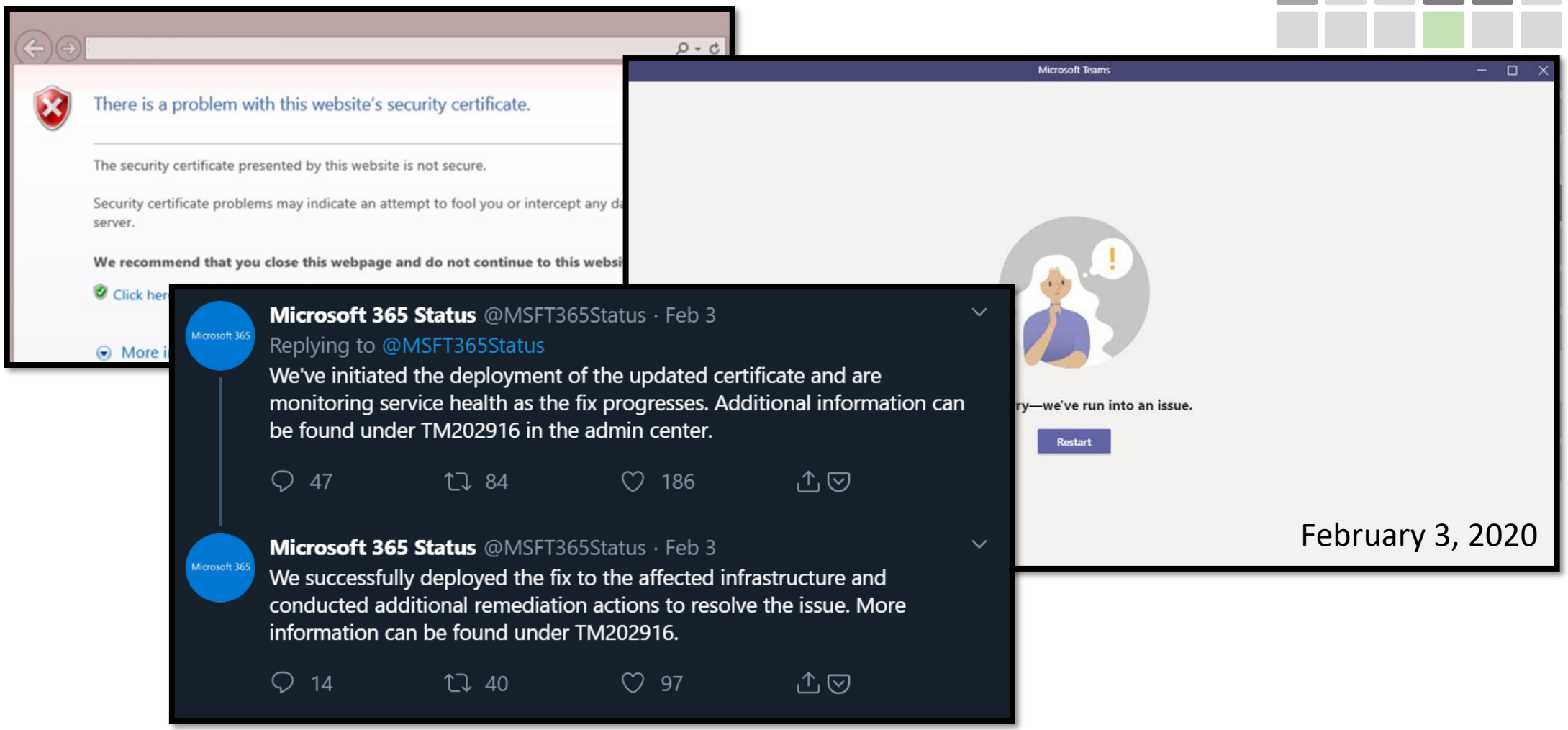
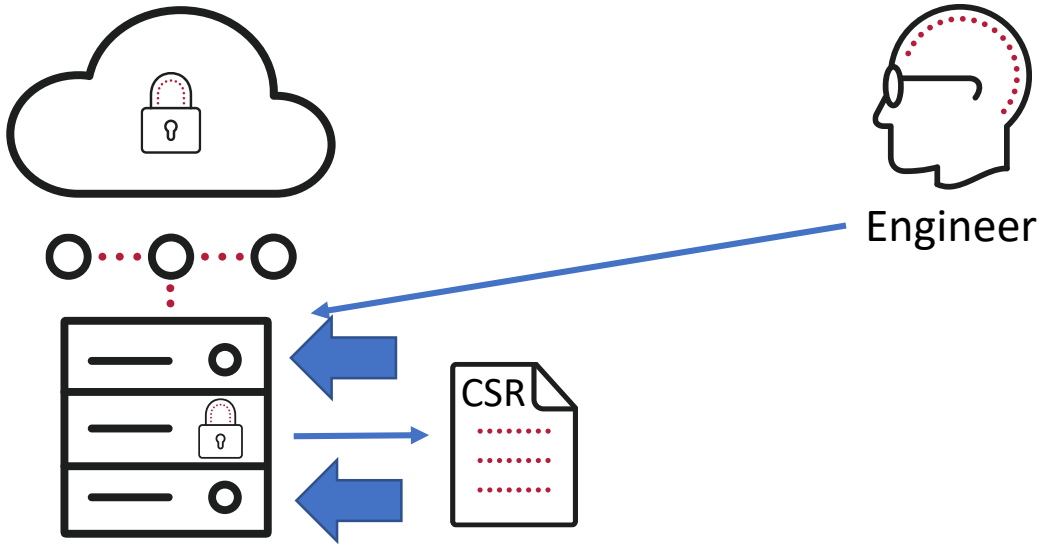
Section 3

