



# **External Secrets Operator**

die Werkzeugkiste fürs Secret Management



## Moritz Johner

Senior Software Engineer bei **FORM3**  
Maintainer @external-secrets



[@moolen](https://github.com/moolen)

# Agenda

- Secret Management
- External Secrets Operator
- Demo

# Was ist Secret Management

...und warum brauche ich das?

# Secret Management

Es geht um **Daten** wie:

- API Schlüssel, Zertifikate
- (kurzlebige) Anmeldeinformationen, geteilte Passwörter

...und das **Drumherum**:

- Werkzeuge, Prozesse, Lifecycle Management

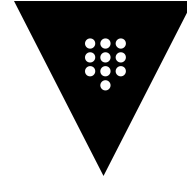
Schnittmenge mit: PAM, Passwort Manager, KMS, Config Management

# Warum? Risikomanagement!

- Böswilliger Akteur
- Exfiltration von Daten
- Wirtschaftsspionage, Sabotage, \$\$\$
- Ransomware

# Secret Management Systeme

- Sichere Speicherung & HSM Integration
- Auditierung & SIEM Integration
- Authn, Authz & ACLs
- Lebenszyklus APIs & Integrationen
- kurzlebige Zugänge bereitstellen
- MFA, Hardware Token & PAM



# Herausforderungen



Fragmentierung



Zugriffsmanagement & Lebenszyklus



Integration & Tooling



schlechte Praktiken



# Perspektive einer Anwendung

- Anwendungen brauchen Secrets
  - aus Umgebungsvariablen, Dateien oder Netzwerk
- z.B. Zertifikate, API Schlüssel, DB Zugangsdaten, sonstige sensiblen Daten
- keine Kontrolle bei Legacy Software und Fremdcode
  - z.B. Prometheus, external-dns & flux

# Integration in Kubernetes



viele, viele Integrationspunkte

> in-app vs. sidecar vs. admission ctrl vs. CSI vs. controller



gängige Tools

> verschlüsselt im Repo: **Sealed Secrets** / **SOPS**

> referenzen im Repo: **External Secrets Operator** / **Secret Store CSI Driver**

> sidecar: **vault sidecar injector**



Denkanstöße

> Konsumenten, Sicherheitsschranken & Prozesse



# Secret Management mit External Secrets Operator



# Zeitleiste

- vor 2019: Ursuppe der Secret Management
- 2019: Ankündigung **godaddy/kubernetes-external-secrets**
- 2020: Rewrite 👉 **external-secrets/external-secrets**
- 2021: Abkündigung **godaddy/kubernetes-external-secrets**
- 2022: Beitritt CNCF, Sponsorship von Container Solutions, Form3 & Pento
- Joint Venture von mehreren Projekten, siehe [#47](#)
- ~2k commits von 160 Mitwirkenden

