# Automatic Secret rotation with ESO

Gergely Brautigam

https://github.com/Skarlso
https://gergelybrautigam.com
https://github.com/external-secrets

QR code link to repository ->

# Agenda

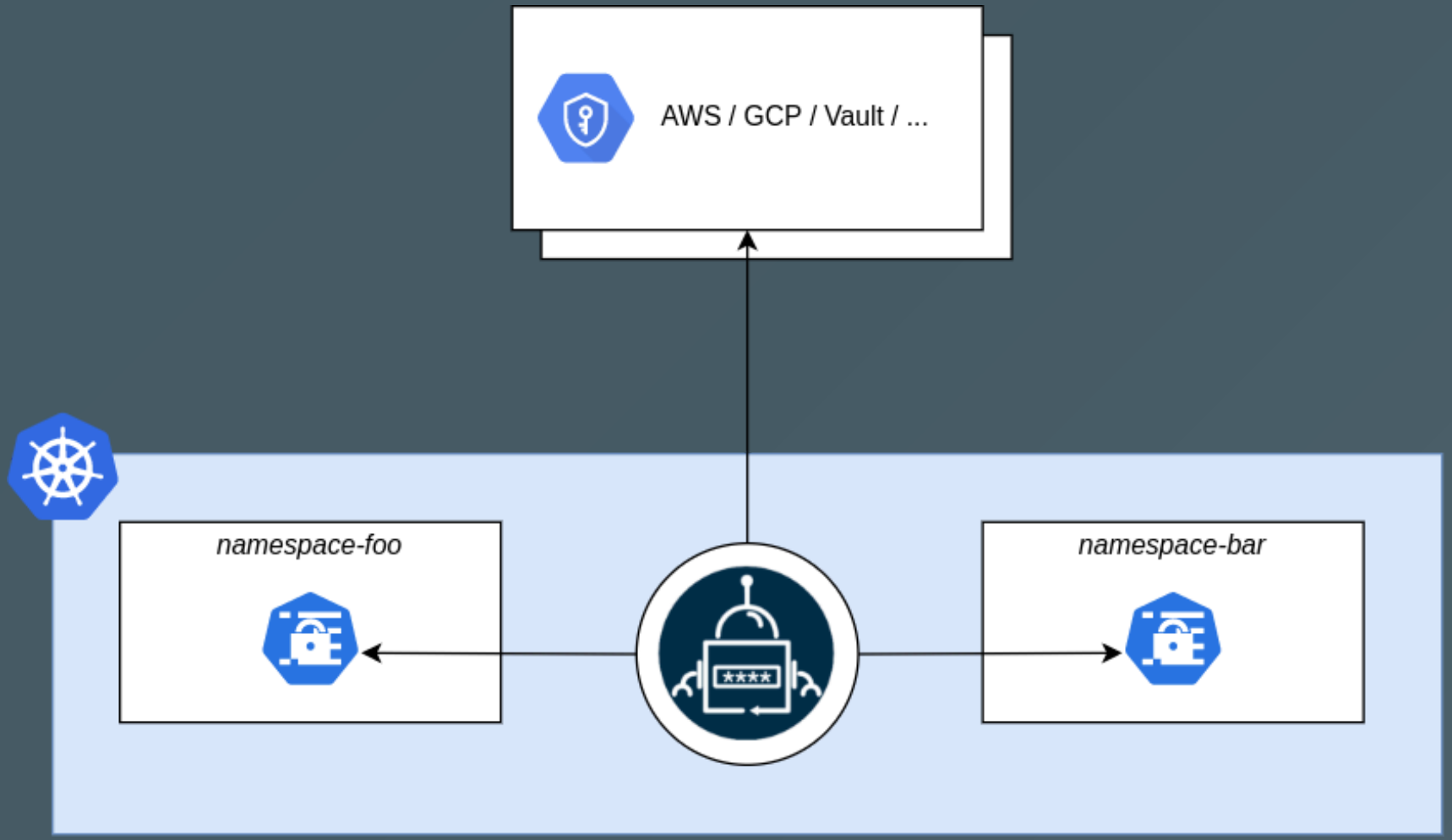
- Why rotation is important
- External Secrets intro
- Rotation
- Demo
- ESO Reloader Demo
- Caveats
  - Downtime
  - Race conditions
- Closing words

# Why is it important to rotate secrets?

- the longer the token the longer the expouser and the chain of custody
- uber 2022 where a mobile device was compromised
- dependabot exploit of 2023
- cloudflare outage 2023. they rotated, however, due to human error some of the tokens
  got exposed and they got inflitrated
- there are many many more...

