Deep dive into **Kubernetes** secrets

Márk Sági-Kazár
@sagikazarmark
https://sagikazarmark.hu
hello@sagikazarmark.hu

Hello!

Márk Sági-Kazár

Engineering Technical Lead @ Cisco

@sagikazarmark

https://sagikazarmark.hu

hello@sagikazarmark.hu

Myth: Kubernetes secrets aren’t secure

Kubernetes secrets

Store sensitive information

Inject into containers

- as files
- as environment variables

Kubernetes secret example

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: my-secret
type: Opaque
data:
  foo: YmFyCg==
```

Kubernetes secret example

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: my-secret
type: Opaque
data:
  foo: YmFyCg==
```

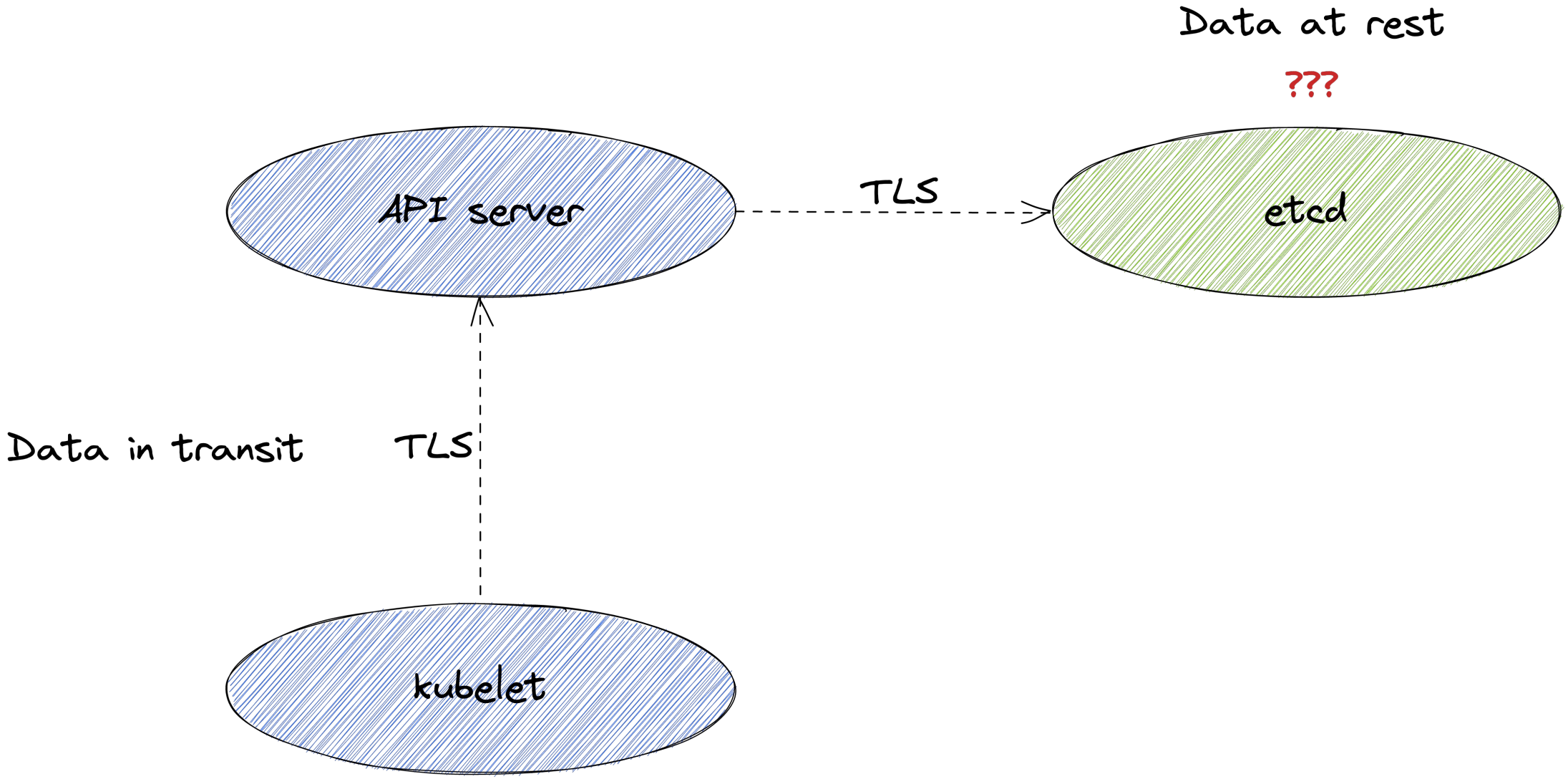

THAT'S NOT ENCRYPTED

This isn’t encrypted either

```
$ vault kv get secret/my-secret
====== Data ======
Key         Value
---         -----
foo         bar
```

base64 is **encoding**, not *encryption*

Kubernetes data (states)