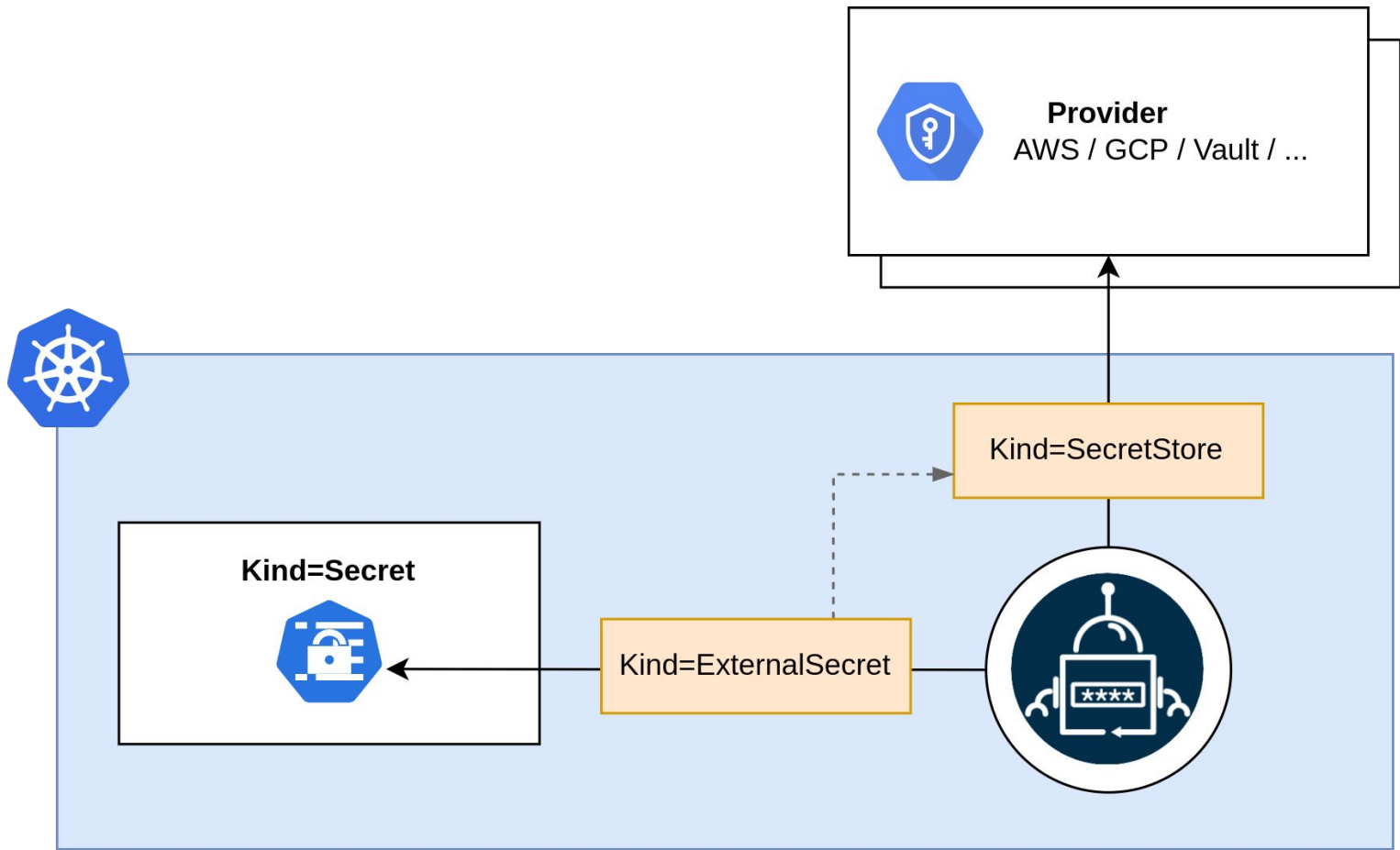


Kind=Secret




**Provider**  
AWS / GCP / Vault / ...





```
apiVersion: external-secrets.io/v1beta1
kind: ExternalSecret
metadata:
  name: "hello-world"
spec:
  secretStoreRef:
    name: "secret-store-name"
  refreshInterval: "1h"
  target:
    name: "my-api-key"
  data:
    - secretKey: "mysecret"
      remoteRef:
        key: "/applications/foo/apikey"
```

A horizontal line connects the value "secret-store-name" under the secretStoreRef.name field in the ExternalSecret to the name field in the SecretStore.

```
apiVersion: external-secrets.io/v1beta1
kind: SecretStore
metadata:
  name: "secret-store-name"
spec:
  provider:
    aws:
      service: SecretsManager
      region: "eu-central-1"
      auth:
        jwt:
          serviceAccountRef:
            name: "my-serviceaccount"
```