# What is External Secrets Operator

# Architecture

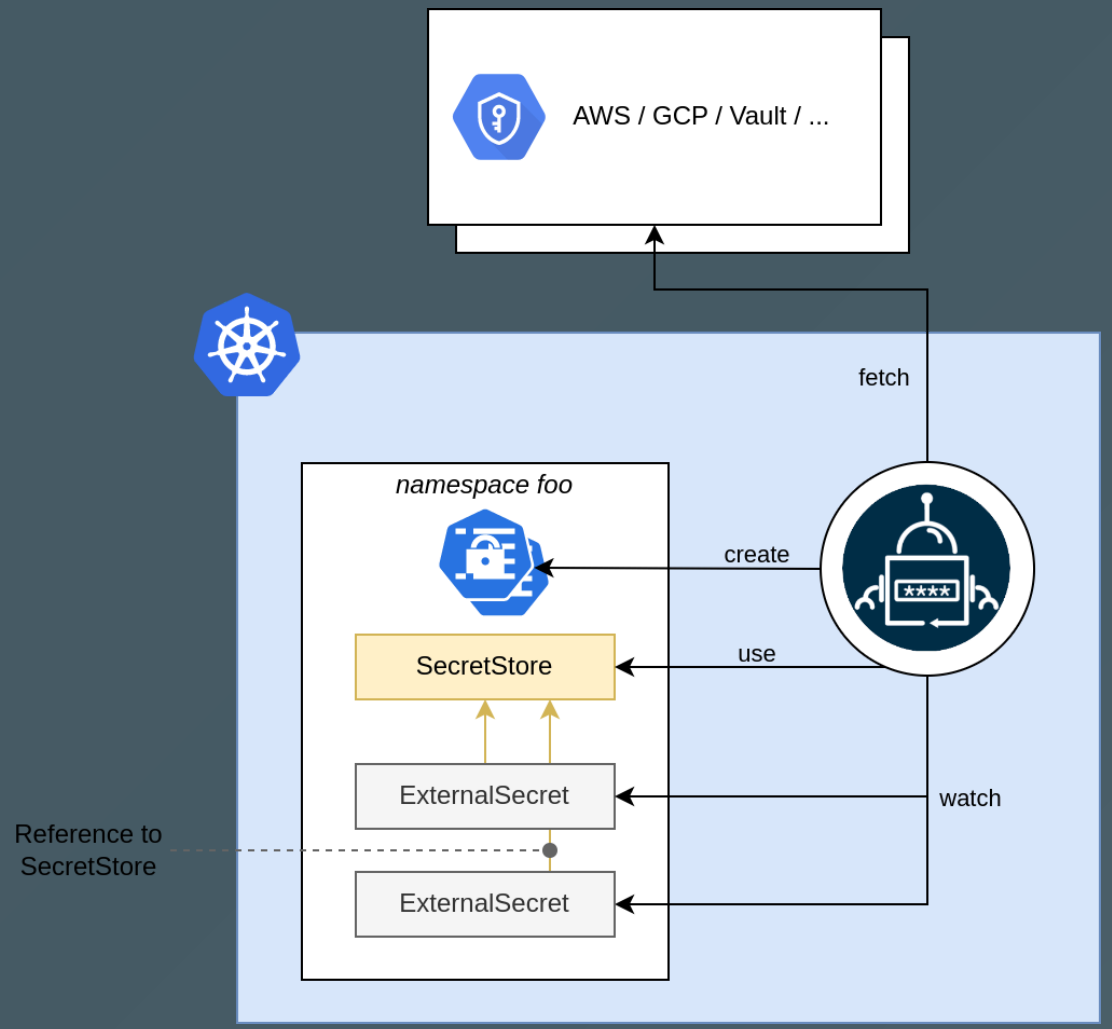


# Providers

- AWS
- GCP
- Vault
- Kubernetes

  ...