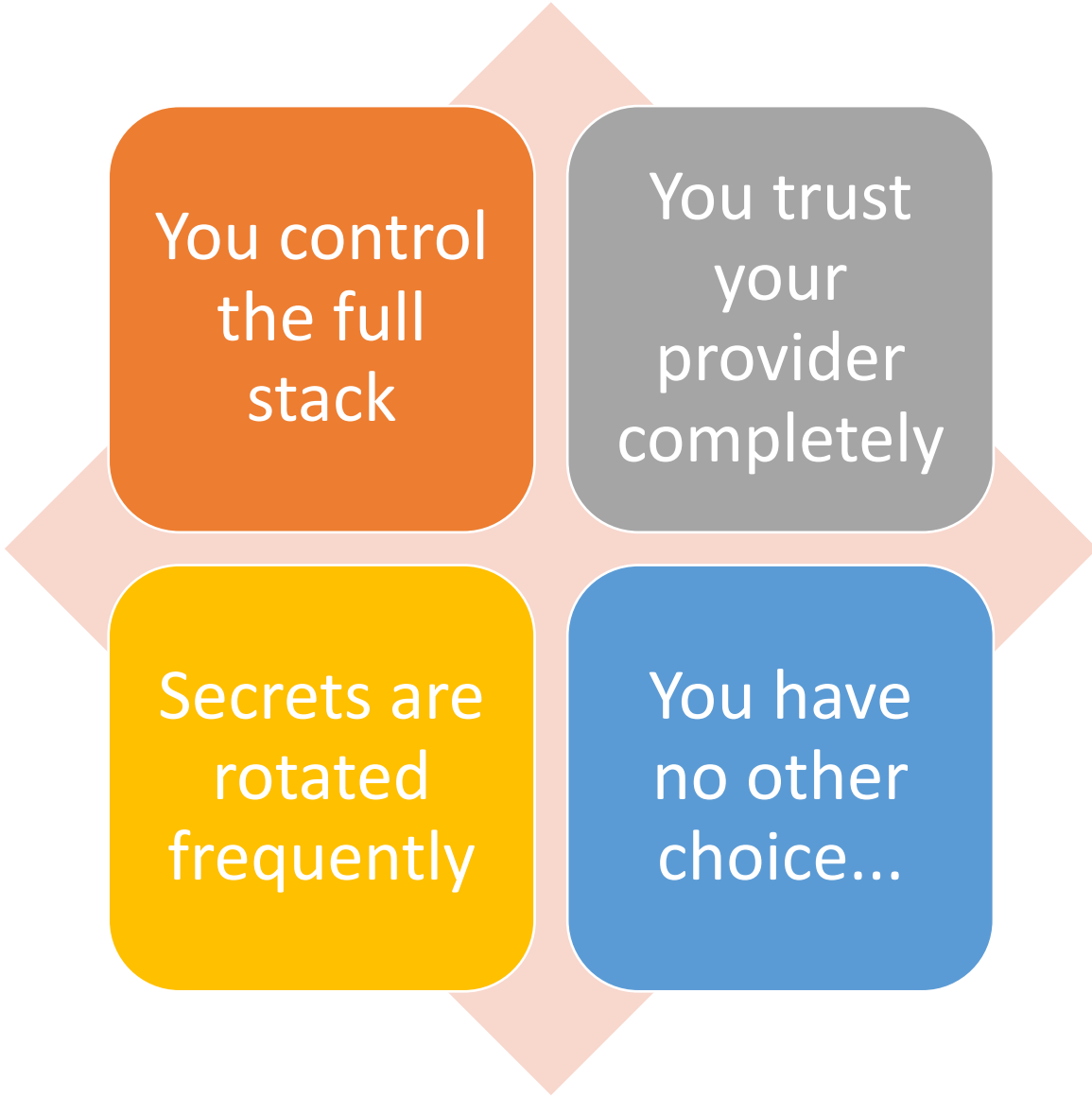
Encryption at rest

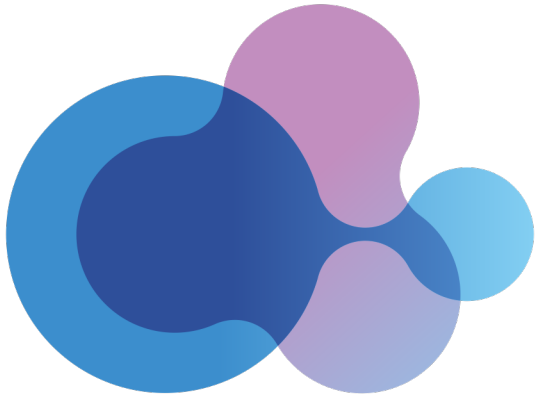
- API server config: „encryption config”
- encrypt secrets before storing (in etcd)
- Plaintext by default!

Myth: Kubernetes secrets aren’t secure

- Secrets are stored in plaintext by default (encryption is optional)
