
KubeCon
CloudNativeCon
North America 2024

KubeCon CloudNativeCon
North America 2024

Best friends keep no secrets: going secretless with cert-manager

Tim Ramlot
cert-manager maintainer - Software engineer @ Venafi a CyberArk company

Ashley Davis
cert-manager maintainer - Software engineer @ Venafi a CyberArk company

KubeCon CloudNativeCon
North America 2024

Best friends keep no secrets: going secretless with **cert-manager**

Tim Ramlot
cert-manager maintainer - Software engineer @ Venafi a CyberArk company

Ashley Davis
cert-manager maintainer - Software engineer @ Venafi a CyberArk company

What's cert-manager?

cert-manager is the best way to get X.509 certificates in Kubernetes

- Use Kubernetes API to request certificates
- Automated issuance and renewal
- Usable for both server and client authentication

Application

Request an X.509 certificate

Return a chain of signed certificates

Certificate Authority

Eg. ACME, Venafi, Vault, AWS, GCP

CNCF graduated project

427+ contributors

12k GitHub stars

20M monthly chart downloads

We’re looking for contributors!

- New contributors always welcome!
- Clear pathway to maintainership!
- Come talk to us after
- Or at the cert-manager booth

https://cert-manager.io/docs/contributing/

KubeCon | CloudNativeCon
North America 2024

Best friends keep no secrets: going **secretless** with cert-manager

Tim Ramlot
cert-manager maintainer - Software engineer @ Venafi a CyberArk company

Ashley Davis
cert-manager maintainer - Software engineer @ Venafi a CyberArk company

What's secretless?

secretless

= no secrets are shared between machines / transported over the wire

What's secretless?

secretless

= no secrets are shared between machines / transported over the wire

(as much as possible)

What's Secretless?

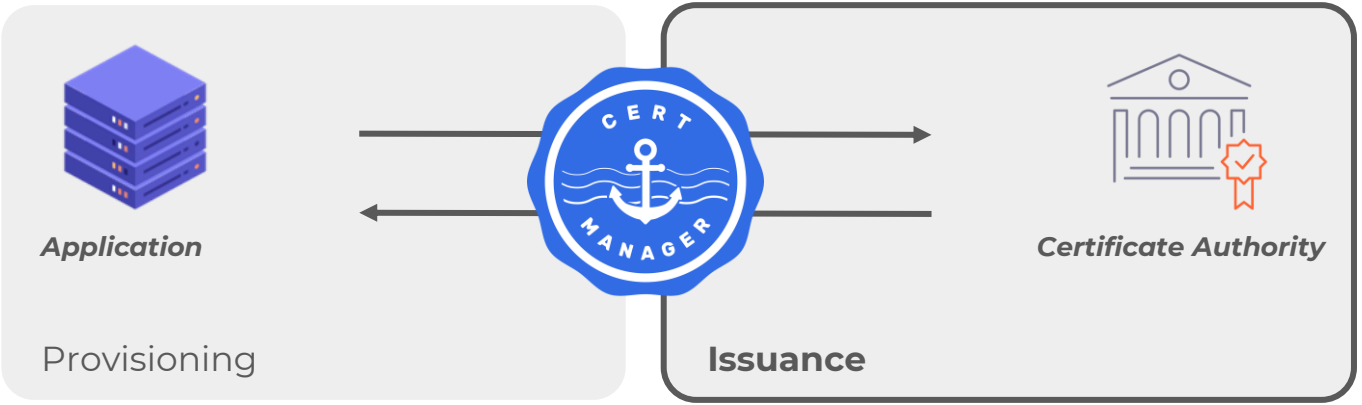
secretless = no secrets are shared between machines/ transported over the wire

