



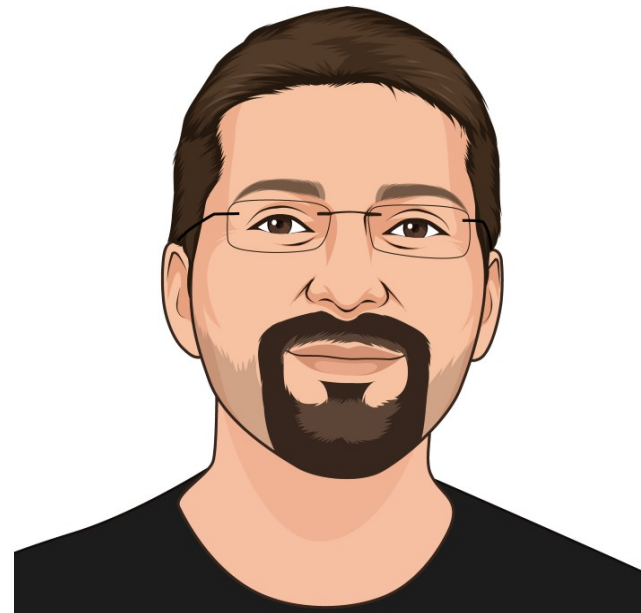
How to use Secrets with GitOps and ArgoCD

Kostis Kapelonis

Your host: Kostis Kapelonis



- Developer Advocate
- Company: Codefresh CI/CD/Gitops
- Check codefresh.io/blog
- Ex-Java dev (10+ years)
- Ex-Release manager (5+ years)
- Member of Argo Rollouts Github Org



Kubernetes secrets



Kubernetes secrets explained



```
apiVersion: v1
kind: Secret
metadata:
  name: secret-sa-sample
  annotations:
    kubernetes.io/service-account.name: "sa-name"
type: kubernetes.io/service-account-token
data:
  # You can include additional key value pairs as you do with Opaque Secret
  extra: YmFyCg==
```

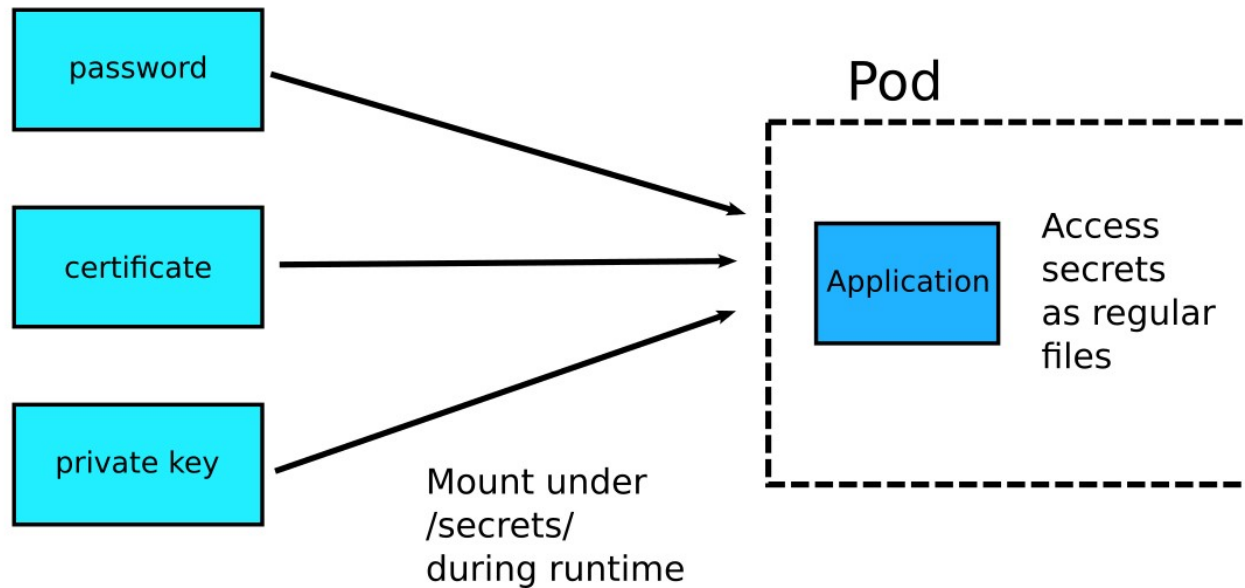
**This is just base64 encoding!
NEVER commit secrets to Git
Anybody can access them**

```
→ Kostis echo YmFyCg== | base64 -d
bar
```



Kubernetes secrets explained

Kubernetes
Secrets (not encrypted)



GitOps and secrets



How to handle secrets with GitOps



There is no standard practice for managing secrets with GitOps

This is a very well known problem with GitOps, so I am including it for completeness. Secret handling is one of the most important aspects of software deployment and yet, GitOps does not address them.

