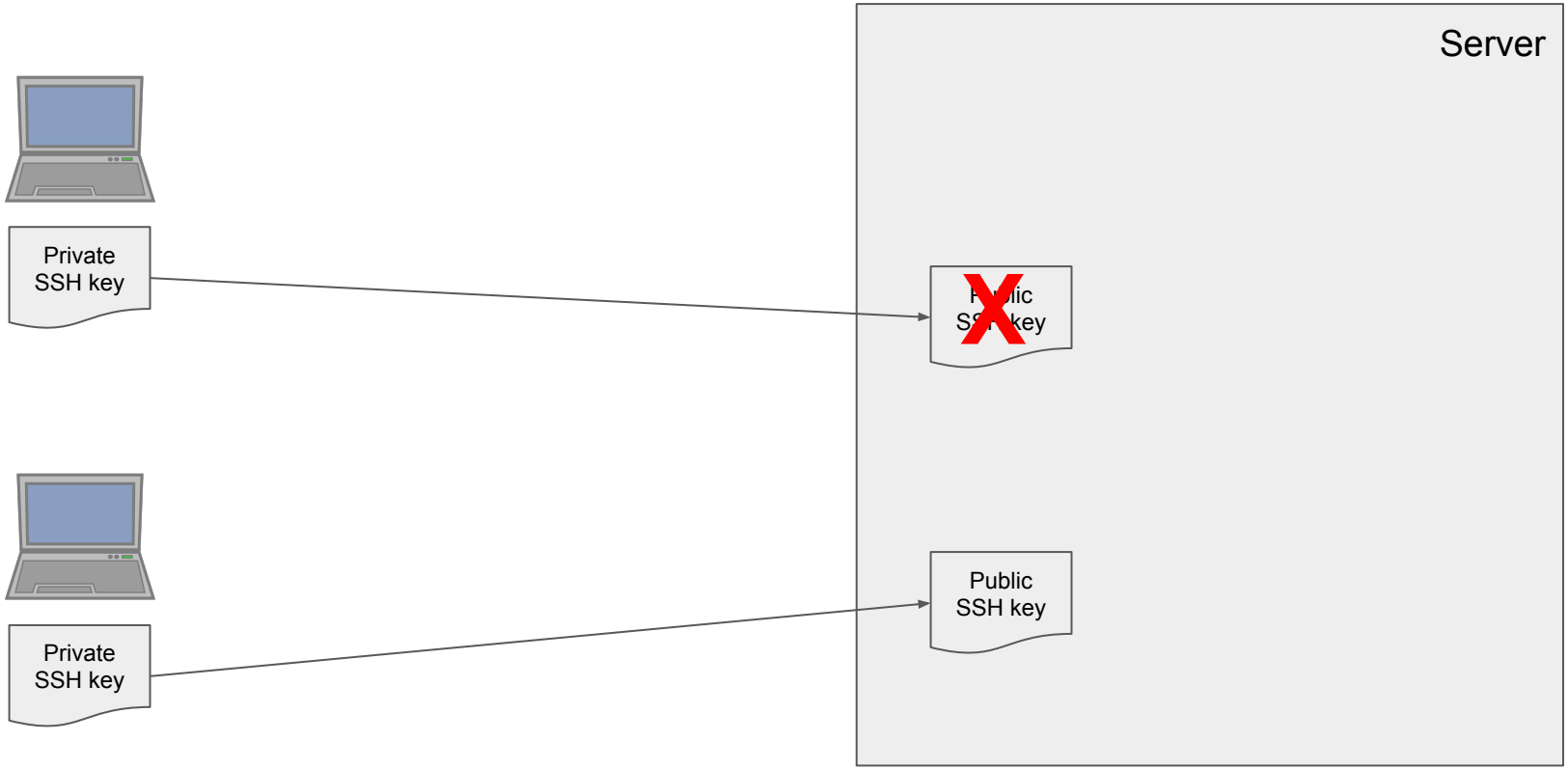
Data Encryption - With Vault



SSH


Server
Private
SSH key
Public
SSH key
