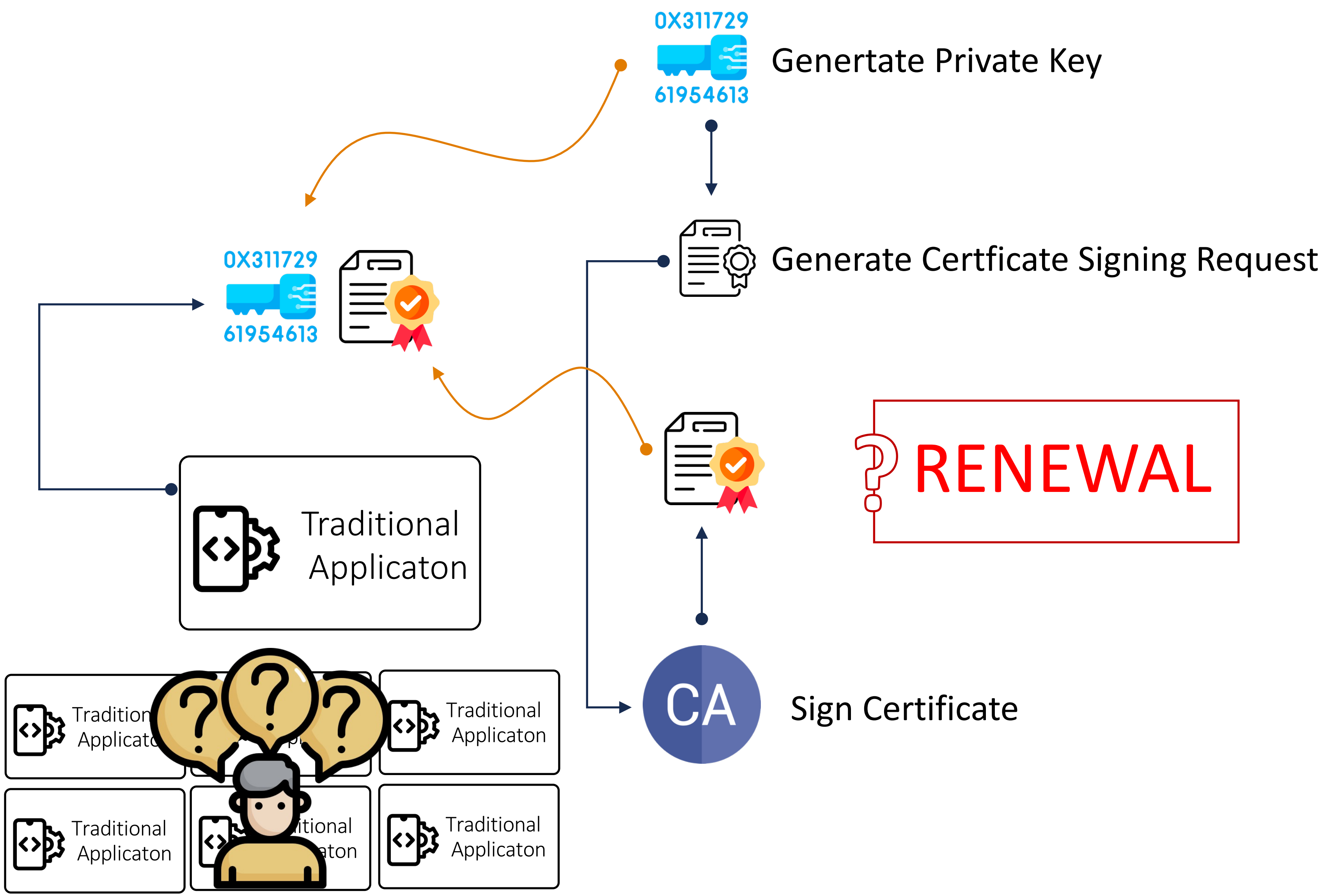
Automating TLS Certificate Management with HashiCorp Vault

Damrongsak Reetanon | HashiCorp Ambassdor | Chief Cybersecurity Officer, MFEC Public Company Limited

Today!!!

Automating TLS Certificate Management with HashiCorp Vault

Why ???