- No control over managed services (trust, compliance)
- RBAC needs to be configured properly
- BUT: base64 is not the reason!!!

When should you use Kubernetes secrets?





bank-vaults
BY BANZAICLOUD

CISCO

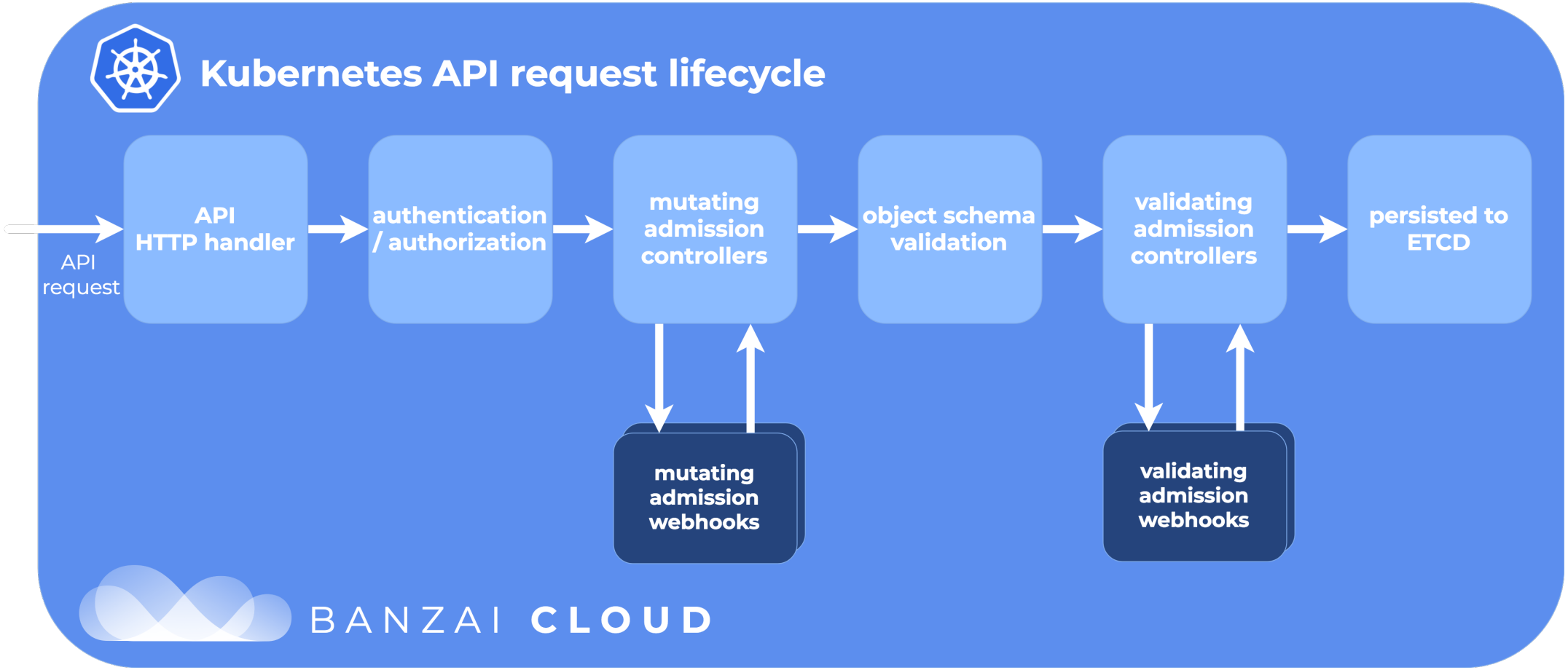
Swiss-army knife for Hashicorp Vault on Kubernetes