Private
SSH key
Public
SSH key

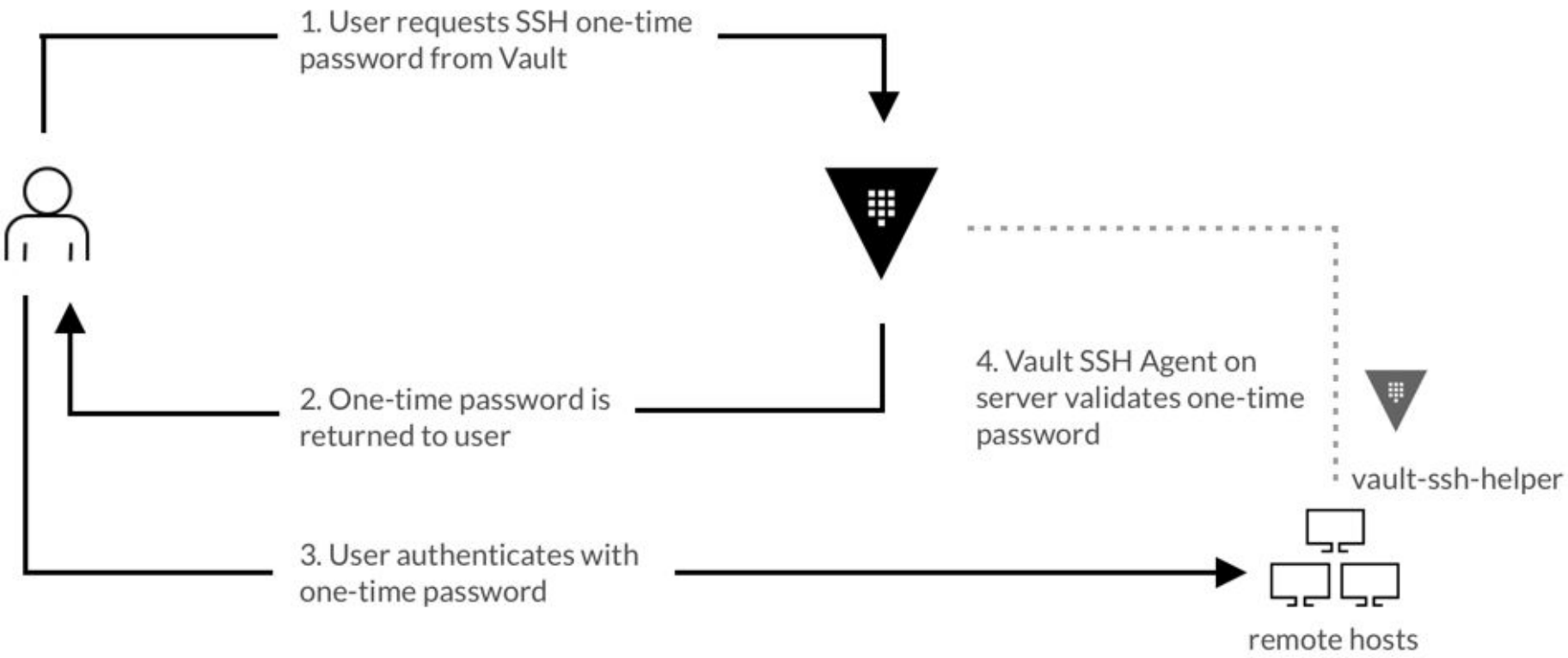
SSH


Server
Private
SSH key
Public
SSH key