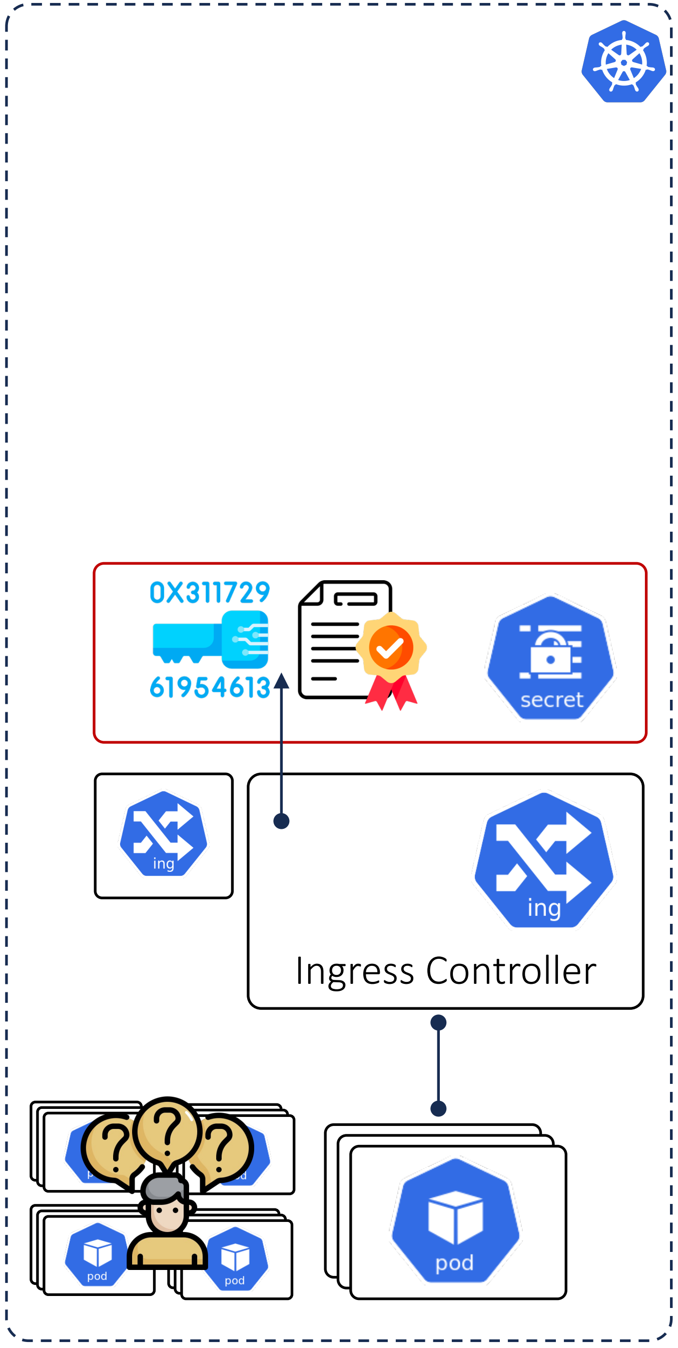


Genertate Private Key

Generate Certficate Signing Request

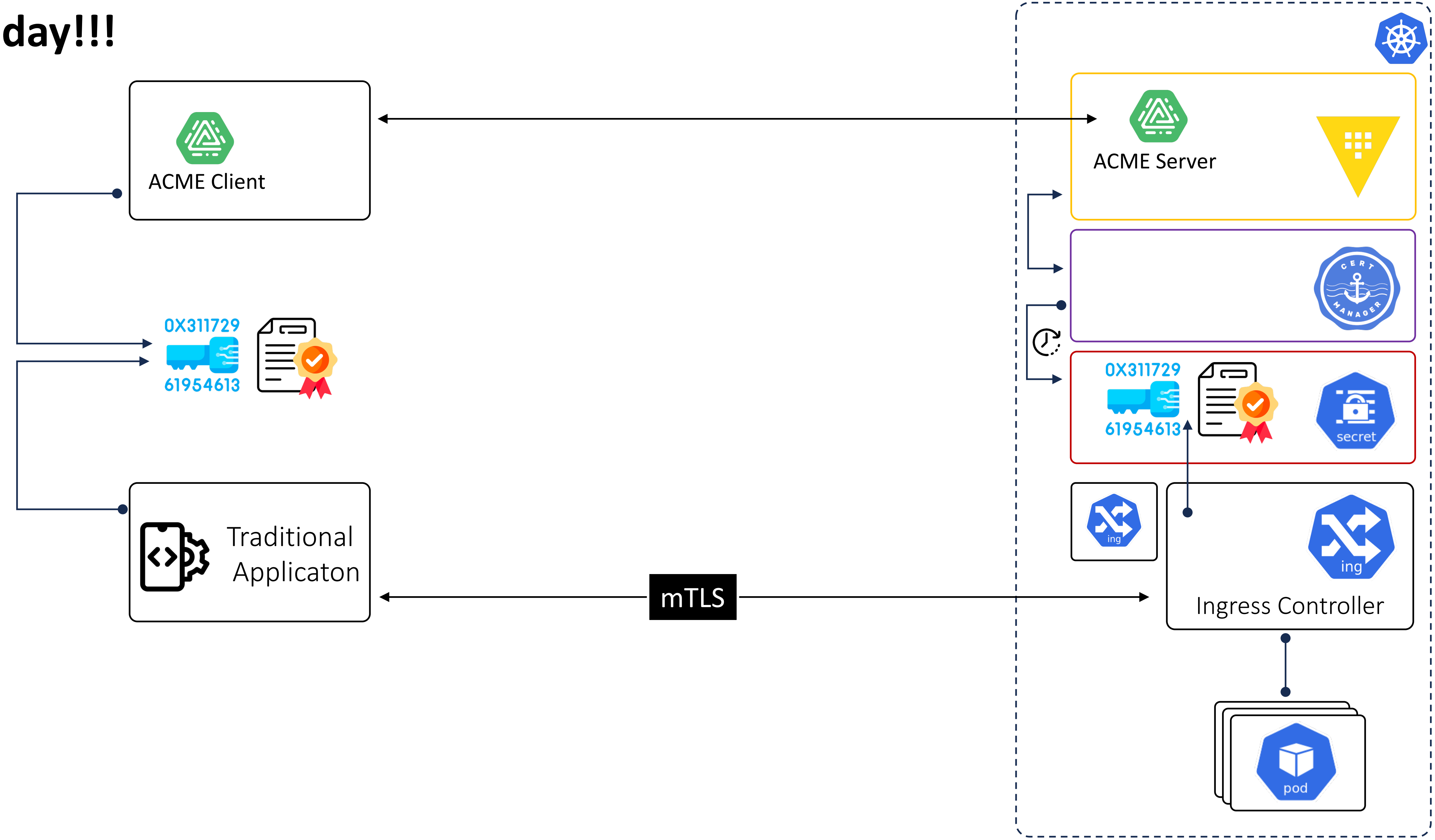
RENEWAL

Sign Certificate



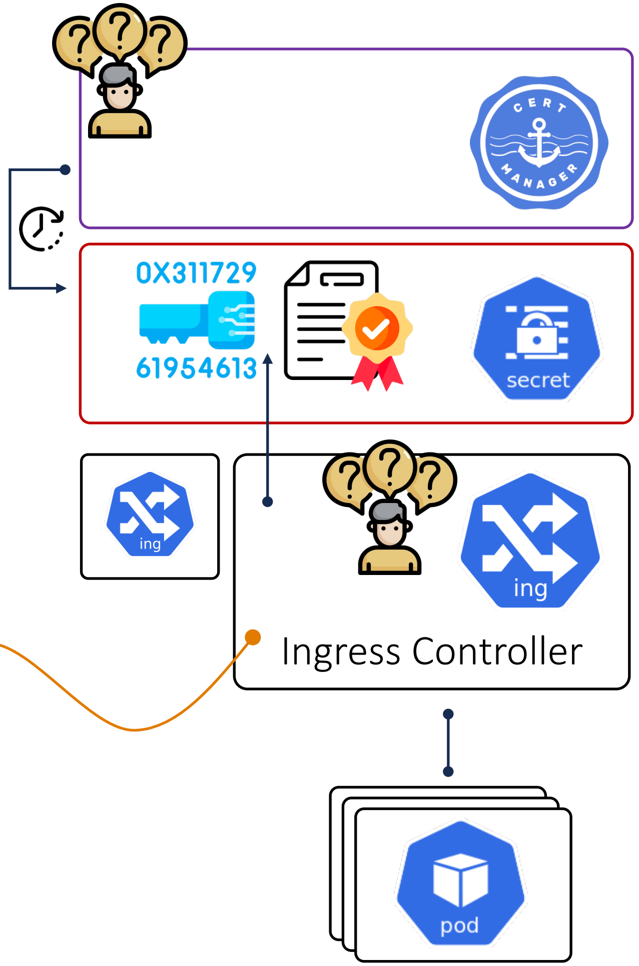
Ingress Controller

Today!!!

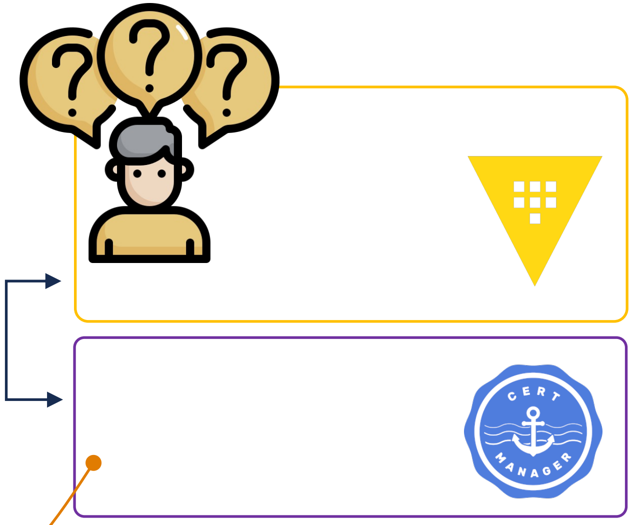

ACME Client
0X311729
61954613
Traditional Applicaton
mTLS
ACME Server
0X311729
61954613
secret
ing
ing
Ingress Controller
pod

cert-manager adds certificates and certificate issuers as resource types in Kubernetes clusters, and simplifies the process of obtaining, renewing and using those certificates.
It can issue certificates from a variety of supported sources, including Let's Encrypt, HashiCorp Vault, and Venafi as well as private PKI.
It will ensure certificates are valid and up to date, and attempt to renew certificates at a configured time before expiry.