Secrets are stored safely in Vault

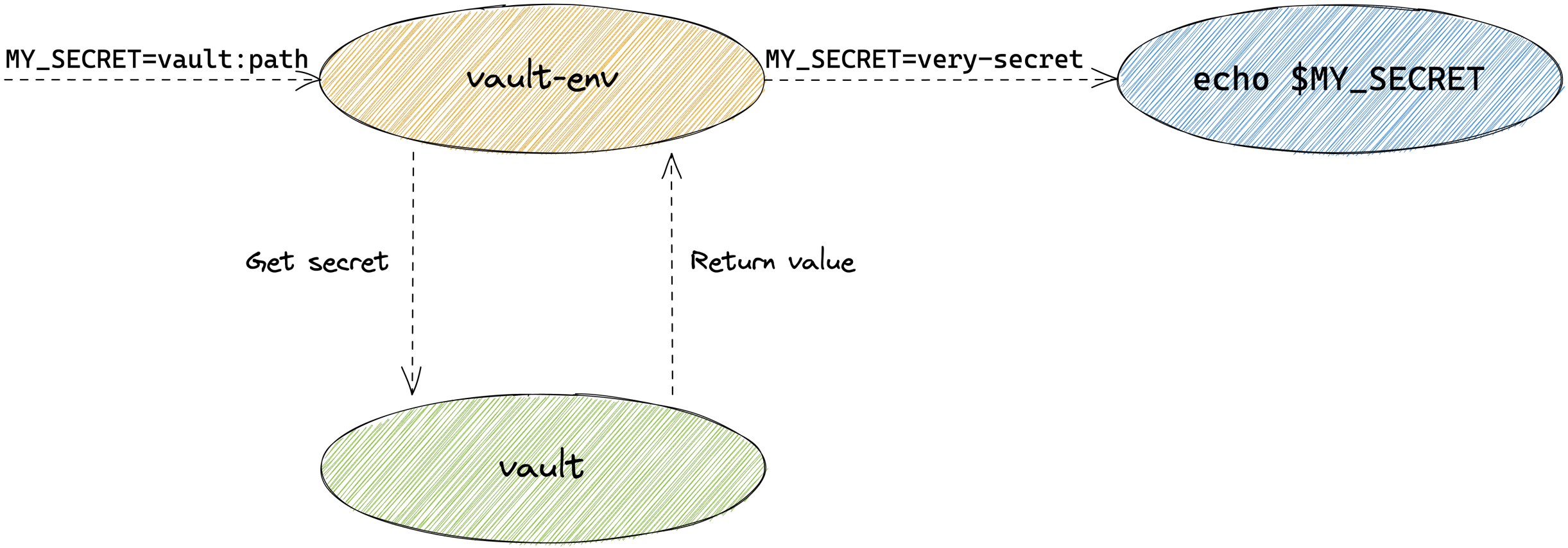
Secret values are injected directly into pods

https://github.com/banzaicloud/bank-vaults

Mutating webhook



Retrieve secret from Vault



Caveats

- Webhook unavailable: you can’t launch new pods
- Vault unavailable: your app won’t function properly
- Webhook misconfigured: Kubernetes mutates every pod

kube-secrets-init

- mutating webhook for AWS/GCP secret stores
- inspired by Bank-Vaults
- Same caveats as for Bank-Vaults
- https://github.com/doitintl/kube-secrets-init

External secrets

- Synchronize secrets from external sources...
- ...to Kubernetes Secret objects...
- ...based on CRDs
- Vault, AWS Secret Manager, GCP Secret Manager, etc

Secret changes?