Private
SSH key
Public
SSH key

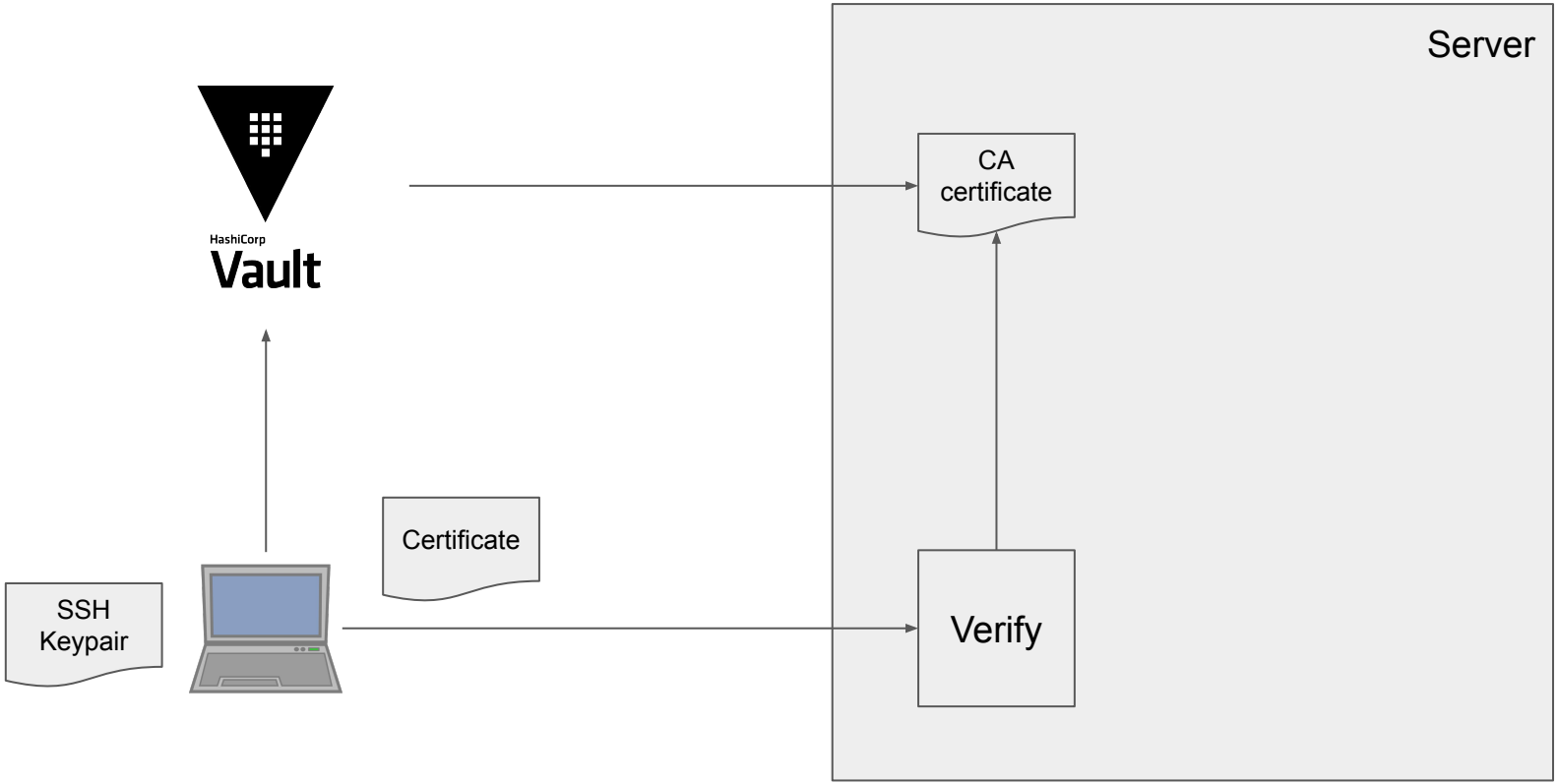
SSH

- One-Time SSH Passwords
- Signed SSH Certificates