and

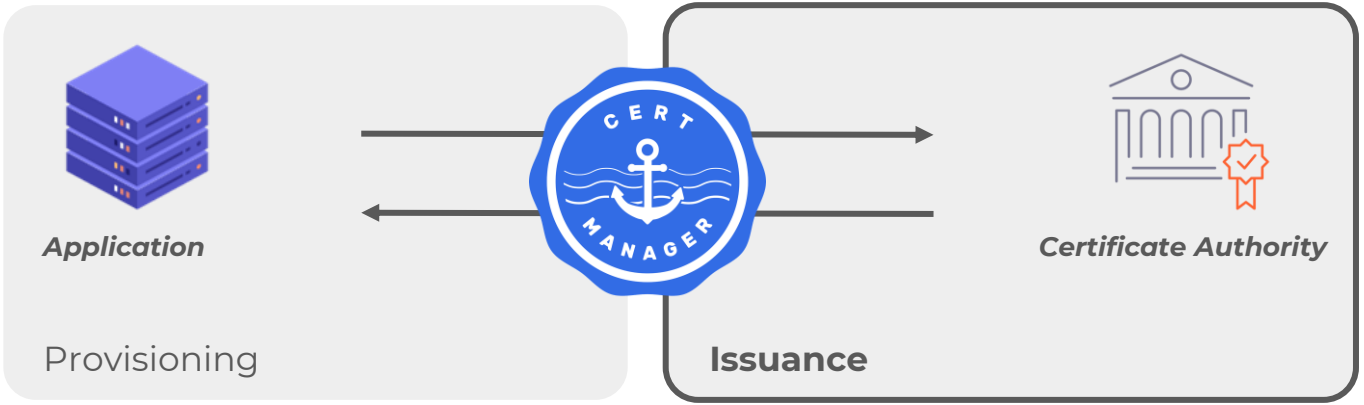
Secretless = no Kubernetes Secret resources are used

cert-manager Issuance

How does cert-manager issue a certificate?



How does cert-manager issue a certificate?



Integration with external CA

(eg. ACME, Venafi, Vault, AWS, GCP)

- requires **authentication**

Full list: https://cert-manager.io/docs/configuration/issuers/

Issuance

X.509 CSR

X.509 Cert

cert-manager issuer

in-tree issuer or out-of-tree issuer

Certificate Authority

Eg. Venafi, Vault, AWS, GCP, Let's Encrypt

Issuance

cert-manager issuer

in-tree issuer or out-of-tree issuer

Certificate Authority

Eg. Venafi, Vault, AWS, GCP, Let's Encrypt

Challenge: prove to CA that you own the identity and are allowed to submit this CSR

Simplest Solution: Static Secret

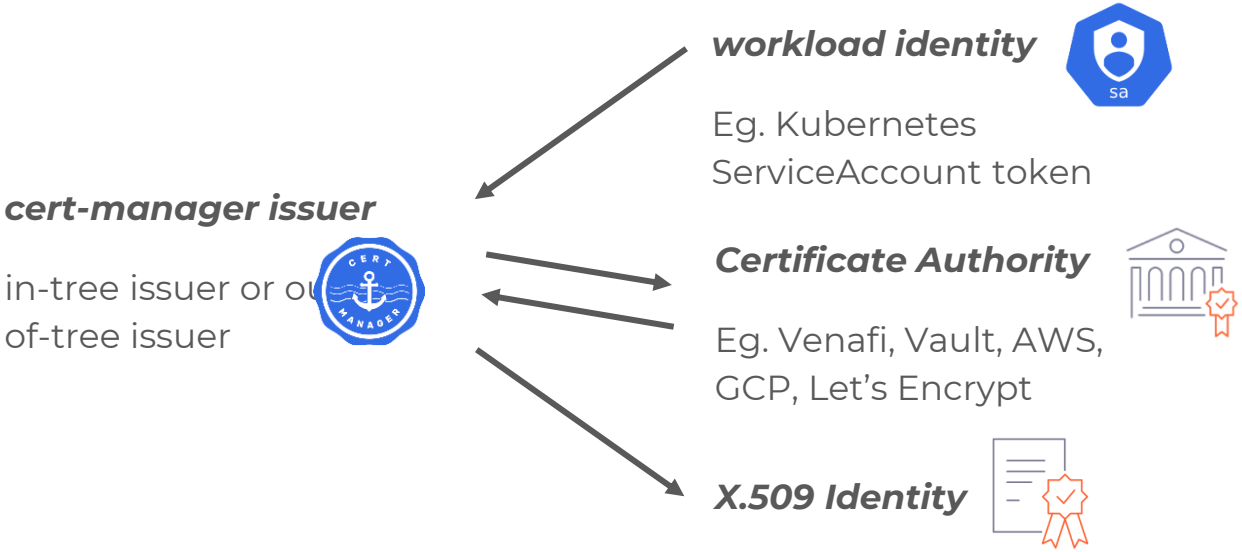

```yaml
apiVersion: cert-manager.io/v1
kind: Issuer
metadata:
  name: my-issuer
spec:
  vault:
    . . .
    auth:
      tokenSecretRef:
          name: my-token
          key: token
```