```
apiVersion: k8s.nginx.org/v1
kind: VirtualServer
metadata:
    name: cafe
spec:
    policies:
      - name: enable-mtls
    host: crd.d8k.dev
    tls:
      secret: ingress-crd
      cert-manager:
             issuer: "vault-issuer"
             common-name: crd.d8k.dev
[... truncated output ...]
```

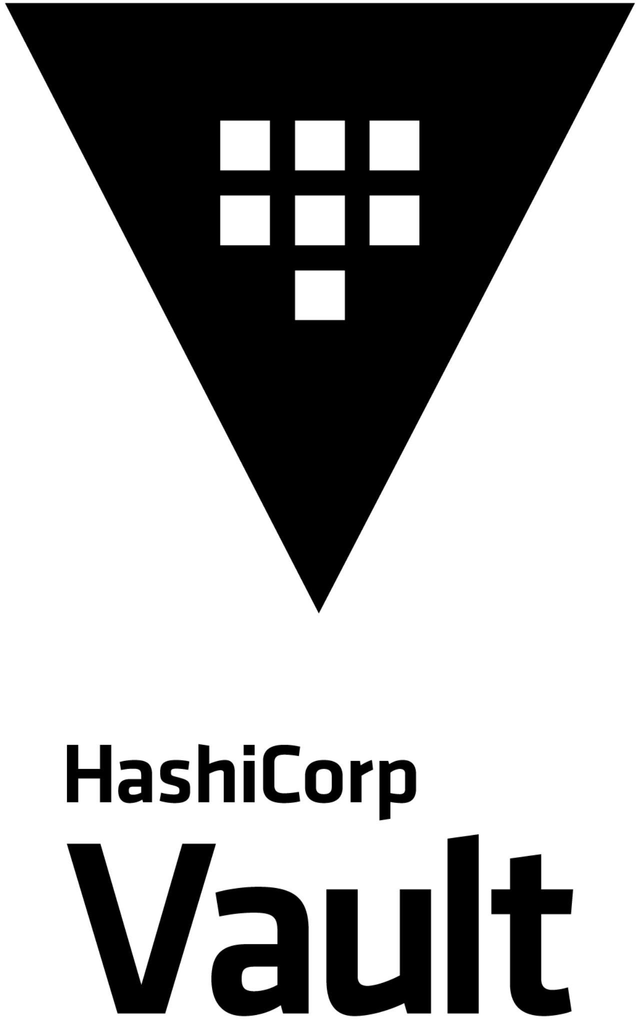


```yaml
apiVersion: cert-manager.io/v1
kind: Issuer
metadata:
  name: vault-issuer
  namespace: default
spec:
  vault:
    caBundleSecretRef:
        key: ca.crt
        name: tls-ca-cert
    server: https://vault.vault.svc.cluster.local:8200
    path: pki_int/sign/d8kint
    auth:
      kubernetes:
        mountPath: /v1/auth/k8s_certmanager
        role: issuer
        secretRef:
          name: issuer-token
          key: token
```