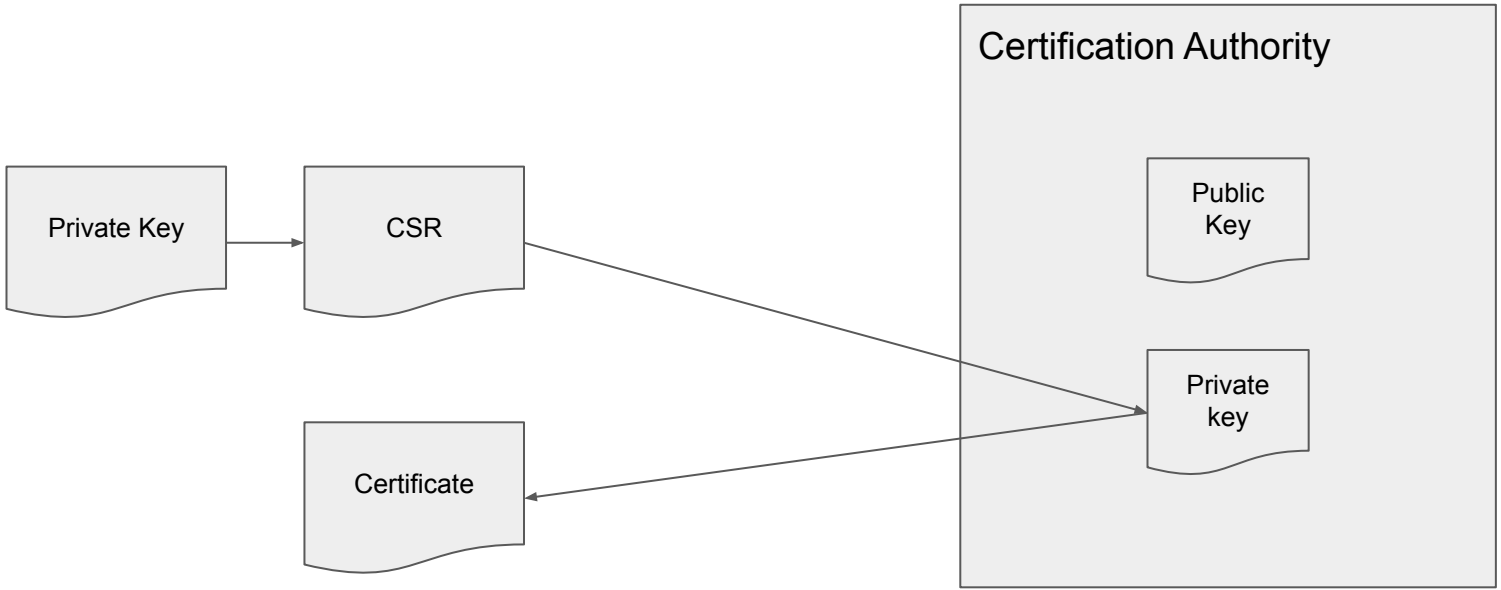
One-Time SSH Passwords



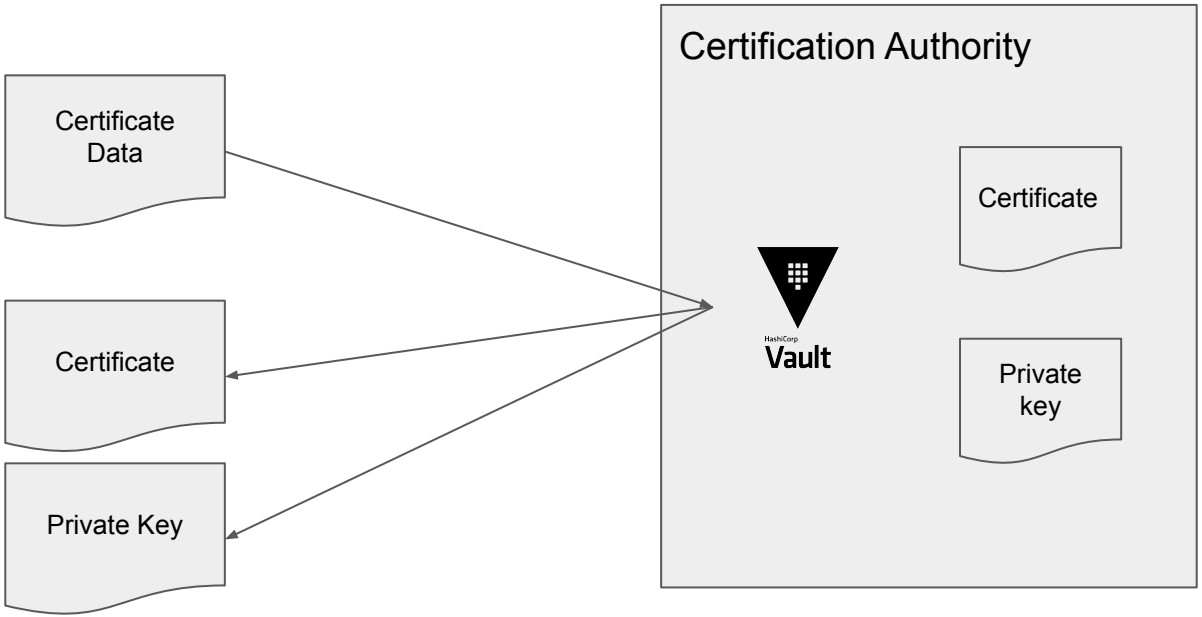
