KubeCon | CloudNativeCon

North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

cert-manager - Past, Present and Future

Ashley Davis & Jake Sanders

cert-manager - Past, Present and Future

KubeCon | CloudNativeCon

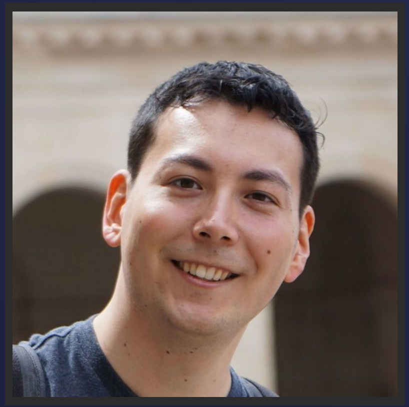
North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

October 24-28, 2021

Ashley Davis
Senior Software Engineer
Jetstack



Jake Sanders
Platform Engineer
G-Research

The Past: Project History

May 2016: kube-lego open-sourced by Jetstack

October 2017: v0.1.0 release of cert-manager

September 2020: cert-manager v1.0.0 released

November 2020: accepted as CNCF Sandbox project

The Present: Incubation

October 2022: cert-manager accepted as a CNCF incubating project!

CERT MANAGER

CLOUD NATIVE
COMPUTING FOUNDATION
INCUBATING PROJECT

The Present: Incubation

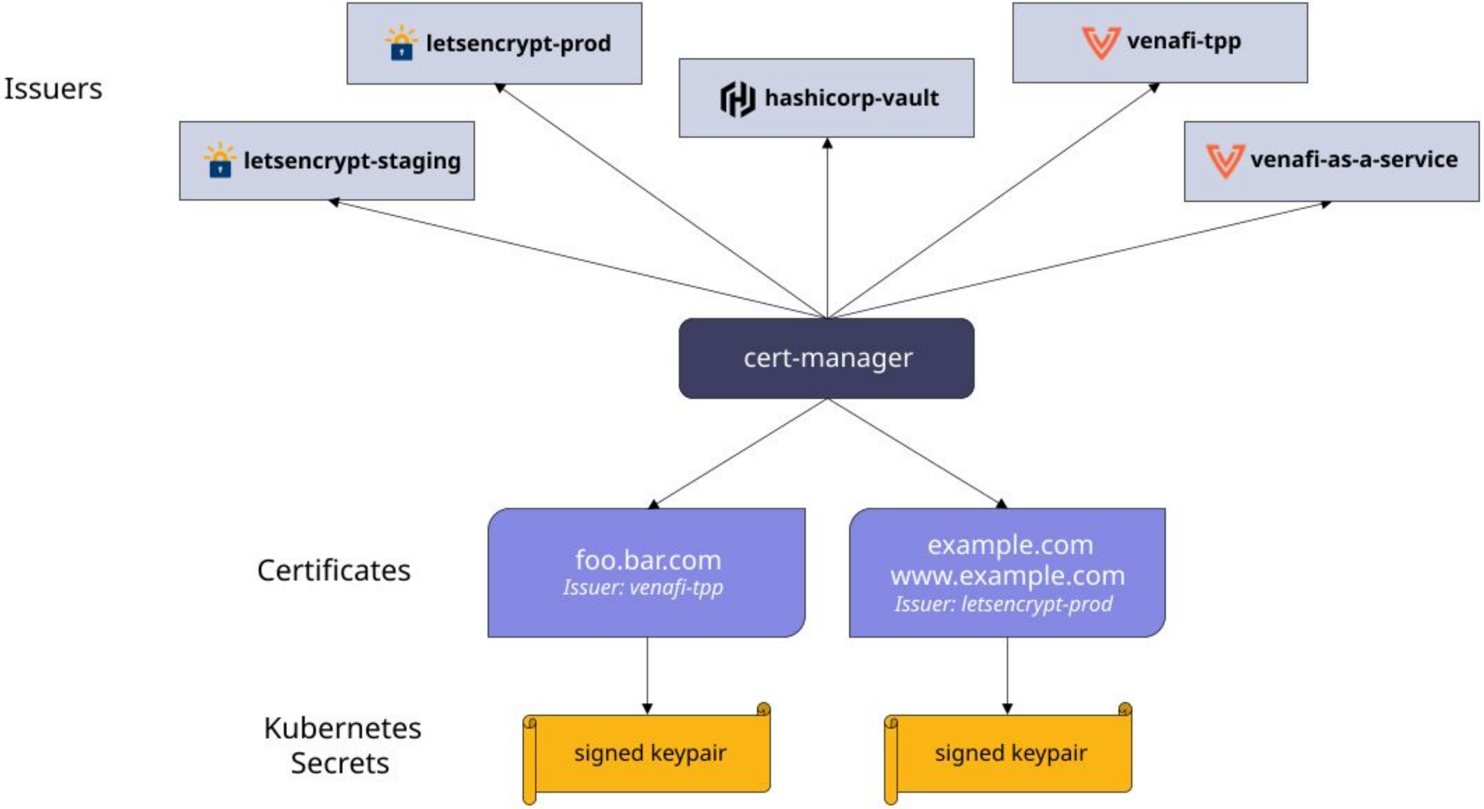
CERT MANAGER ❤️ CLOUD NATIVE COMPUTING FOUNDATION

INCUBATING PROJECT

The Present: What’s cert-manager?