# Features



zeroconf authentication



designed für multi-tenancy



lifecycle management



verteilung von secrets über namespaces hinweg



cross-cluster sync



secret templating

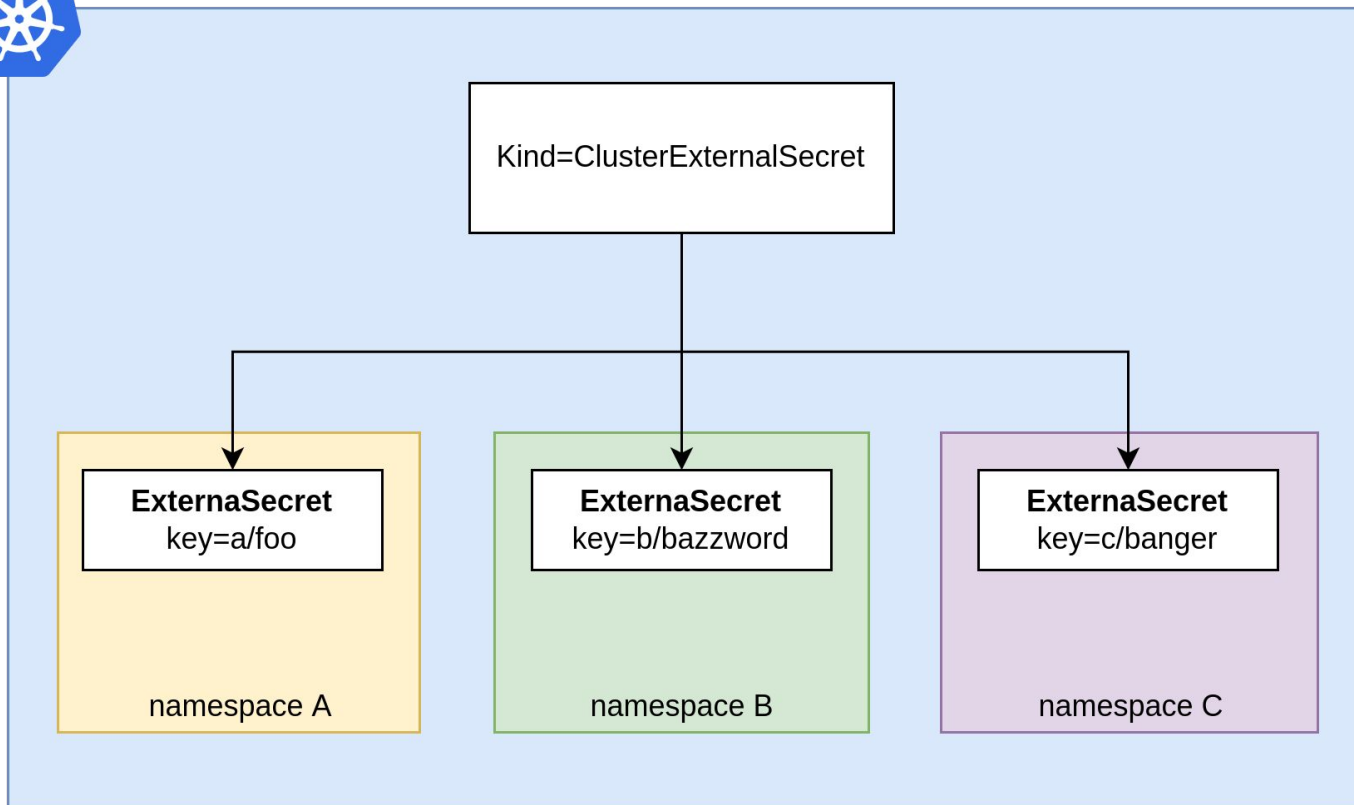


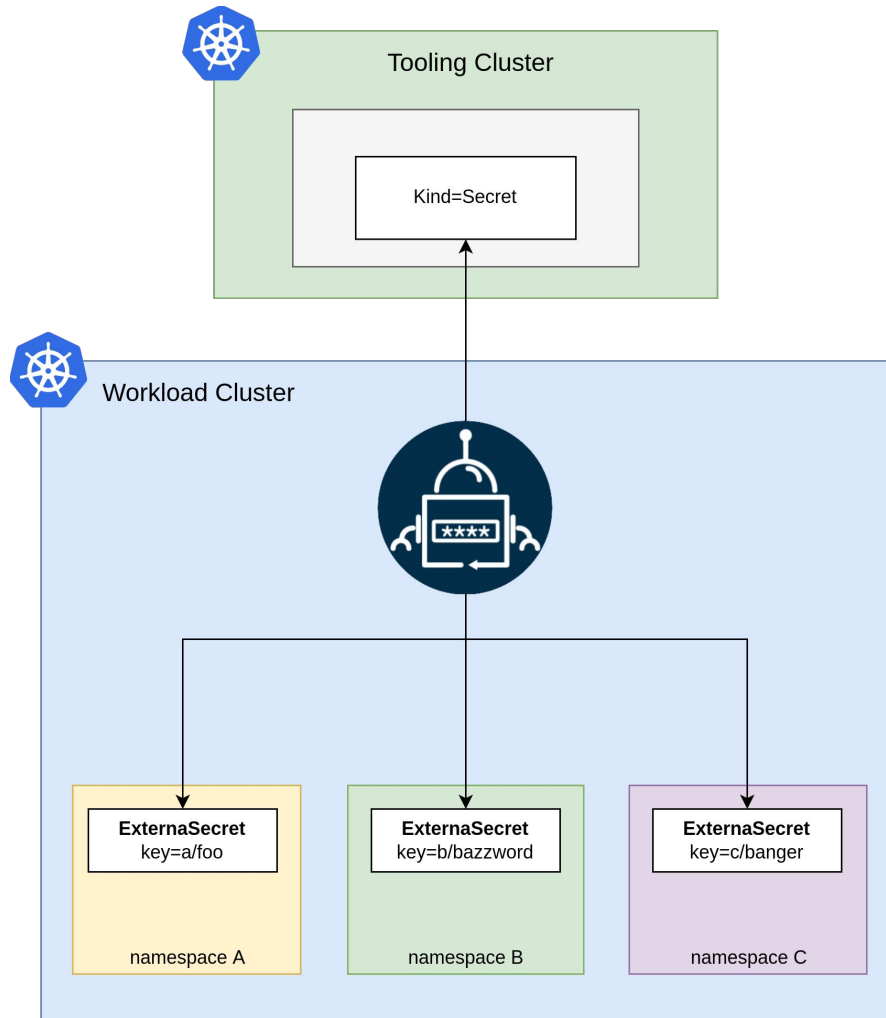