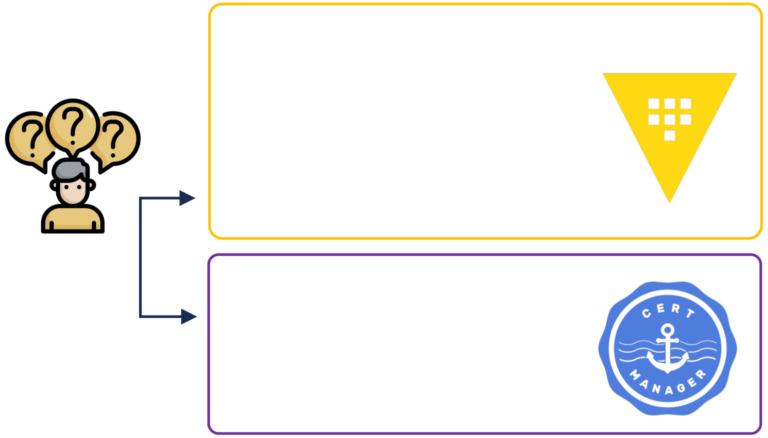


What are HashiCorp Vault?

HashiCorp Vault is an identity-based secrets and encryption management system. It provides encryption services that are gated by authentication and authorization methods to ensure secure, auditable and restricted access to secrets. It is used to secure, store and protect secrets and other sensitive data using a UI, CLI, or HTTP API.



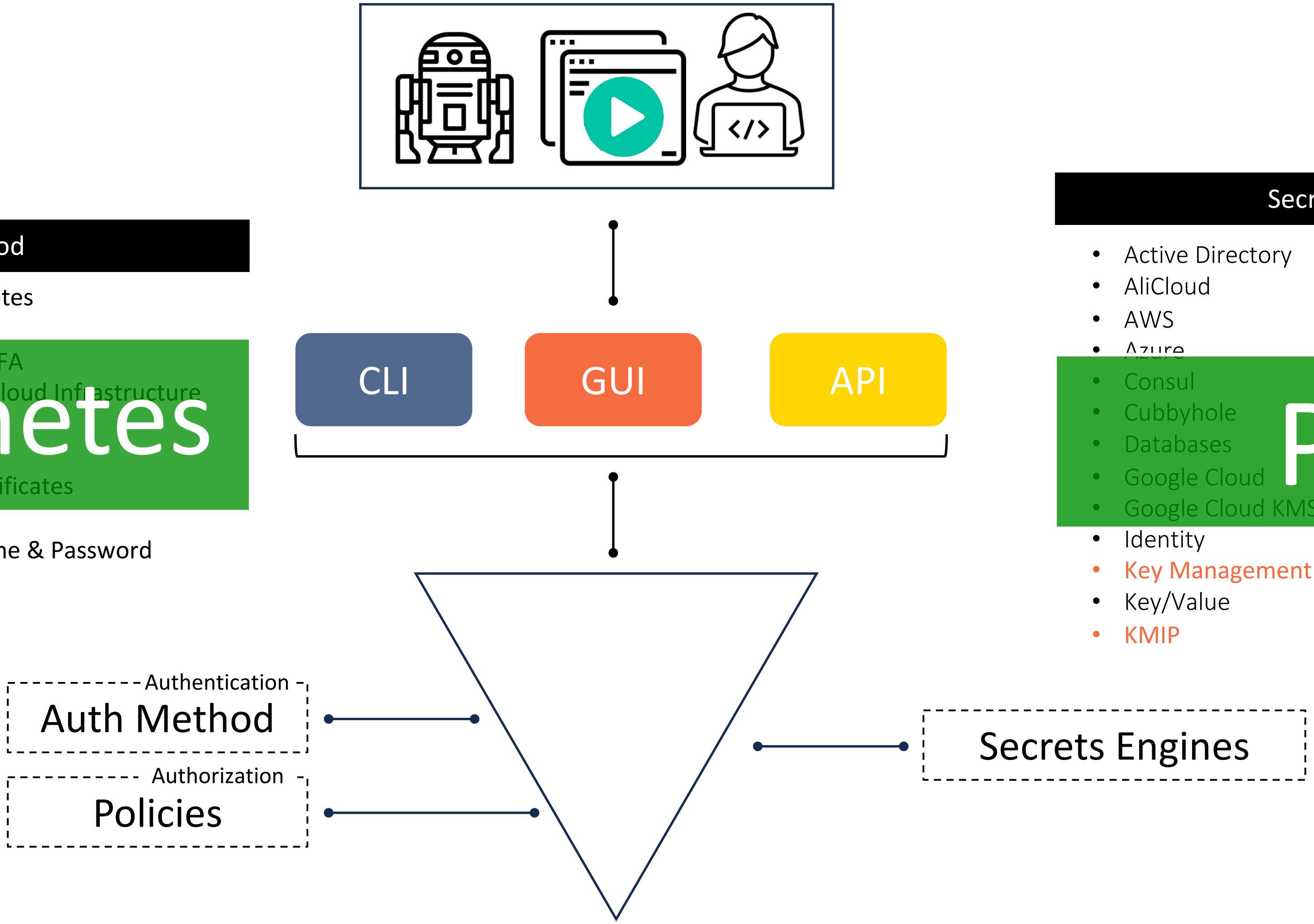
Ref: https://www.vaultproject.io/



Auth Method

- AppRole
- AliCloud
- AWS
- Azure
- Cloud Foundry
- GitHub
- Google Cloud
- JWT/OIDC
- Kerberos
- Kubernetes
- LDAP
- Login MFA
- Oracle Cloud Infrastructure
- Okta
- RADIUS
- TLS Certificates
- Tokens
- Username & Password