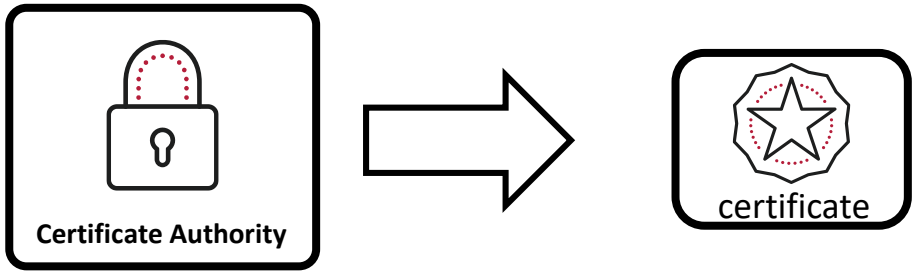
PKI Secrets Engine

Identifying the Problem with Certs

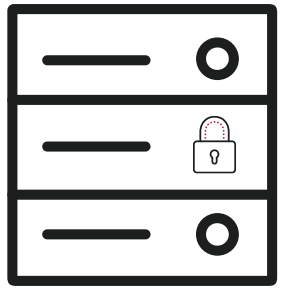


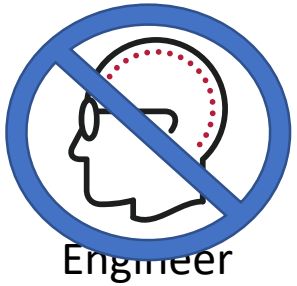
Identifying the Problem with Certs



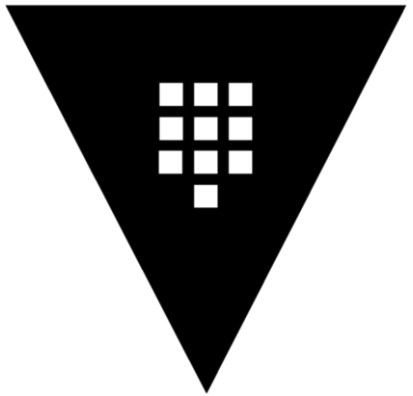


How Does Vault Fix It?





Engineer



PKI Secrets Engine
(Intermediate)

PKI Secrets Engine

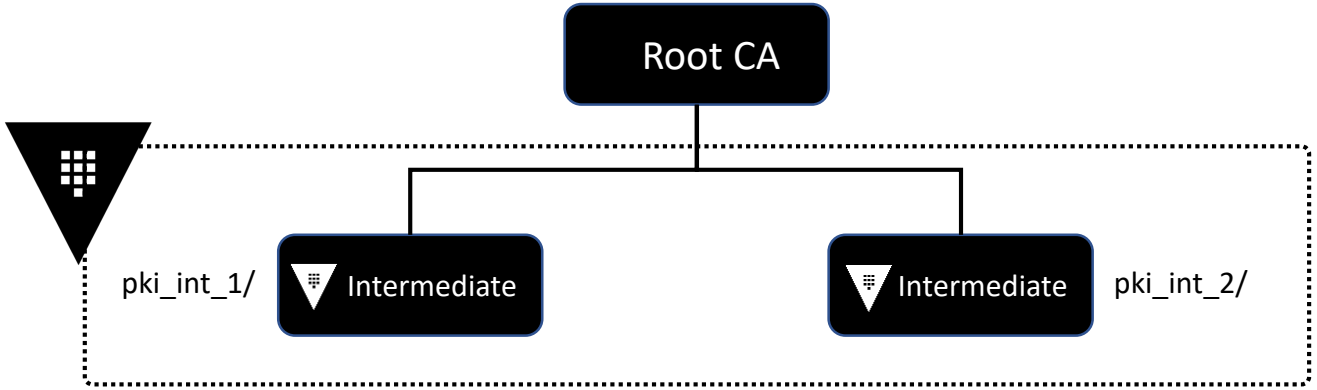
- Generates dynamic X.509 certificates
- Eliminates the manual process for generating a private key and CSR, submitting to the CA, and waiting for verification and signing