- Cloud-native management of X.509 certificates
- Simple workflow
- Automatic lifecycle management
- Extensible issuers and policies
- 9.5k+ GitHub Stars!

The Present: High-level Overview



The Present: Certificate Issuance

🧑‍💻

- Automated ACME challenge solving for publicly trusted certificates
- Supports ACME (Let’s Encrypt, Smallstep step-ca), Hashicorp Vault, Venafi
- Automated renewal of short-lived X.509 certificates
- Extensible - easy to support new issuers and DNS providers

CERT MANAGER

The Present: Security

- cert-manager is critical security infrastructure!
- We’re early adopters of Project sigstore; all our main release artifacts are signed with cosign
- “Self-certified” SLSA 2 compliance, almost level 3

sigstore cosign

The Present: Policy

- cert-manager isn’t just a single app, it’s a whole project!
- approver-policy: who requested that certificate? Should it be allowed?
- Short-lived certificates for mTLS credentials
- Private Key rotation policies

The Present: Integrations

- Custom approval policy integration, e.g. OPA
- Integrates with other cloud native projects:
  - Istio (replacing citadel)
  - Linkerd
  - sig-network Gateway API (Traefik, Contour, Istio)
  - Prometheus (rich metrics for certificate state)
- CSI driver integration
  - SPIFFE (X.509)
- CAInjector - Easily secure your admission / conversion webhooks

The Future: Integrations

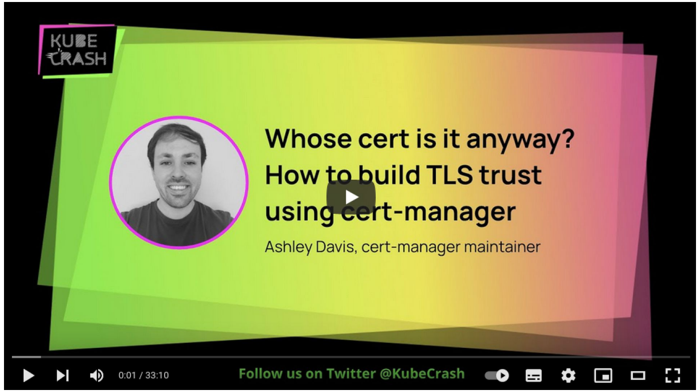
- An integration with your project?
- We’d love to talk to you!
- Drop by our booth in the pavilion!

The Future: Roadmap

- Increase collaboration with other CNCF projects
  - Service Meshes
  - SPIFFE/SPIRE
- Continue to improve developer experience
- Better support for X.509 features - extended attributes, CRLs/OCSP
- Explore other key management opportunities e.g. code signing
- Public roadmap available in the cert-manager repo

The Future: trust-manager

- Getting a certificate is only half the TLS problem!
- We need to know how clients can verify certificates
- trust-manager seeks to solve this for TLS
- NB: There's upstream work on this: trust anchor sets



Whose cert is it anyway? How to build TLS trust using cert-manager

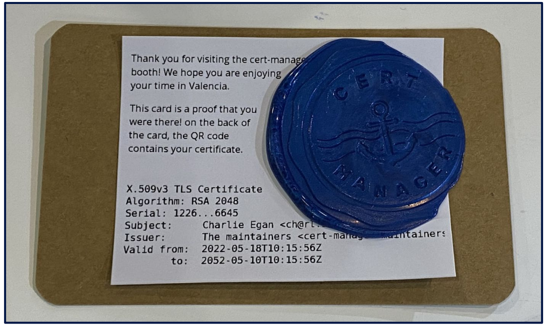
Ashley Davis, cert-manager maintainer

The Future: You?

- We get a lot of issues and PRs (that’s great!)
- There’s a tonne to do!
- We’d love more maintainers to get stuck in with us
- If you’re interested, please talk to us
- Open source maintainership experience not required!
- We can help

Visit Our Booth!

- Drop by the cert-manager booth if you haven’t already!
- Get your own souvenir certificate
- We’d love to have a TLS handshake (or elbow bump) with you!



Thank you for visiting the cert-manage
booth! We hope you are enjoying
your time in Valencia.

This card is a proof that you
were there! on the back of
the card, the QR code
contains your certificate.

```
X.509v3 TLS Certificate
Algorithm: RSA 2048
Serial: 1226...6645
Subject:     Charlie Egan <ch@rl
Issuer:      The maintainers <cert-mana   aintainers
Valid from:  2022-05-18T10:15:56Z
        to:  2052-05-10T10:15:56Z
```

Links / Get In Touch

- https://cert-manager.io - cert-manager website
- https://github.com/cert-manager - GitHub org
- Meetings - Details on when we have public meetings
- Slack - Chat with us on Kubernetes slack
- cert-manager-maintainers@googlegroups.com - email the maintainer team!

Thank you!