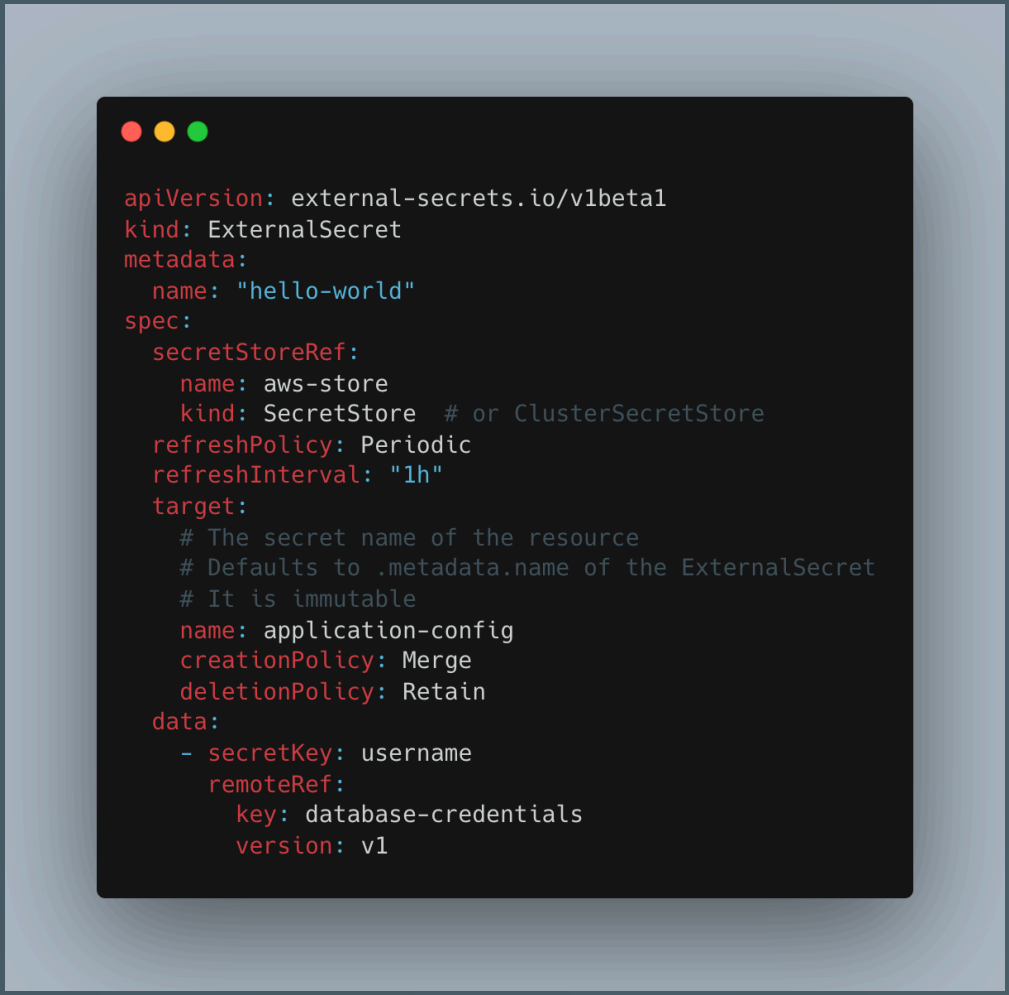
# SecretStore architecture



# SecretStore

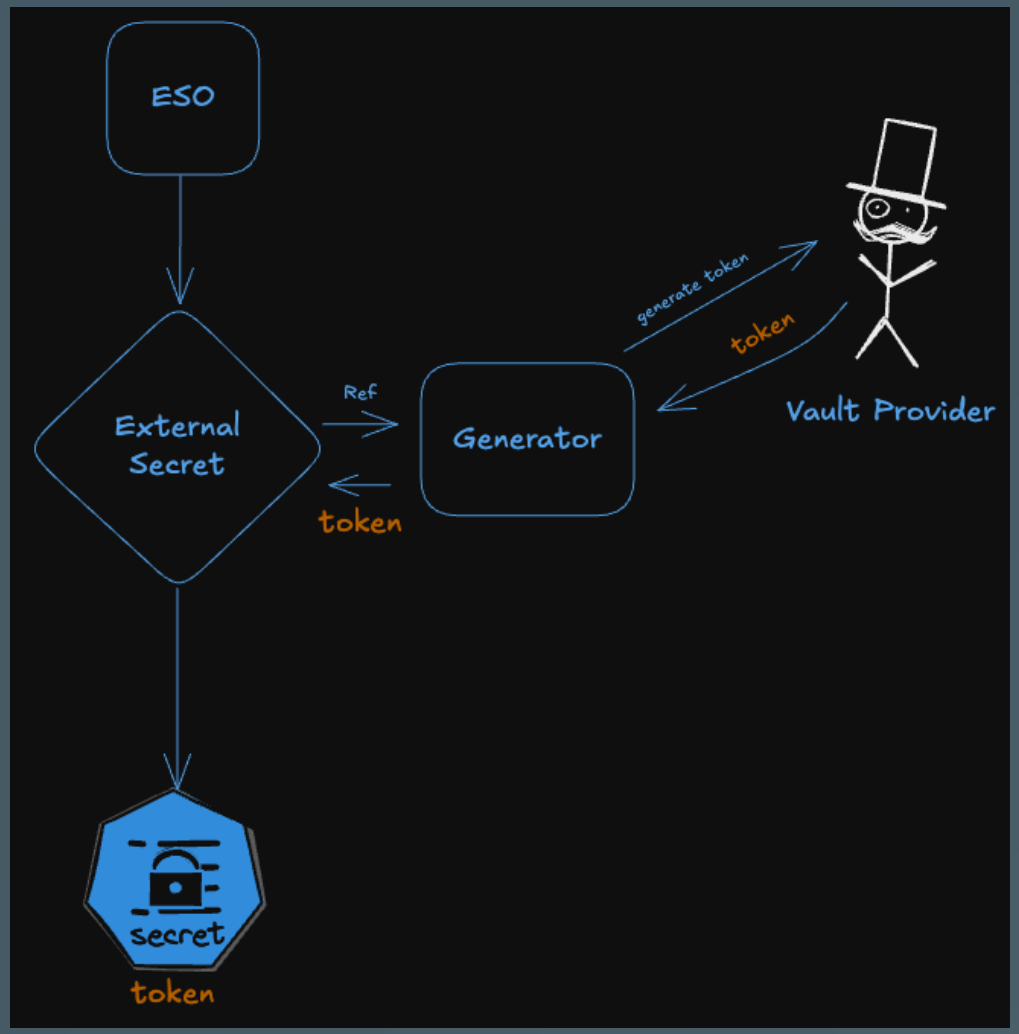
```yaml
apiVersion: external-secrets.io/v1beta1
kind: SecretStore
metadata:
  name: example
  namespace: example-ns
spec:
  controller: dev
  retrySettings:
    maxRetries: 5
    retryInterval: "10s"
  provider:

    # (1): AWS Secrets Manager
    aws: ...
    # (2) Hashicorp Vault
    vault: ...
    # (3): GCP Secret Manager
    gcpsm: ...
```