- Allows certs to have short TTLs because certs are now ephemeral
- Virtually eliminates revocations

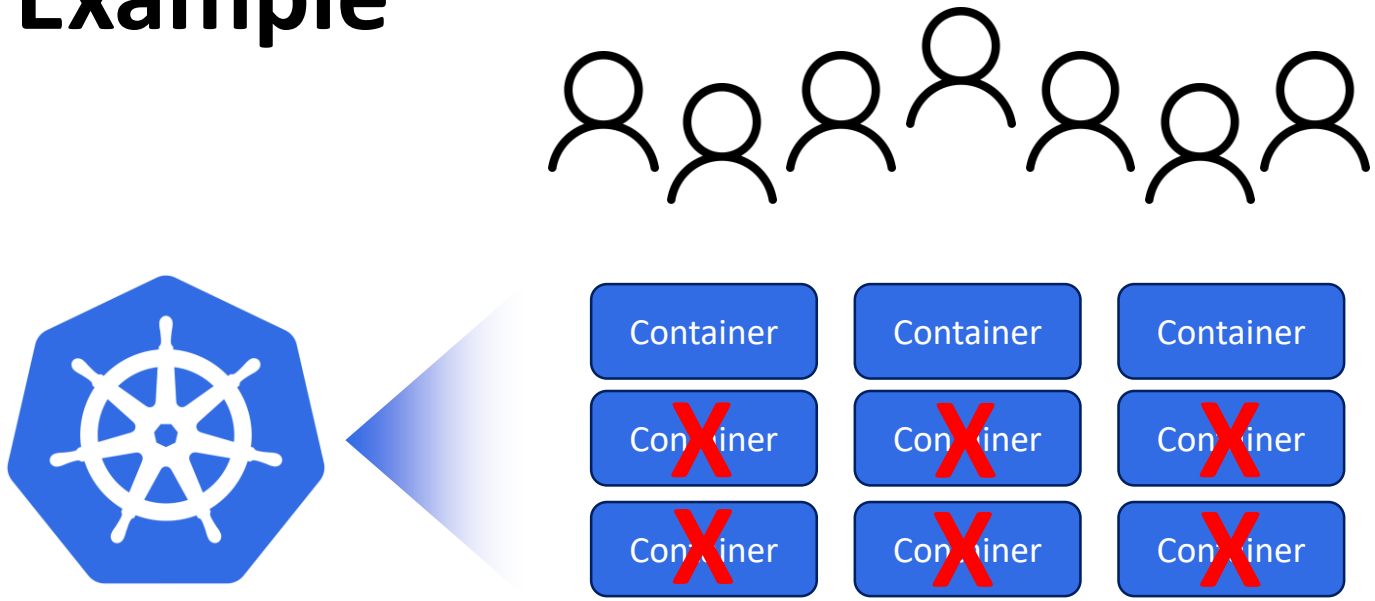
- Simple to allocate a certificate to each workload
- Stops the certificate sharing, use of wildcard certificates, or using self-signed certificates which are prone to MITM attacks

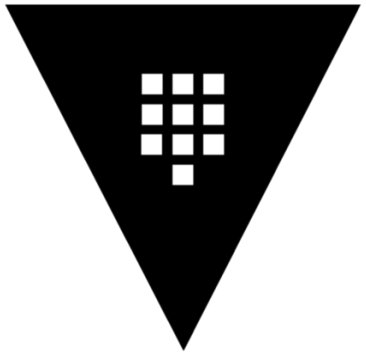
PKI Secrets Engine

- Most likely, you're going to use Vault as an Intermediate as your root CA is generally offline.
- Most organizations already have an existing CA structure in place and Vault can plug right into that, if needed.
- Using multiple PKI secrets engines, Vault can perform the root and the intermediate(s) CA functionality from the same cluster