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: my-token
type: Opaque
data:
  token: "Abc123"
```

Issues with Static Secrets

- Need rotation
- High-value targets
- Usually manually set up
- E.g. Hard to do using GitOps

Better Solution: Workload Identity



Better Solution: Workload Identity


```
apiVersion: cert-manager.io/v1
kind: Issuer
metadata:
  name: my-issuer
  namespace: sandbox
spec:
  vault:
    . . .
    kubernetes:
       . . .
       role: my-role
       serviceAccountRef:
          name: my-sa
```

Workload Identity is “secretless”

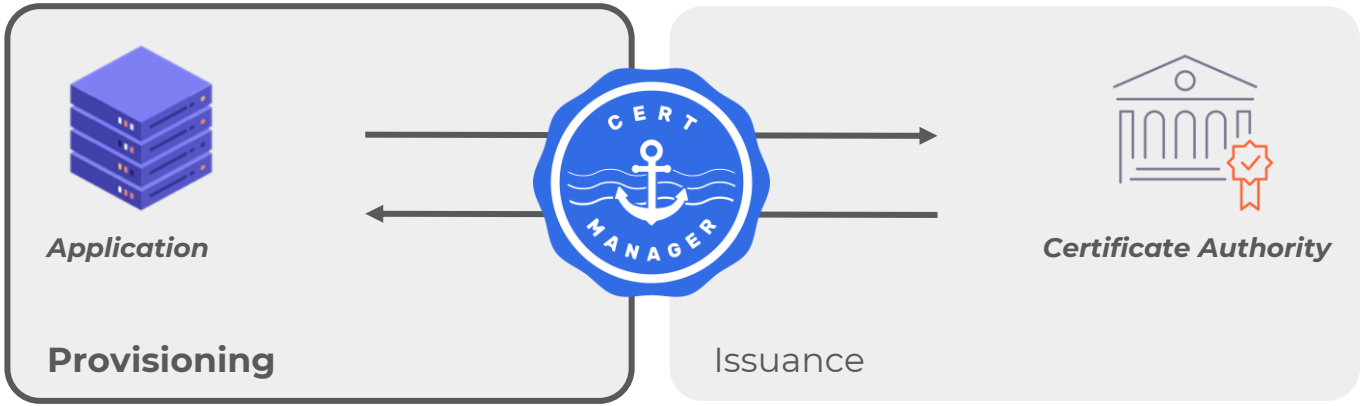
	static secret	signed tokens (e.g. JWT)
Restricting use	none	audience
Restricting validity	none	time-limited one-time-use*
How to trust	share the secret	trust public key
How to use	share the secret	share the JWT

Workload Identity is “secretless”