Signed SSH Certificates



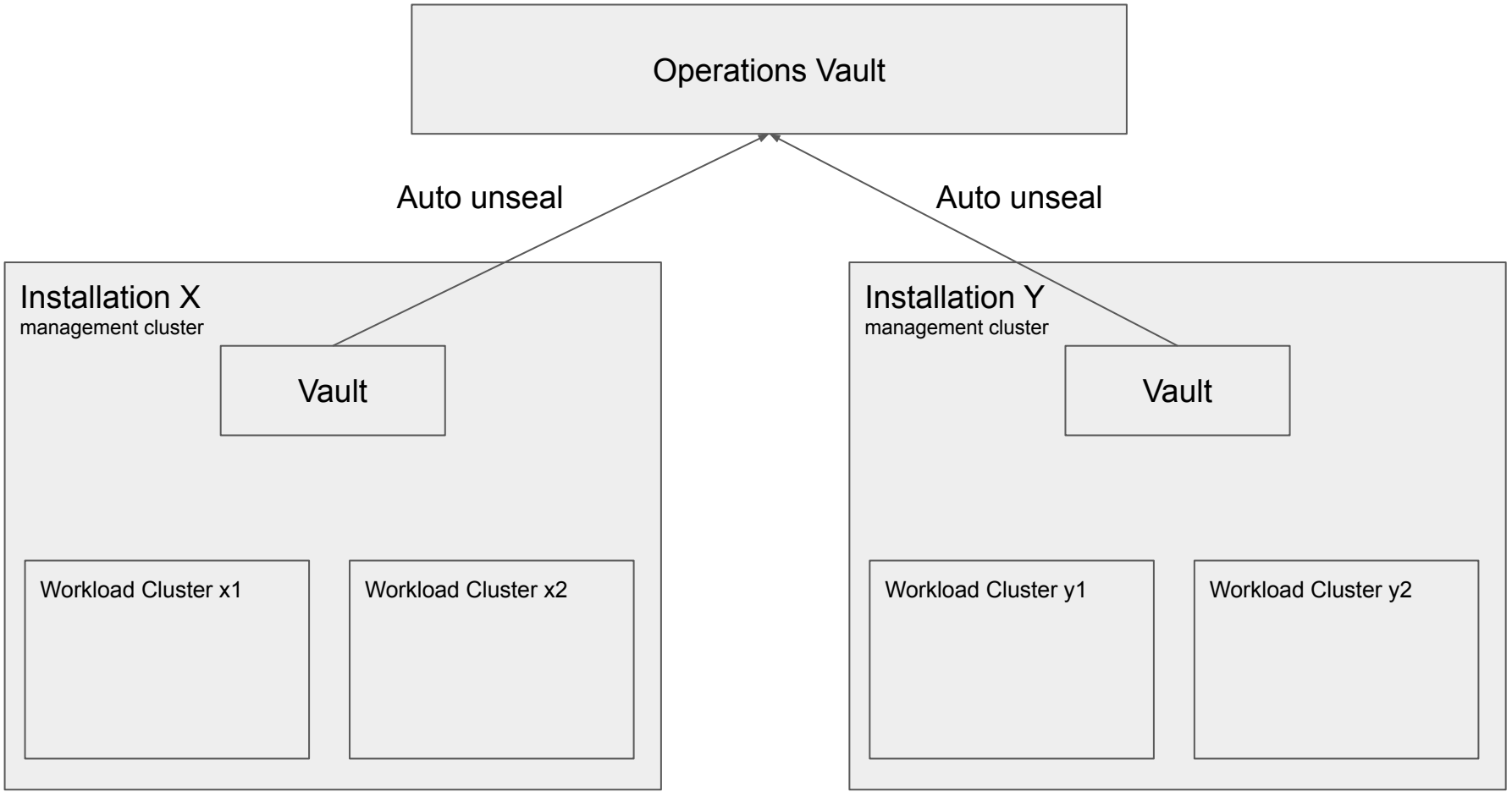
PKI/TLS - Generate a Certificate Without Vault