PKI Example


Container
Container
Container
Container
Container
Container
Container
Container
Container

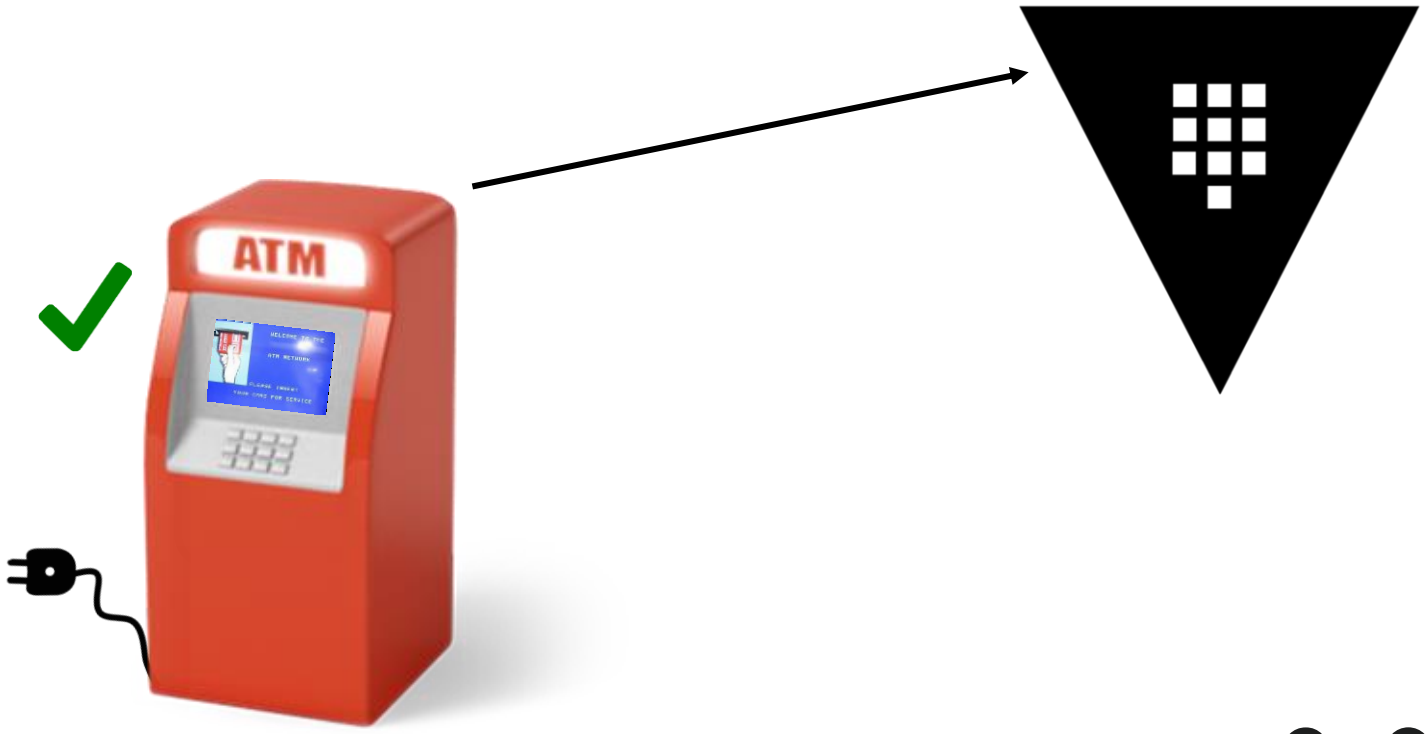


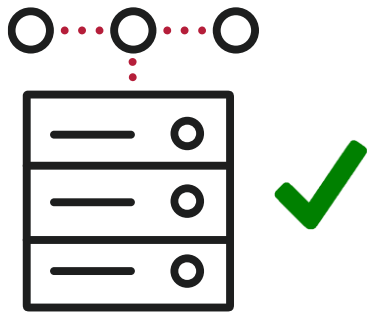
PKI Example

Need a certificate for authentication to:

- Update firmware
- Download configuration files
- Communicate with banking account application
- Report inventory