Kubernetes



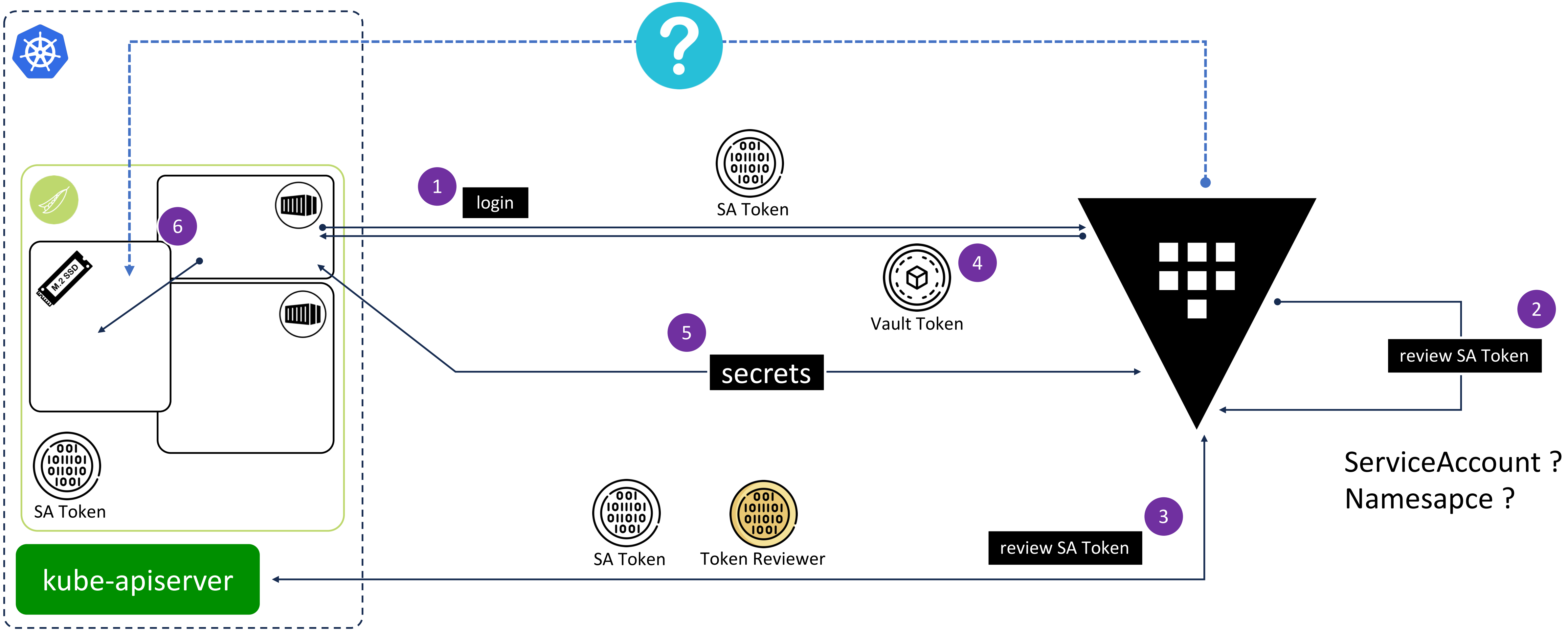
Secrets Engines

- Active Directory
- AliCloud
- AWS
- Azure
- Consul
- Cubbyhole
- Databases
- Google Cloud
- Google Cloud KMS
- Identity
- Key Management
- Key/Value
- KMIP
- Kubernetes
- MongoDB Atlas
- Nomad
- LDAP
- PKI (Certificates)
- RabbitMQ
- SSH
- Terraform Cloud
- TOTP
- Transform
- Transit
- Venafi (Certificates)

PKI

Kubernetes auth method

The Kubernetes auth method facilitates authentication with Vault by a Kubernetes Service Account Token. Employing this authentication method simplifies the process of integrating a Vault token into a Kubernetes Pod.



Public Key Infrastructure (PKI) Secrets Engine

A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. The PKI includes the hierarchy of certificate authorities that allow for the deployment of digital certificates that support encryption, digital signature and authentication to meet business and security requirements.

Sources: NIST SP 800-95 under Public Key Infrastructure (PKI) from OASIS Glossary of Terms

Public Key Infrastructure

Cryptography that uses **two separate keys to exchange data**, one to encrypt or digitally sign the data and one for decrypting the data or verifying the digital signature. Also known as public key cryptography.