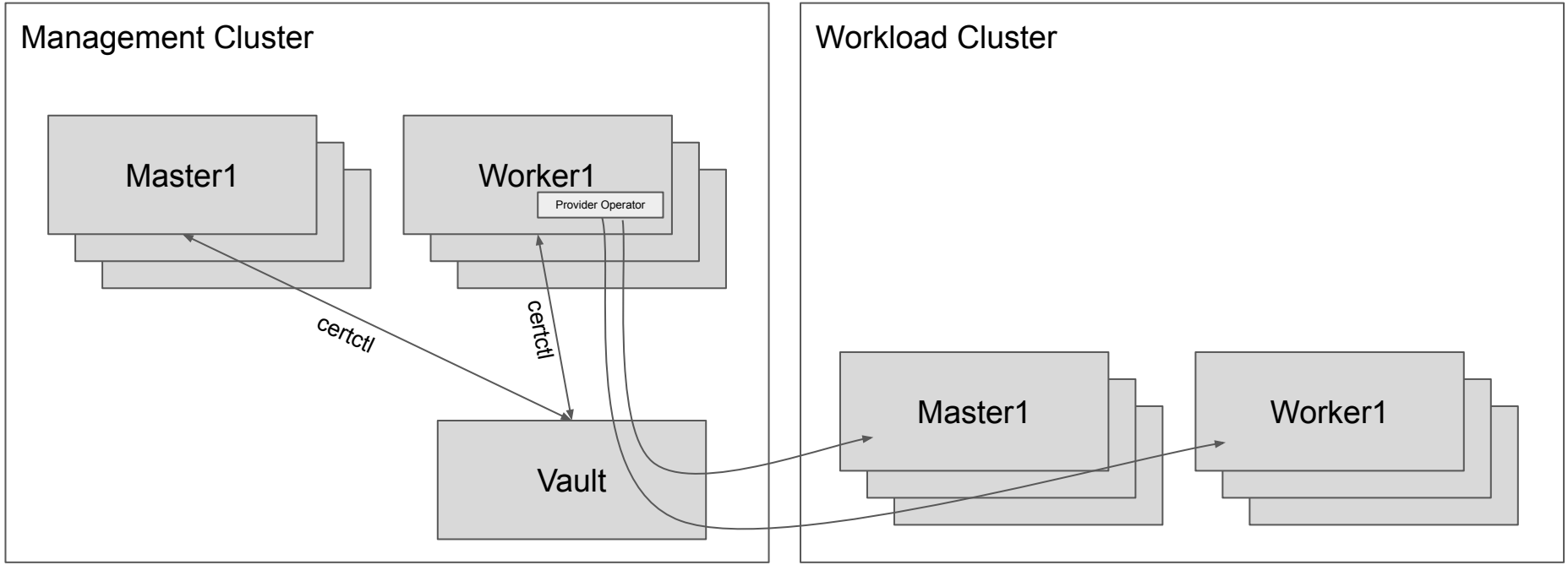


PKI/TLS - With Vault

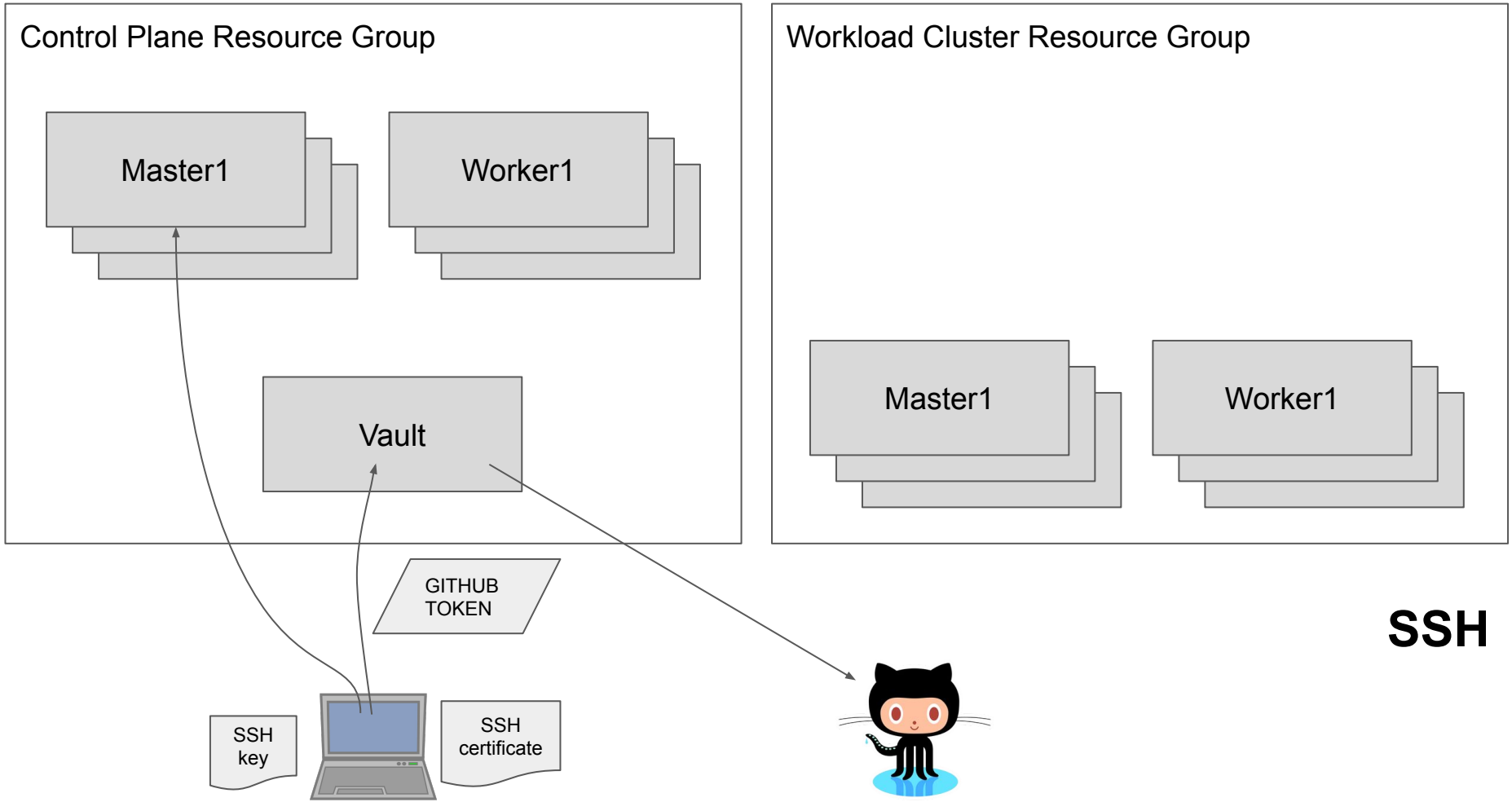


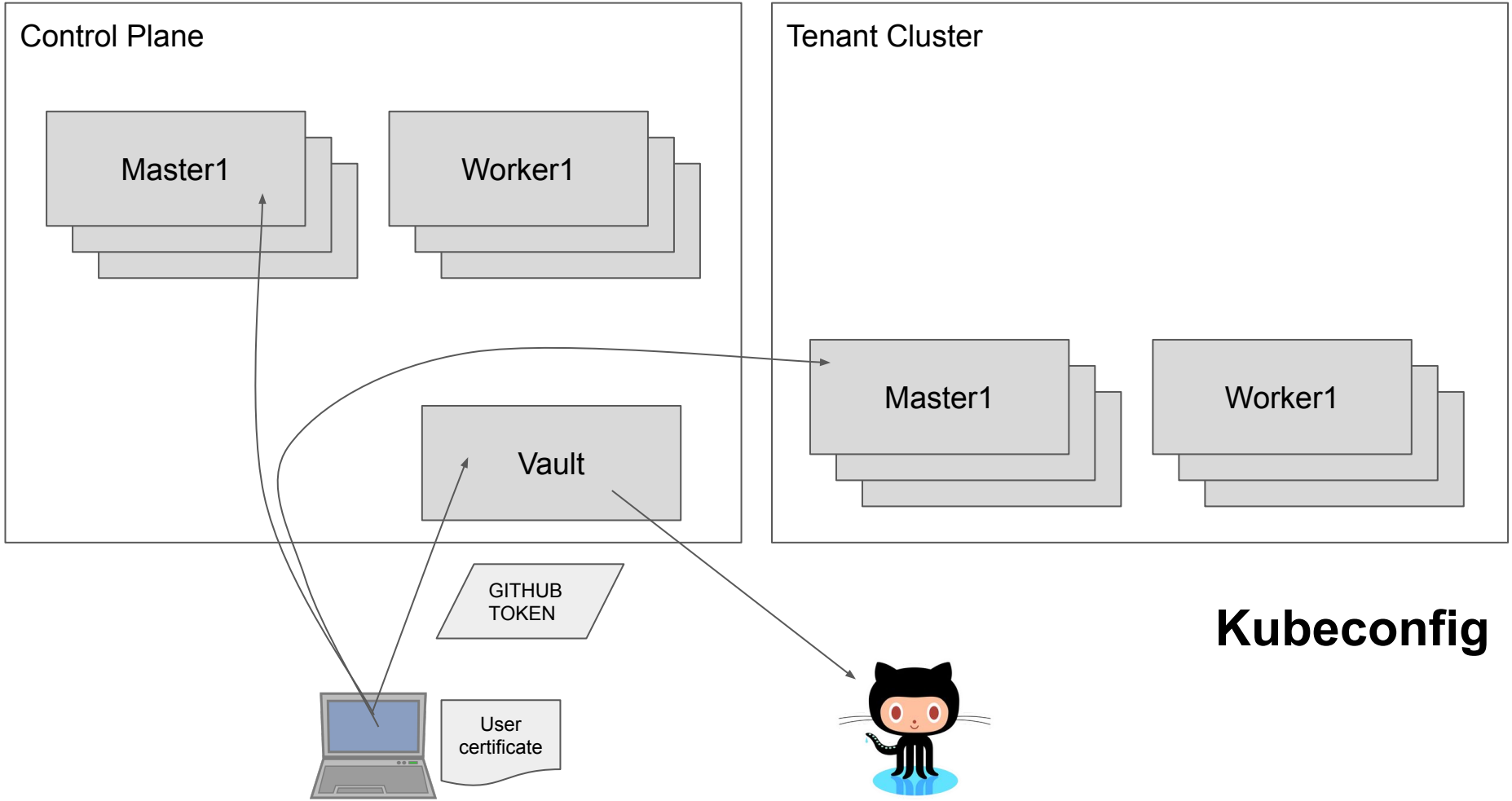

Giant Swarm
How does Giant Swarm use Vault?
KUBERNETES


Operations Vault
Auto unseal
Auto unseal
Installation X
management cluster
Vault
Workload Cluster x1
Workload Cluster x2
Installation Y
management cluster
Vault
Workload Cluster y1
Workload Cluster y2


Management Cluster
Master1
Worker1
Provider Operator
certctl
certctl
Vault
Workload Cluster
Master1
Worker1

TLS


Control Plane Resource Group
Master1
Worker1
Vault
Workload Cluster Resource Group
Master1
Worker1
GITHUB
TOKEN
SSH
key
SSH
certificate
SSH


Control Plane
Master1
Worker1
Vault
Tenant Cluster
Master1
Worker1
GITHUB
TOKEN
User
certificate
Kubeconfig


Giant Swarm
Questions?
KUBERNETES