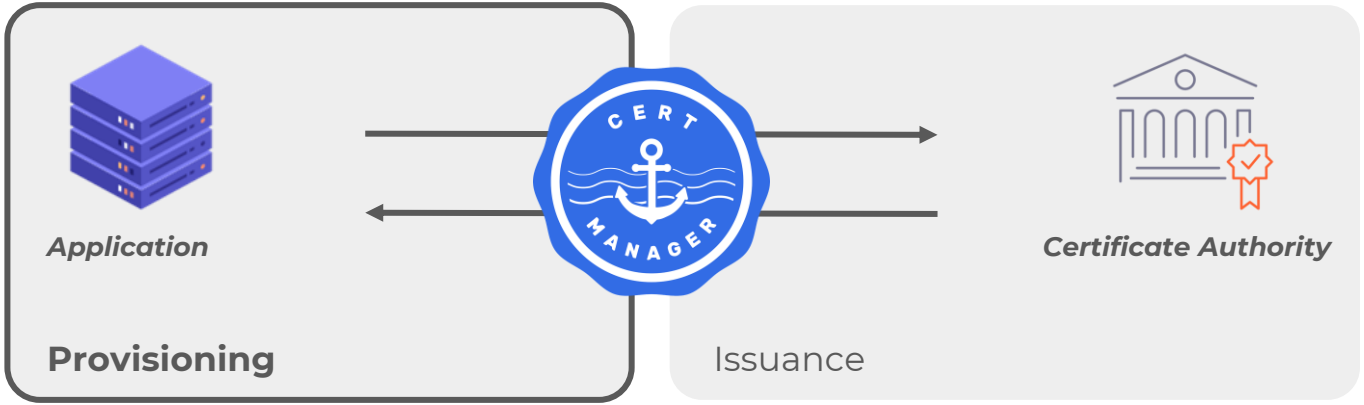
	static secret	signed tokens (e.g. JWT)	X.509
Restricting use	none	audience	embedded identity
Restricting validity	none	time-limited one-time-use*	time-limited
How to trust	share the secret	trust public key	trust public key
How to use	share the secret	share the JWT	use private key

cert-manager Provisioning

What does cert-manager provision?



What does cert-manager provision?

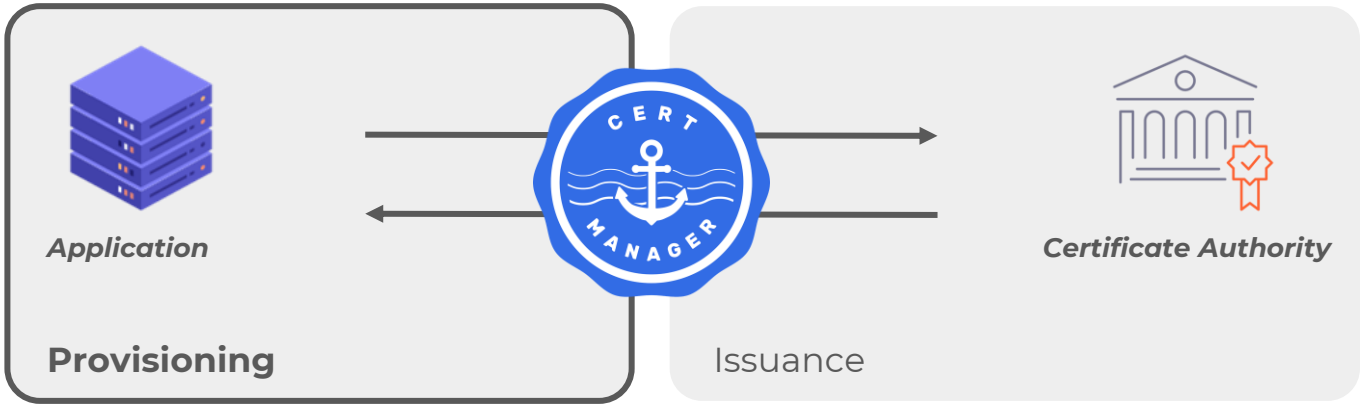


X.509 certificate + private key

Provisioned through:

- Kubernetes Secret resource
- CSI Volume mount *(csi-driver)*
- Service Mesh *(istio-csr)*

What does cert-manager provision?



X.509 certificate + private key

Provisioned through:

- Kubernetes Secret resource
- **CSI Volume mount (*csi-driver*)**
- Service Mesh (*istio-csr*)

A Secretless certificate