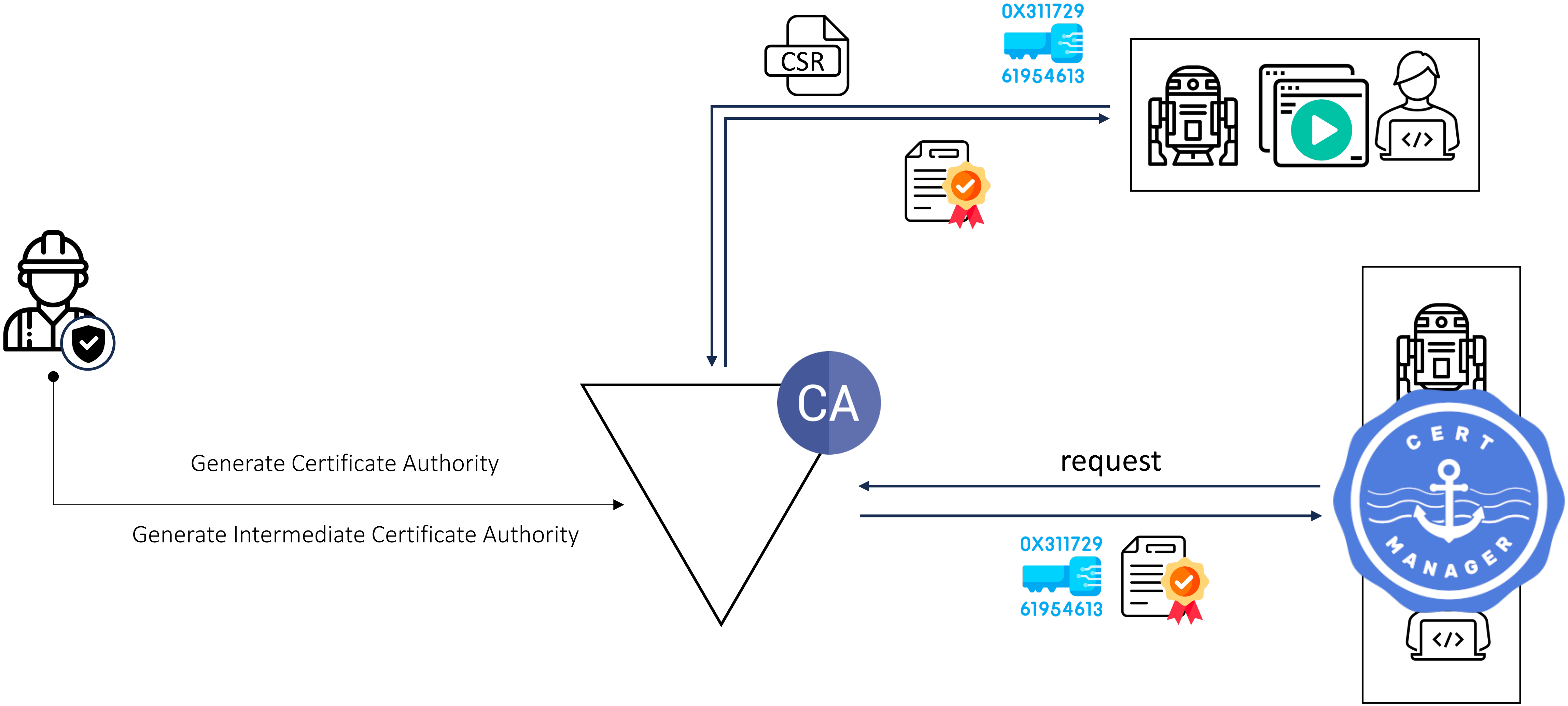
Sources: NIST SP 800-77 Rev. 1 under Asymmetric Cryptography

asymmetric cryptography

The PKI secrets engine generates dynamic X.509 certificates. With this secrets engine, services can get certificates without going through the usual manual process of generating a private key and CSR, submitting to a CA, and waiting for a verification and signing process to complete. Vault's built-in authentication and authorization mechanisms provide the verification functionality.