PKI Example





Backend Systems

Configuring the PKI Secrets Engine

Enabling the PKI Secrets Engine

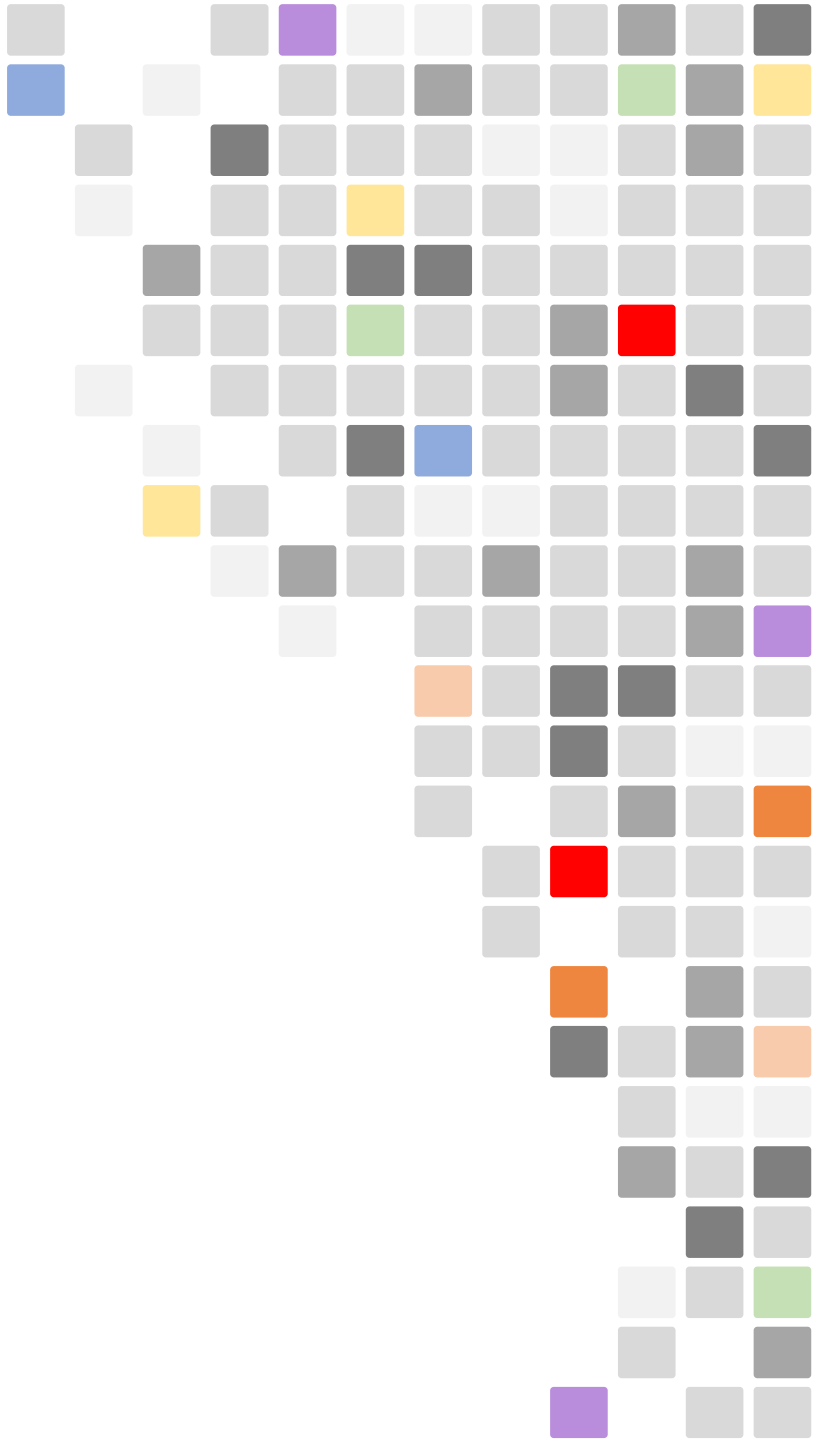
```
$ vault secrets enable \
  –path=intermediate \
  –description=“PKI Intermediate for vaultadvanced.com” \
  pki
```

Create Role

```
$ vault write intermediate/roles/vaultadvanced \
  allowed_domains=vaultadvanced.com \
  allow_subdomains=true max_ttl=72h
```

Request Certificates

```
$ vault write intermediate/issue/vaultadvanced \
  common_name=learn.vaultadvanced.com
```