There is no single accepted practice on how secrets should be managed. If they are stored in Git, they need to be encrypted and thus have their own workflow process during a deployment. If they are not stored in Git, then the whole idea of having your cluster state the same as Git is not true anymore.

Secrets management is one of those areas where each company does their own thing, so at the very least I would expect GitOps tools to offer an out of the box solution for them.

<https://codefresh.io/about-gitops/pains-gitops-1-0/>

Secret Management

Argo CD is un-opinionated about how secrets are managed. There's many one-size-fits-all solutions. Here's some ways people are doing GitOps sec

- [Bitnami Sealed Secrets](#)
- [GoDaddy Kubernetes External Secrets](#)
- [External Secrets Operator](#)
- [Hashicorp Vault](#)
- [Banzai Cloud Bank-Vaults](#)
- [Helm Secrets](#)
- [Kustomize secret generator plugins](#)
- [aws-secret-operator](#)
- [KSOPS](#)
- [argocd-vault-plugin](#)

For discussion, see [#1364](#)

[ArgoCD official Documentation](#)



How to handle secrets with GitOps



- GitOps = commit EVERYTHING in git
- Everything means secrets as well.
- Big catch: **Never** commit secrets in raw form

- Solution -> encrypt secrets and **then** commit them to Git
- Decrypt secrets at the **last possible moment** (just before they are needed)




Bitnami Sealed Secrets



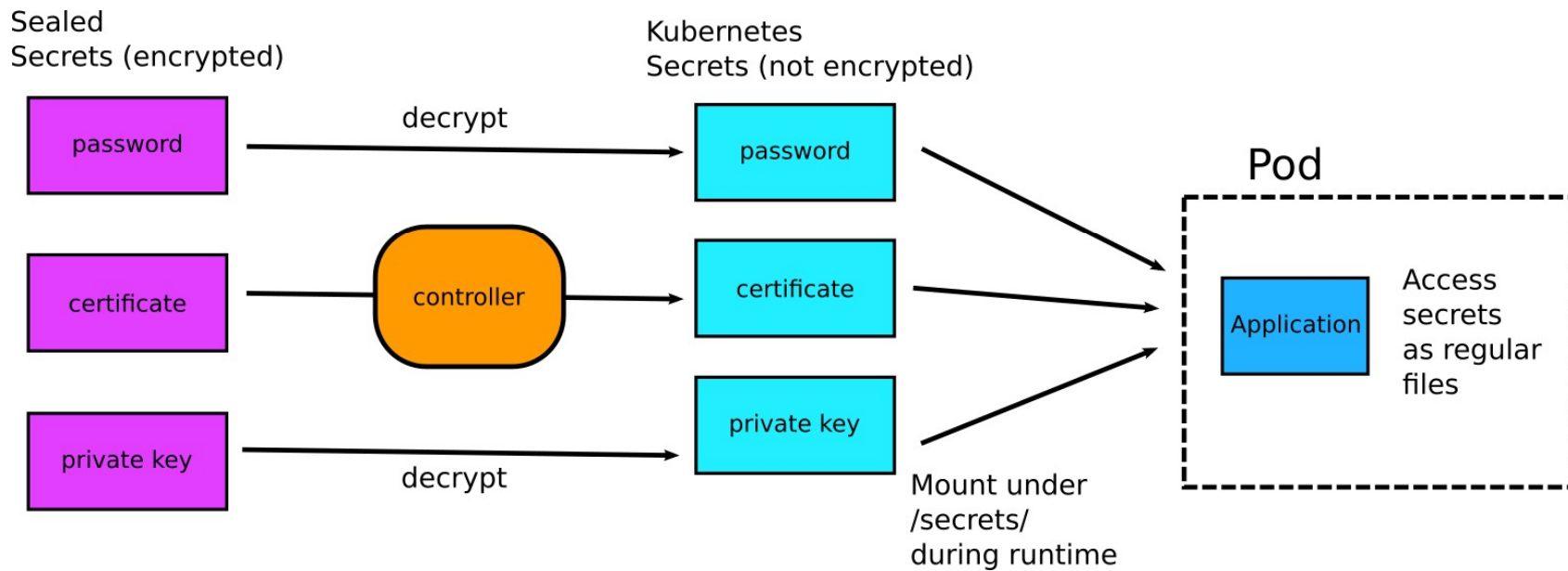
Sealed secrets controller

**This is actual encryption!
You CAN and should commit
Sealed secrets in Git**

```
apiVersion: bitnami.com/v1alpha1
kind: SealedSecret
metadata:
  name: mysecret
  namespace: mynamespace
spec:
  encryptedData:
    foo: AgBy3i40JSWK+PiTySYZZA9r043cGDEq.....
```