https://developer.hashicorp.com/vault/docs/secrets/pki

Public Key Infrastructure (PKI) Secrets Engine

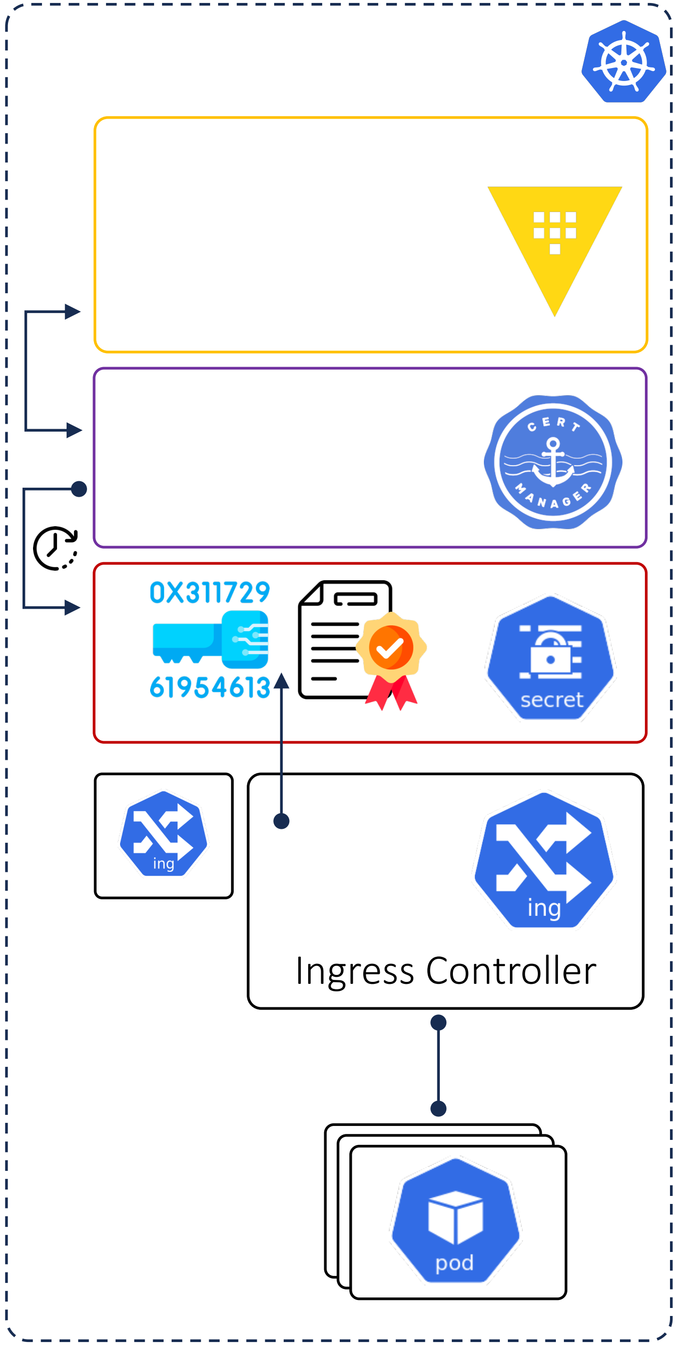

CSR
0X311729
61954613
Generate Certificate Authority
Generate Intermediate Certificate Authority
CA
request
0X311729
61954613
CERT MANAGER
</>

- **Enable PKI Engine**
- Generate Root Certificate Authority
- Generate Intermediate Certificate Authority

- **Enable the Kubernetes auth method**
- Configure Vault to talk to Kubernetes to validate the Token
- Create Role and Policy that maps to Policy used to generate key pair
- Create a named role to specific authentication condition

- Create issuer that authenticate to Kubernetes auth method’s role and request to Vault PKI Secrets Engine’s role.

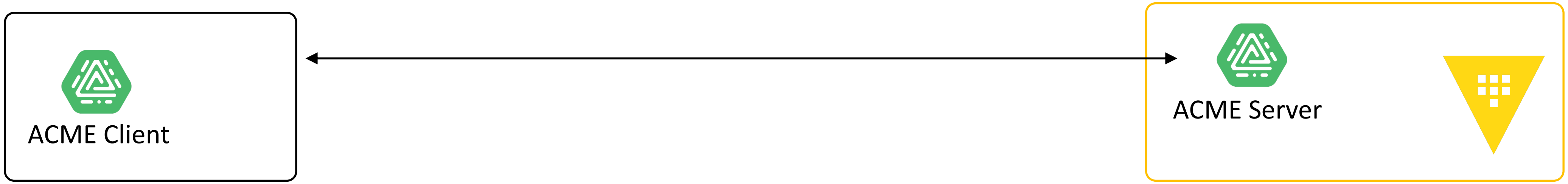
- Create CRD called “VirutalServer” that request TLS secrets from cert-manager with specific issuer and common name.



DEMO

https://github.com/rdamrong/hashitalk2023

What is ACME?



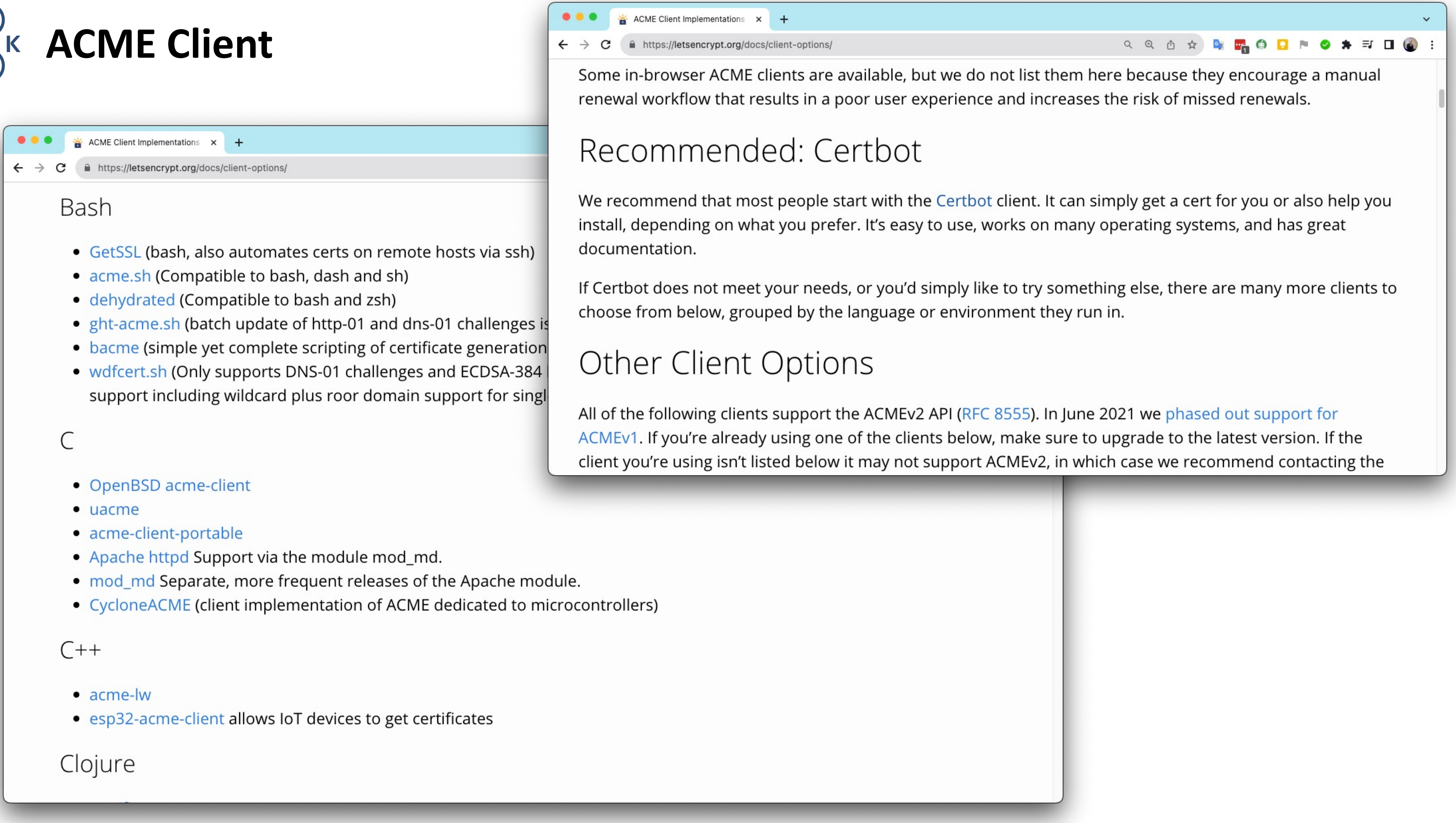
Automated Certificate Management Environment (ACME)