# ExternalSecret

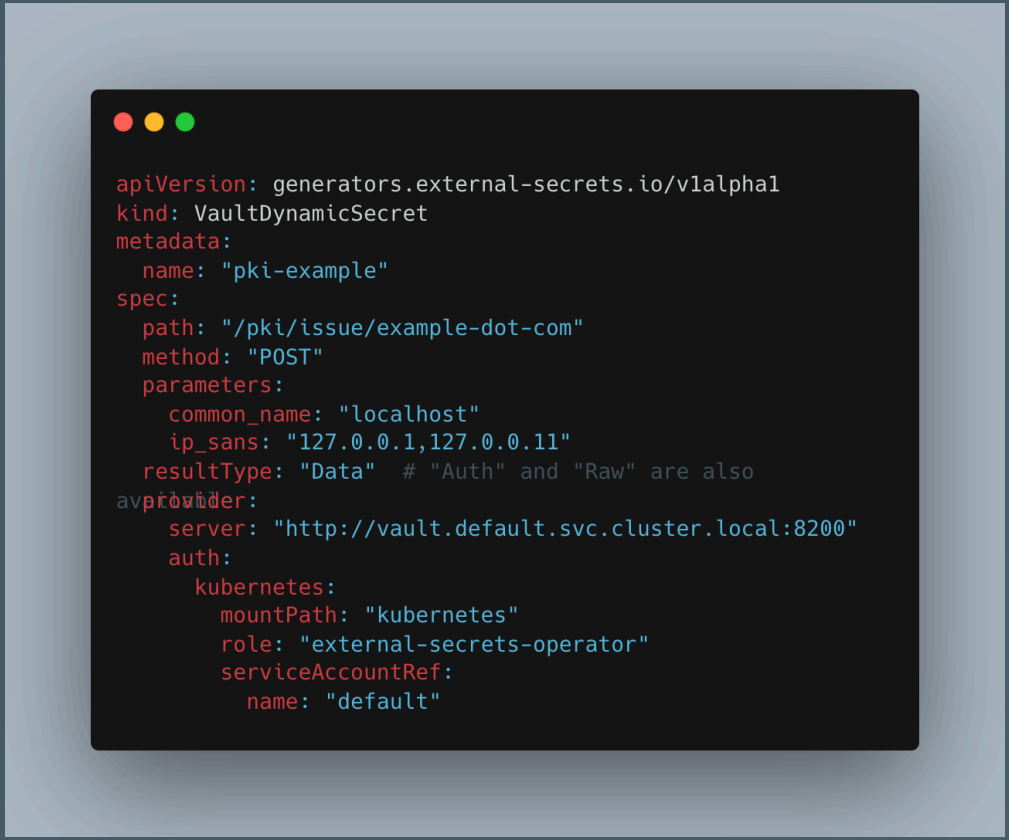


```yaml
apiVersion: external-secrets.io/v1beta1
kind: ExternalSecret
metadata:
  name: "hello-world"
spec:
  secretStoreRef:
    name: aws-store
    kind: SecretStore  # or ClusterSecretStore
  refreshPolicy: Periodic
  refreshInterval: "1h"
  target:
    # The secret name of the resource
    # Defaults to .metadata.name of the ExternalSecret
    # It is immutable
    name: application-config
    creationPolicy: Merge
    deletionPolicy: Retain
  data:
    - secretKey: username
      remoteRef:
        key: database-credentials
        version: v1
```