Sealed secrets controller

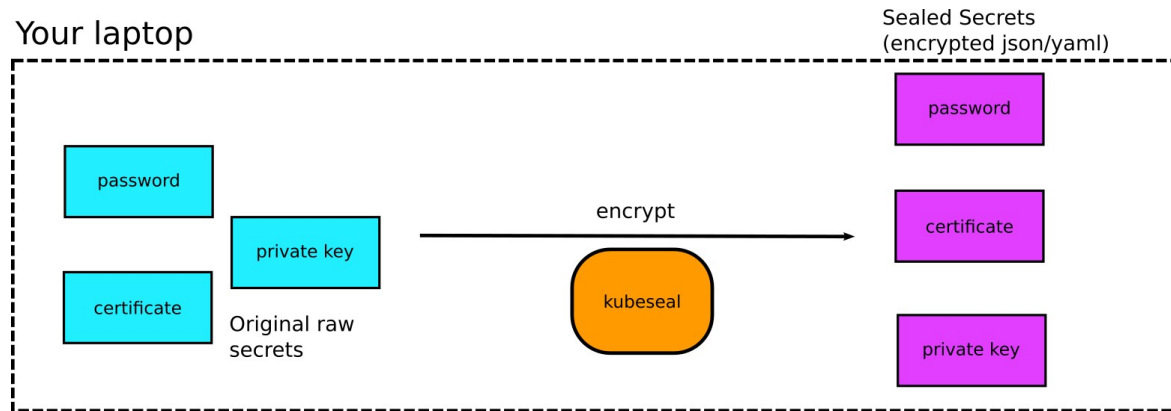


How the Sealed Secrets Controller works

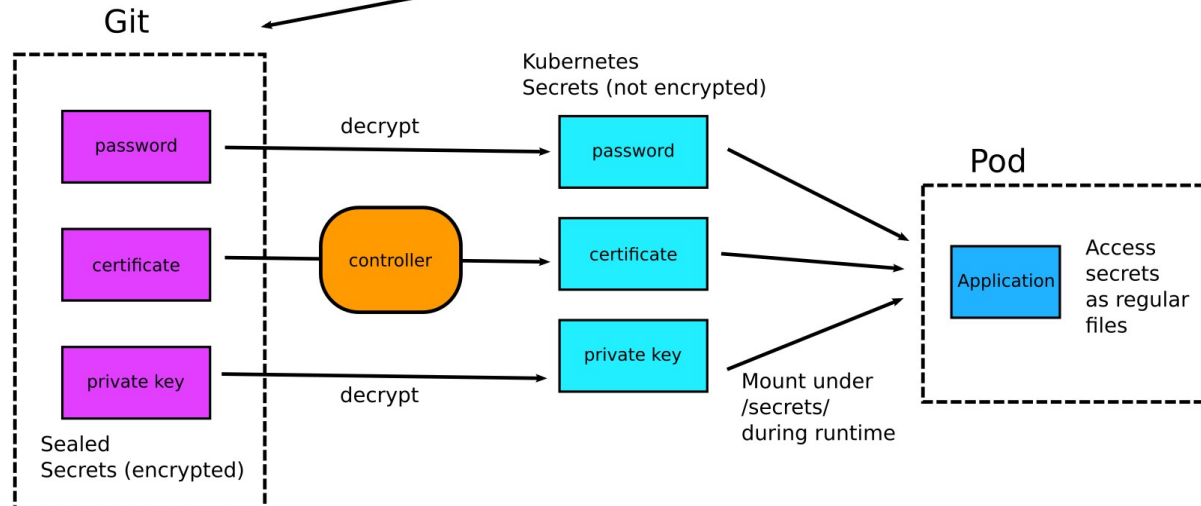


- The controller has a public/private key
- Private key stays always within the cluster
- Private key is used to decrypt secrets
- Public key is accessible to everybody
- Public key is used by kubeseal executable





commit to Git



Demo application



Secrets are always hard



- How to maintain/upgrade the Sealed Secrets controller itself?
- How to store/backup the private/public key?
- How to update the controller and change the keys?
- How to rotate secrets?
- How to handle leaked secrets?

The controller is now a critical piece of your infrastructure



Resources



Argo CD - <https://argo-cd.readthedocs.io/en/stable/operator-manual/secret-management/>

GitOps Pain points- <https://codefresh.io/about-gitops/pains-gitops-1-0/>

Sealed secrets controller- <https://github.com/bitnami-labs/sealed-secrets>

Using Sealed secrets- <https://codefresh.io/about-gitops/handle-secrets-like-pro-using-gitops/>

Example repo - <https://github.com/codefresh-contrib/gitops-secrets-sample-app>

Mozilla SOPS- <https://github.com/mozilla/sops>

SOPS example- <https://codefresh.io/docs/docs/yaml-examples/examples/decryption-with-mozilla-sops/>