A protocol defined in IETF RFC 8555 that provides for the automated enrollment of certificates.

https://csrc.nist.gov/glossary/term/acme

the process of certificate issuance, renewal, and management for websites. It simplifies the traditionally complex and manual process of obtaining and managing SSL/TLS certificates, which are essential for securing web traffic through HTTPS.

ACME Client


ACME Client Implementations
https://letsencrypt.org/docs/client-options/

Some in-browser ACME clients are available, but we do not list them here because they encourage a manual renewal workflow that results in a poor user experience and increases the risk of missed renewals.

Recommended: Certbot

We recommend that most people start with the Certbot client. It can simply get a cert for you or also help you install, depending on what you prefer. It's easy to use, works on many operating systems, and has great documentation.

If Certbot does not meet your needs, or you'd simply like to try something else, there are many more clients to choose from below, grouped by the language or environment they run in.

Other Client Options

All of the following clients support the ACMEv2 API (RFC 8555). In June 2021 we phased out support for ACMEv1. If you're already using one of the clients below, make sure to upgrade to the latest version. If the client you're using isn't listed below it may not support ACMEv2, in which case we recommend contacting the

Bash

- GetSSL (bash, also automates certs on remote hosts via ssh)
- acme.sh (Compatible to bash, dash and sh)
- dehydrated (Compatible to bash and zsh)
- ght-acme.sh (batch update of http-01 and dns-01 challenges is
- bacme (simple yet complete scripting of certificate generation
- wdfcert.sh (Only supports DNS-01 challenges and ECDSA-384 support including wildcard plus roor domain support for singl

C

- OpenBSD acme-client
- uacme
- acme-client-portable
- Apache httpd Support via the module mod_md.
- mod_md Separate, more frequent releases of the Apache module.
- CycloneACME (client implementation of ACME dedicated to microcontrollers)

C++

- acme-lw
- esp32-acme-client allows IoT devices to get certificates

Clojure

https://letsencrypt.org/docs/client-options/

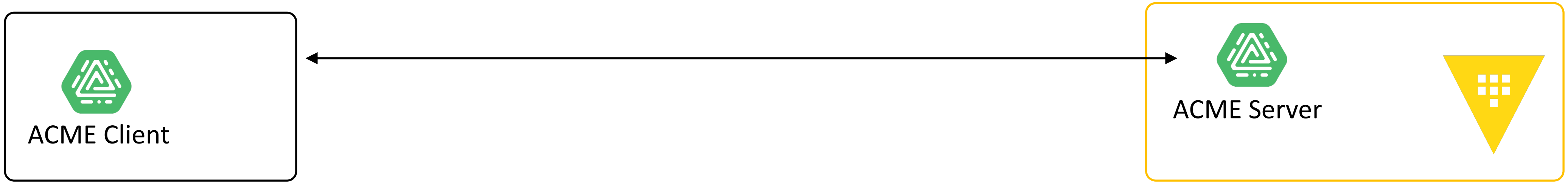
ACME Client
ACME Server

```
> vault secrets tune  \
   -passthrough-request-headers=If-Modified-Since \
   -allowed-response-headers=Last-Modified  \
   -allowed-response-headers=Location \
   -allowed-response-headers=Replay-Nonce \
   -allowed-response-headers=Link pki_int

> vault write pki_int/config/acme enabled=true \
   eab_policy=always-required \
   allow_role_ext_key_usage=true
```

```
> vault write -force pki_int/roles/d8kint/acme/new-eab
Key                 Value
---                 -----
acme_directory      roles/d8kint/acme/directory
created_on          2023-11-14T16:47:58Z
id                  6849c779-05a7-ef0b-8c9d-25a0cb794352
key                 vault-eab-0-TCm3AwptaJe-xXX9XF2PkftoXXGzVfhumPjxR3-rR-0
key_type            hs
```

The ACME protocol defines an external account binding (EAB) field that ACME clients can use to access a specific account on the certificate authority (CA).



```
> certbot certonly --config-dir=. --work-dir=. --logs-dir=. --no-eff-email  \
  --server https://localhost:30200/v1/pki_int/roles/d8kint/acme/directory \
  --email damrongs@gmail.com -d drs.d8k.dev --key-type rsa \
  --eab-kid=$EAB_ID --eab-hmac-key=$EAB_KEY \
  --dns-digitalocean --dns-digitalocean-credentials ./.digitaloceanrc

Saving debug log to /Users/drs/letsencrypt.log
Renewing an existing certificate for drs.d8k.dev
Waiting 10 seconds for DNS changes to propagate

Successfully received certificate.
Certificate is saved at: /Users/drs/live/drs.d8k.dev/fullchain.pem
Key is saved at:         /Users/drs/live/drs.d8k.dev/privkey.pem
This certificate expires on 2023-11-14.
These files will be updated when the certificate renews.

[... truncated output ...]
```

DEMO

https://github.com/rdamrong/hashitalk2023

[Once in A Lifetime]

一期一会