extract secrets von json/yaml

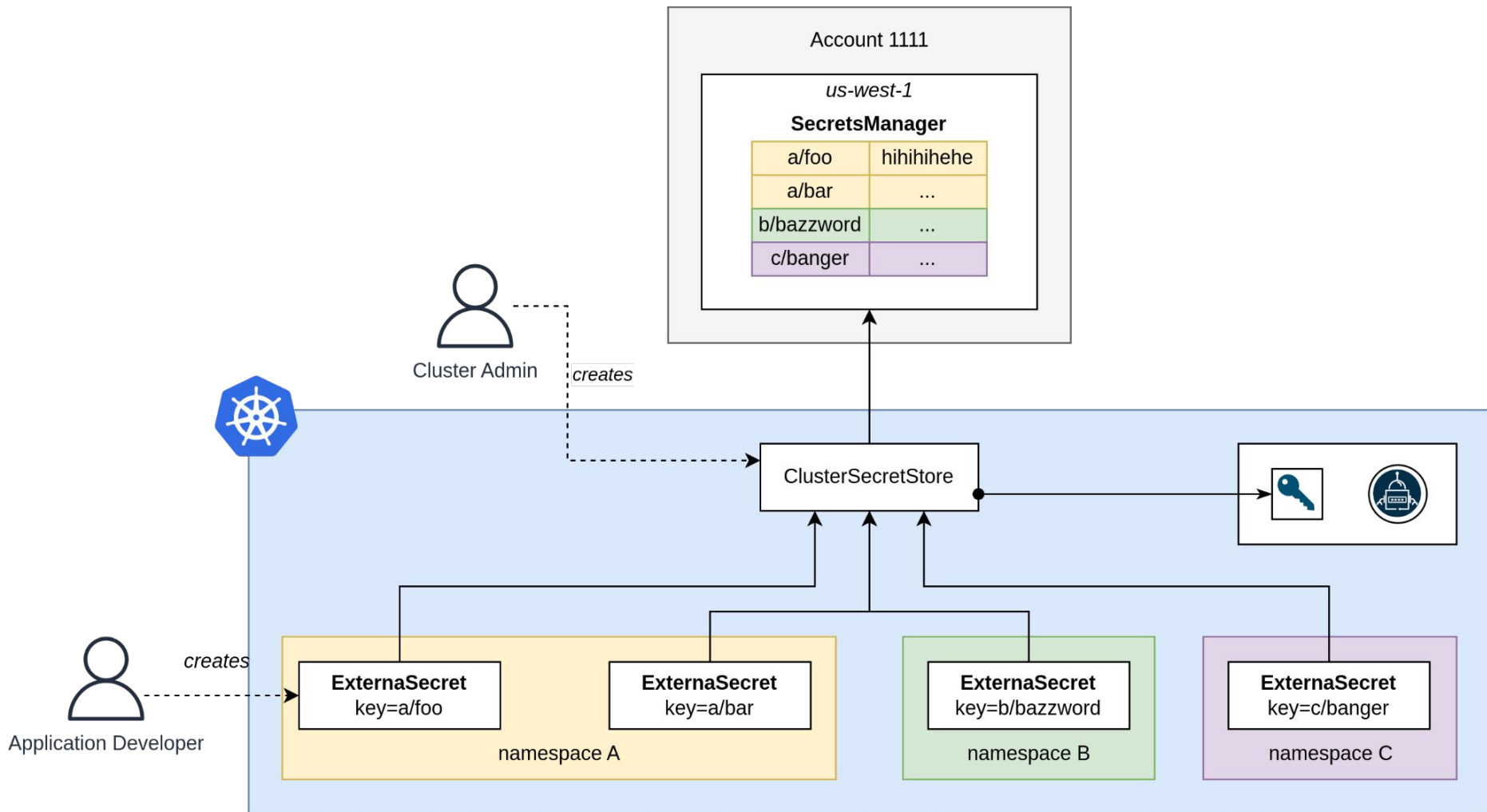


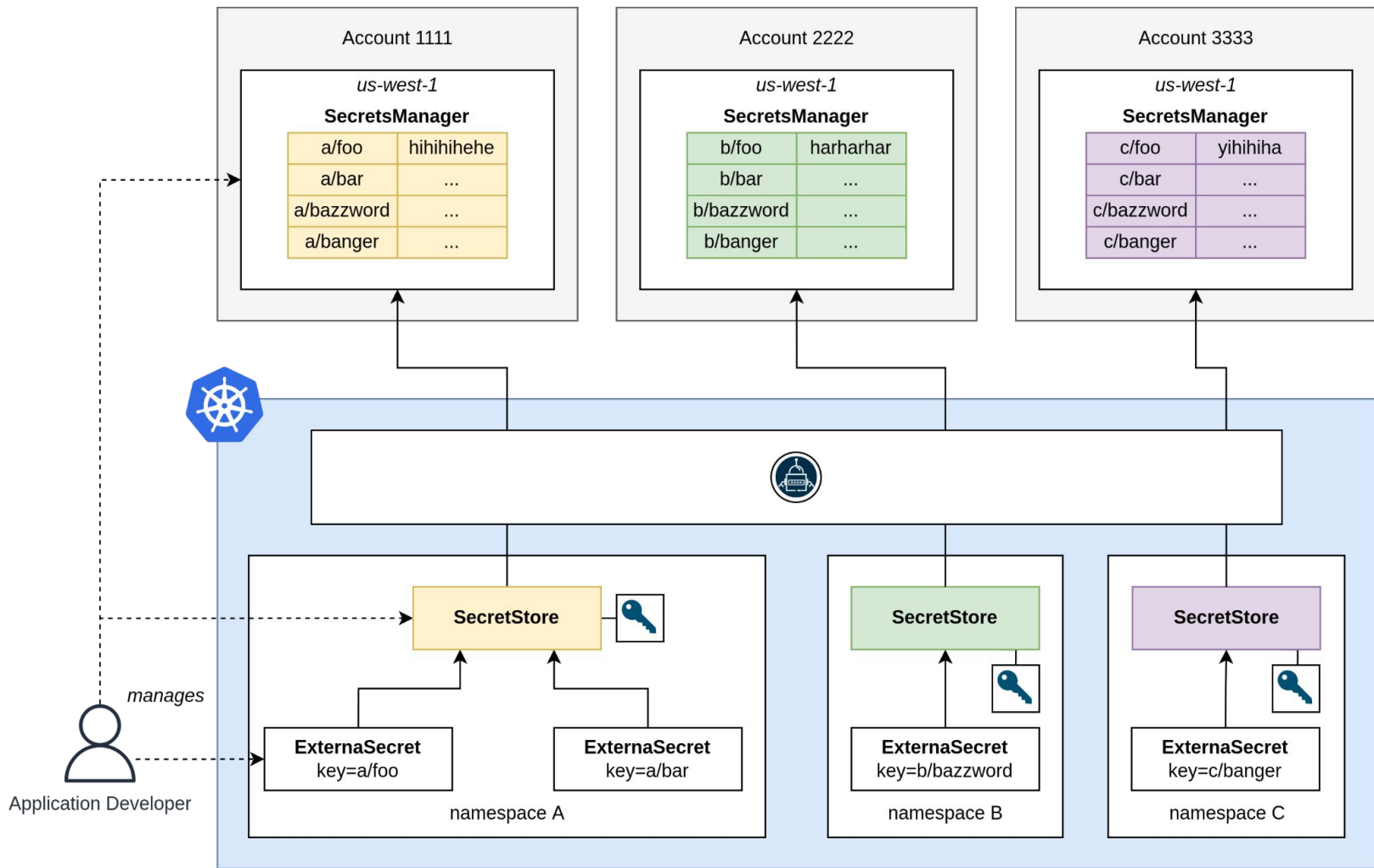
fetch & aggregate multiple secrets











# Ausblick

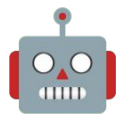
- Push Secrets
- Secret Generator
- contributor & maintainer gesucht ;)

## Wo ihr uns findet

Kubernetes slack **#external-secrets**

<https://external-secrets.io/>

[github.com/external-secrets/external-secrets](https://github.com/external-secrets/external-secrets)



Demo



Dankeschön

 Fragen 