- Secrets are updated by Bank Vaults/kube-secrets-init/External Secrets
- How does the workload notice the secret changed?
- Not many solutions out there
- https://github.com/stakater/Reloader
- Works well with External Secrets

Demo

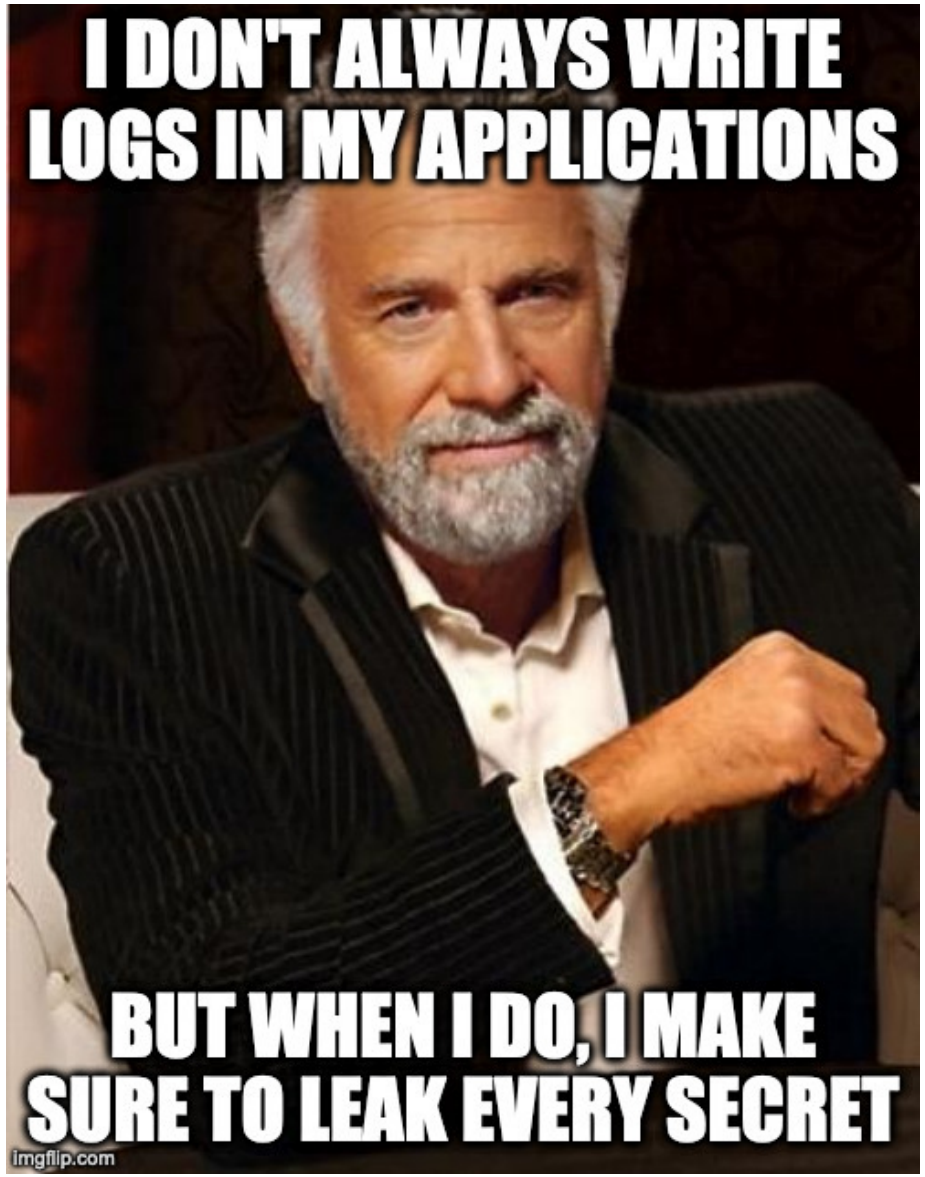
- kube-secrets-init
- External secrets
- https://github.com/sagikazarmark/gdg-budapest-demo-20220922

Wait, there is more.....

Root users can still access everything

You are an `exec` away from secrets

Secrets can be leaked




ROTATE
ALL THE SECRETS
imgflip.com

Any questions?

Hint: There are no stupid questions

Márk Sági-Kazár
@sagikazarmark
https://sagikazarmark.hu
hello@sagikazarmark.hu