Vault Policies - PKI

Administration of PKI

```
path “intermediate /*” {
  capabilities = [“read”, “list”, “update”, “write”, “delete”]
}
```

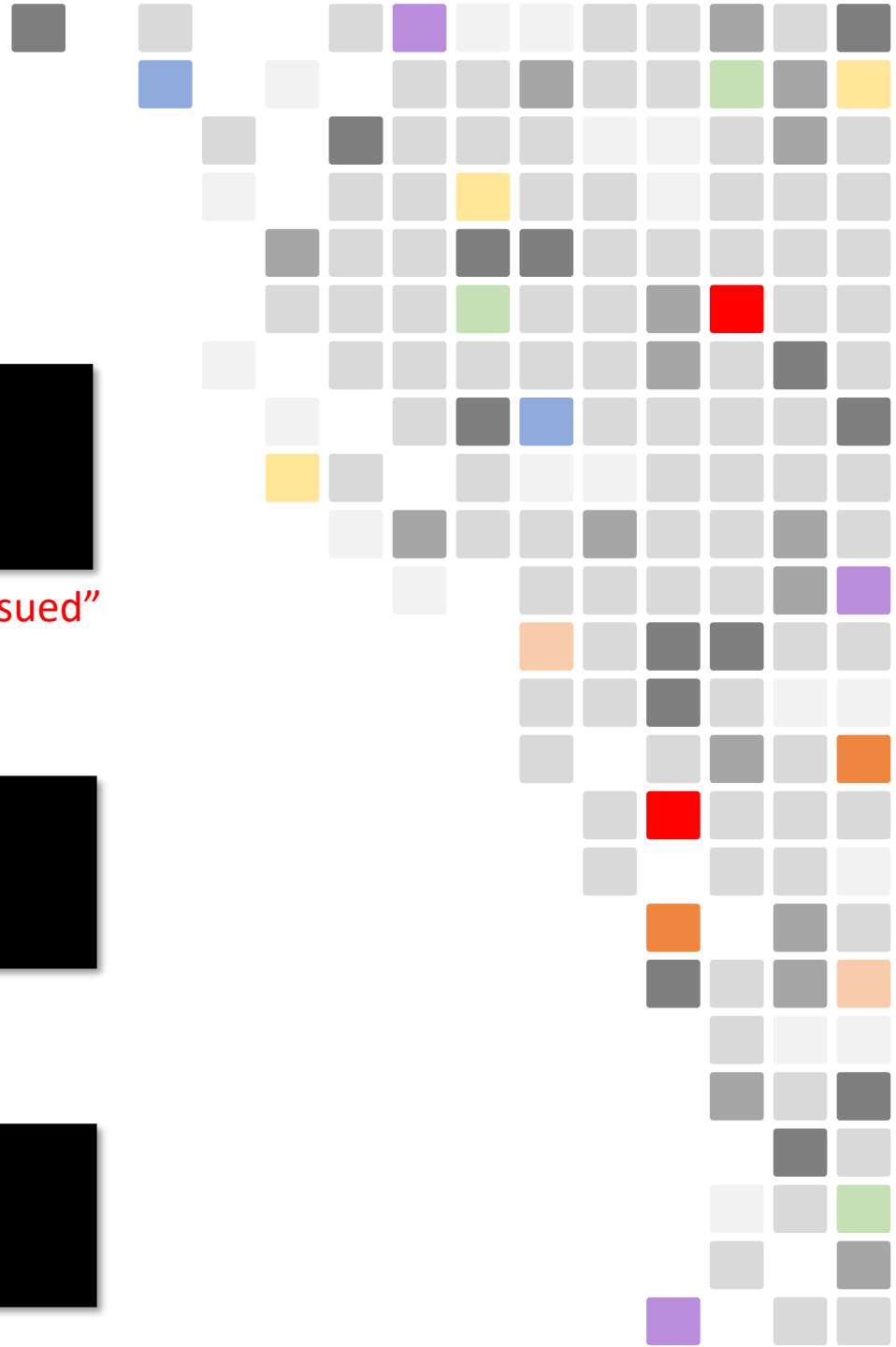
Note: sudo required for “delete root” and “sign self-issued”

Generate a Certificate

```
path “intermediate /issue/vaultadvanced” {
  capabilities = [“update”]
}
```

Revoke Certificate

```
path “intermediate/revoke” {
  capabilities = [“update”]
}
```



Demo

PKI Secrets Engine

Enable PKI Secrets Engine

Configure Vault as an Intermediate

Issue Certificates from Vault