# What are generators



# Vault Dynamic Secret Generator

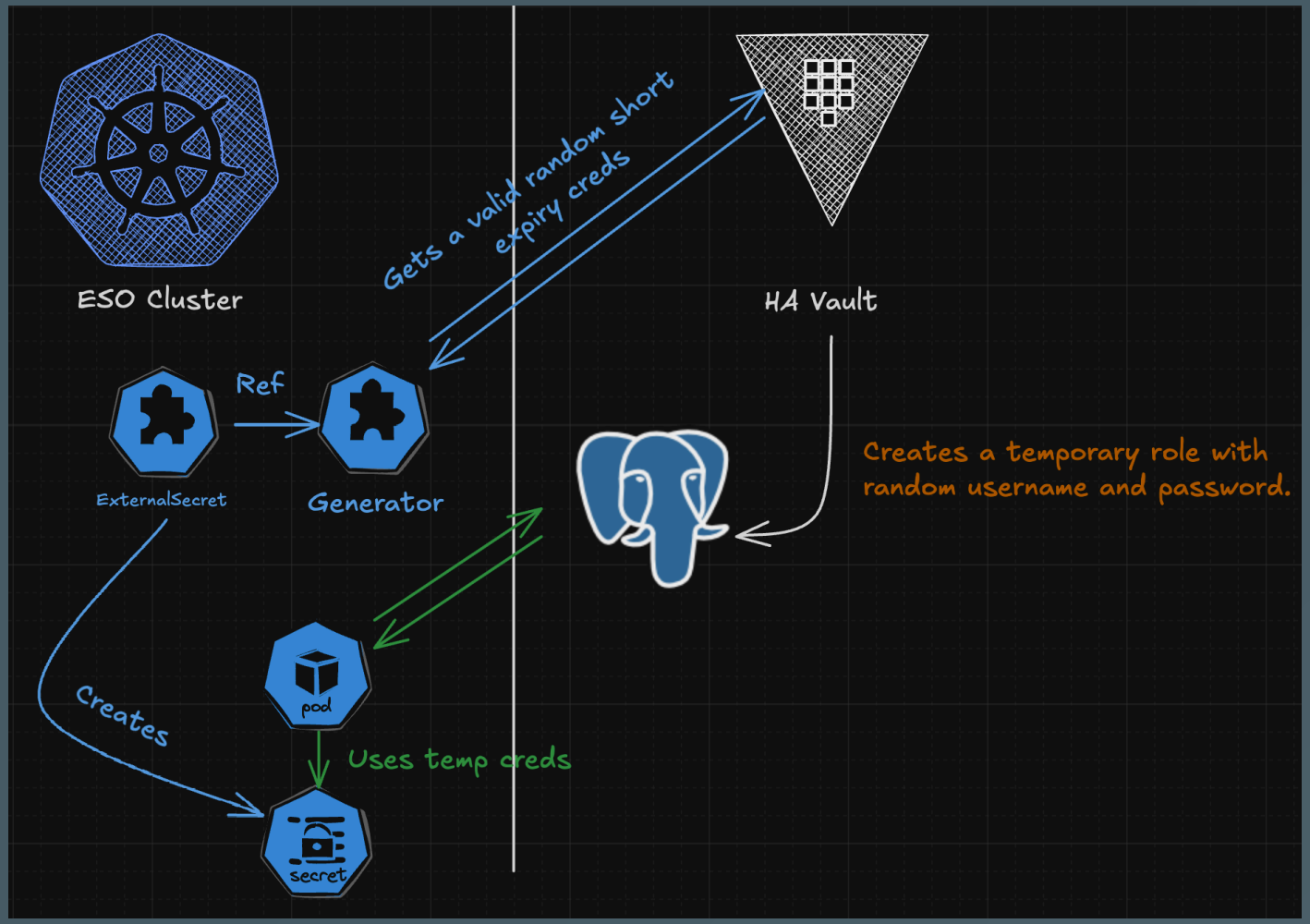


```yaml
apiVersion: generators.external-secrets.io/v1alpha1
kind: VaultDynamicSecret
metadata:
  name: "pki-example"
spec:
  path: "/pki/issue/example-dot-com"
  method: "POST"
  parameters:
    common_name: "localhost"
    ip_sans: "127.0.0.1,127.0.0.11"
  resultType: "Data"  # "Auth" and "Raw" are also
  provider:
    server: "http://vault.default.svc.cluster.local:8200"
    auth:
      kubernetes:
        mountPath: "kubernetes"
        role: "external-secrets-operator"
        serviceAccountRef:
          name: "default"
```

# Different Generator Types

- Azure Container Registry
- AWS Elastic Container Registry
- AWS STS Session Token
- Google Container Registry
- Quay
- Vault Dynamic Secret
- Password
- Webhook ( *any* type )
- Github
- UUID

# What we are trying to achieve



# Demo

Rotation demo

# Reloader

Demo if time allows

# Drawbacks

- No second secret rotation process ( where you switch over to a second secret instead of updating
  the current one )
- Race condition can occur when rotation happens at the wrong time ( retry )

# Conclusion

Thank you for listening!
Gergely.
@Skarlso