```
apiVersion: v1
kind: Pod
…
spec:
 …
 volumes:
    - name: spiffe
      csi:
        driver: csi.cert-manager.io
        readOnly: true
        volumeAttributes:
          csi.cert-manager.io/issuer-name: workload-issuer
          csi.cert-manager.io/issuer-kind: ClusterIssuer
          csi.cert-manager.io/issuer-group: cert-manager.io

          csi.cert-manager.io/dns-names: example.com
```

CSI driver

Request and provision certificate directly via Pod mount

+ no secrets in cluster state
+ private key does not leave machine
- new certificate must be issued when pod reschedules

https://cert-manager.io/docs/usage/csi-driver/

Demo

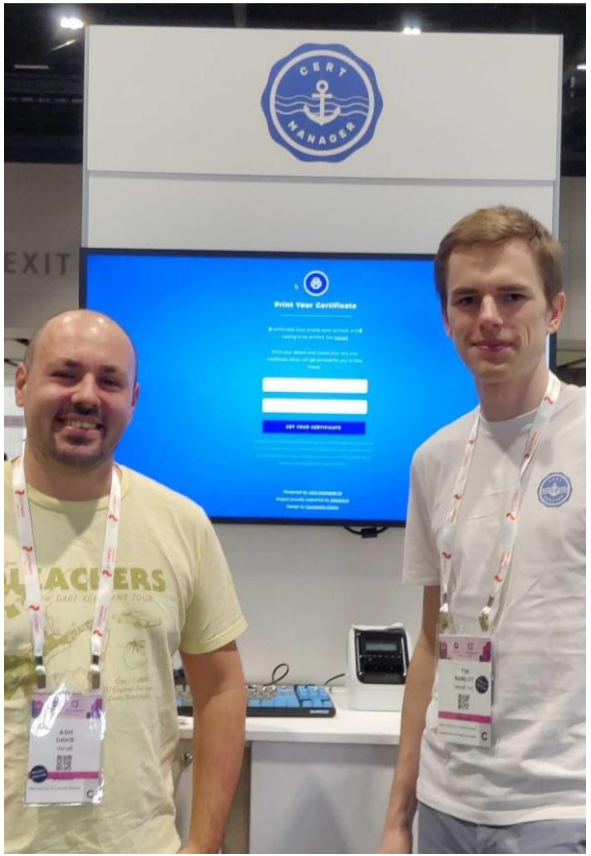
Recap: Going Secretless

- Auth is important!
  - How does cert-manager authenticate for you?
  - Avoid static secrets, if possible
- Reduce use of Secrets with csi-driver
  - More details on cert-manager.io
  - Works great with private PKI!

Outro: Visit our booth!

Kiosk 10A

Salt Palace Level 1
Project Pavilion (Hall 1)



Outro: Swag!


CERT
MANAGER
GRADUATED
CERT
MANAGER
GRADUATED


Thank you for coming to Workload Identity Day Zero!
We hope you're enjoying Salt Lake City.
This card is proof you were there!
The QR code on the back will allow you to download your certificate.
X.509v3 TLS Certificate
Algorithm: ECDSA P-256
Serial: 1082...1910
Subject: Ashley Davis
ashley.davis@venafi.com
Issuer: The cert-manager maintainers
Valid from: 2024-11-12T16:01:01Z
to: 2054-11-05T16:01:01Z
CERT
MANAGER

Outro: Thank you!

Questions?

Feedback: