
KubeCon
CloudNativeCon
North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022
TiKV
TiKV
HELM

KubeCon CloudNativeCon North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022

Securing Edge Workloads with cert-manager and SPIFFE

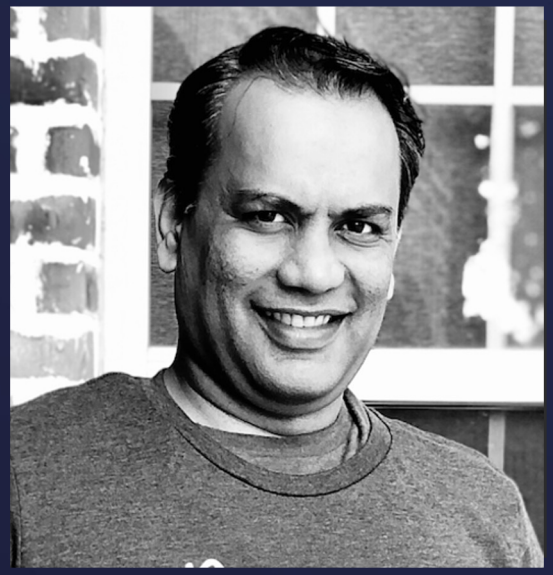
Riaz Mohamed & Sitaram Iyer

Secure edge workloads with cert-manager and SPIFFE

KubeCon | CloudNativeCon
North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022

KubeCon | CloudNativeCon
North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022

Riaz Mohamed
Global Security Architect
Venafi / Jetstack

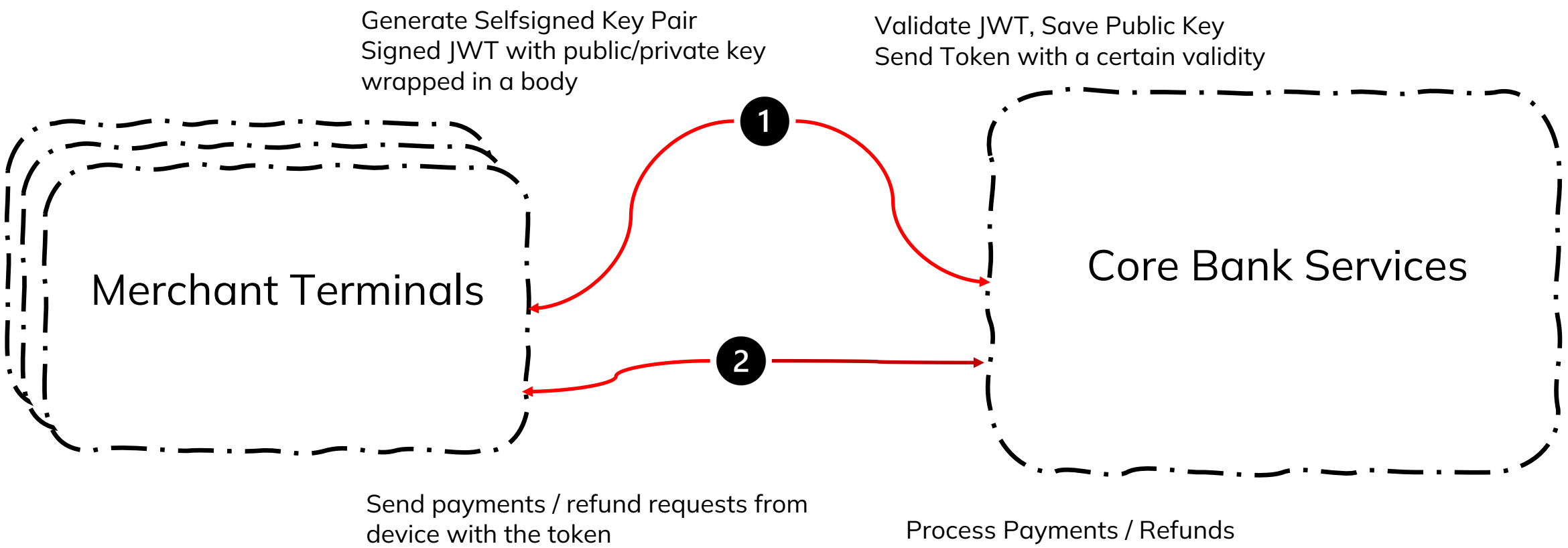


Sitaram IYER
Senior Director, Cloud Native Solutions
Venafi / Jetstack

Motivation

Provide a standard way of generating identities for workloads across clusters and create *trust*

Let’s talk about a real-world scenario



What if ?

.... every workload has a unique identity ?

.... this identity was used by the workload to prove who it says it is?

.... “trust” was distributed automatically when a terminal is activated ?

.... “trust” was revoked when a merchant is offboarded?

SPIFFE to the rescue !

Secure identity for every workload irrespective of where they are running

Authenticate mutually in an easy & reliable way

CNCF Graduated [Open Source]

spiffe

SPIFFE basics

Workload	Any software essentially
SPIFFE ID	A URI that uniquely identifies a workload *spiffe://trust-domain/workload-identifier* For e.g. spiffe://dev.jetstack.com/ns/prod/sa/payments
Trust Domain	A well-defined security boundary
SPIFFE SVID	Cryptographically verifiable identity document
SPIFFE Workload API	For X.509-SVID. Private Key tied to SPIFFE ID for signing
Trust Bundle	Specific to X.509-SVID's, a collection of one or more CA's

cert-manager

Automatically provision & manage TLS certificates

Several add-ons to support additional use cases

CNCF Incubating [Open Source]

cert-manager + CSI Driver

KubeCon CloudNativeCon North America 2022

csi-driver-spiffe

csi-driver-spiffe is a Container Storage Interface (CSI) driver plugin for Kubernetes to work along cert-manager. This CSI driver transparently delivers SPIFFE SVIDs in the form of X.509 certificate key pairs to mounting Kubernetes Pods.

https://spiffe.io/docs/latest/spiffe-about/overview/#which-tools-implement-spiffe

https://cert-manager.io/docs/projects/csi-driver-spiffe/

cert-manager + CSI Driver + trust

Distributing Trust Bundles in Kubernetes

trust is an operator for distributing trust bundles across a Kubernetes cluster. trust is designed to complement cert-manager by enabling services to trust X.509 certificates signed by Issuers, as well as external CAs which may not be known to cert-manager at all.

https://cert-manager.io/docs/projects/trust/

cert-manager + CSI Driver + trust + policy approver

KubeCon CloudNativeCon North America 2022

approver-policy

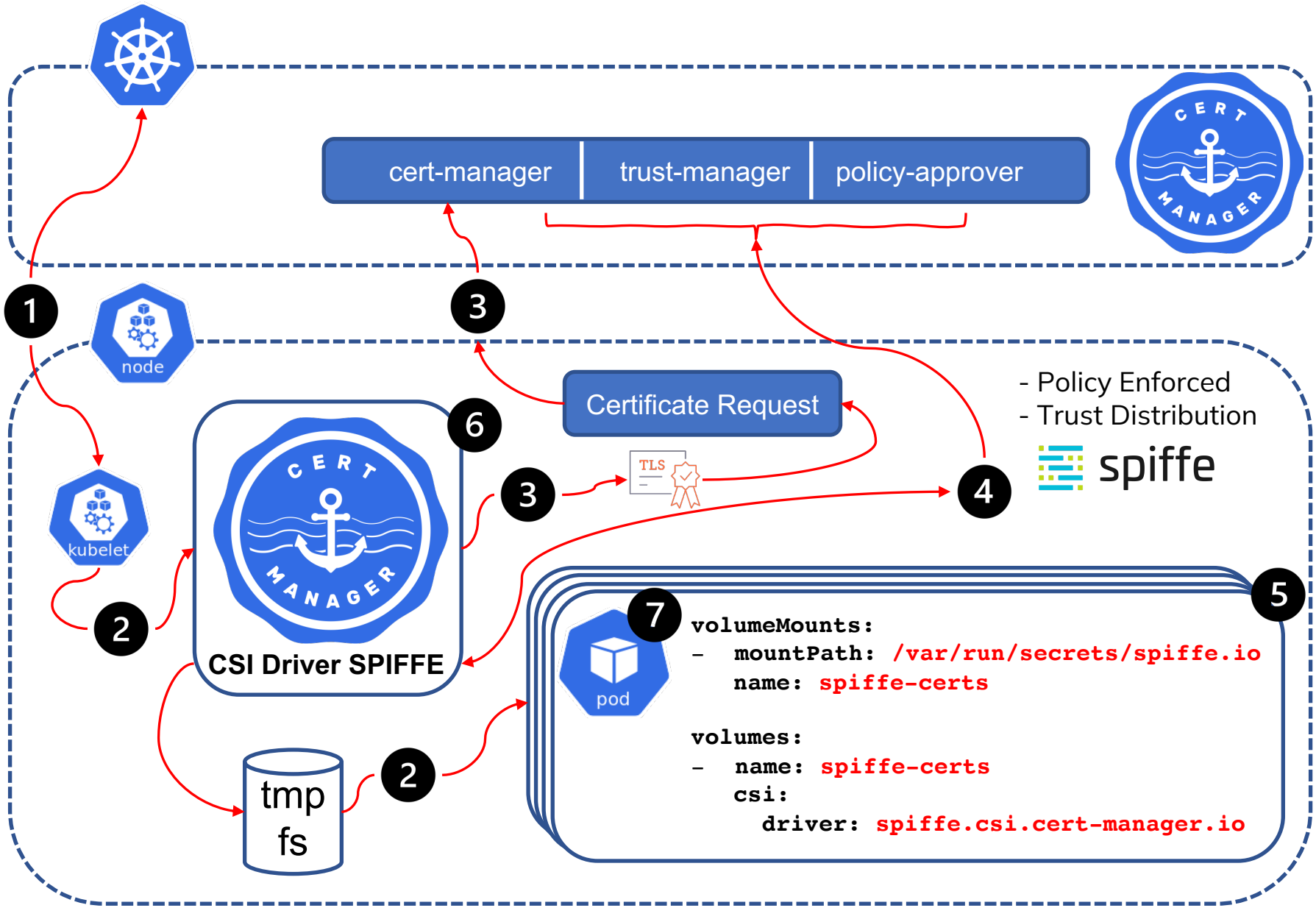
approver-policy is a cert-manager approver that will approve or deny CertificateRequests based on CRD defined policies.

A distinct cert-manager approver Deployment is responsible for managing the approval and denial condition of created CertificateRequests that target the configured SPIFFE Trust Domain signer. The approver ensures that requests have:

1. the correct key type (ECDSA P-521);
2. acceptable key usages (Key Encipherment, Digital Signature, Client Auth, Server Auth);
3. the requested duration matches the enforced duration (default 1 hour);
4. no SANs or other identifiable attributes except a single URI SANs;
5. the single URI SAN is the SPIFFE identity of the ServiceAccount who created the CertificateRequest;
6. the SPIFFE ID Trust Domain is the same as configured.

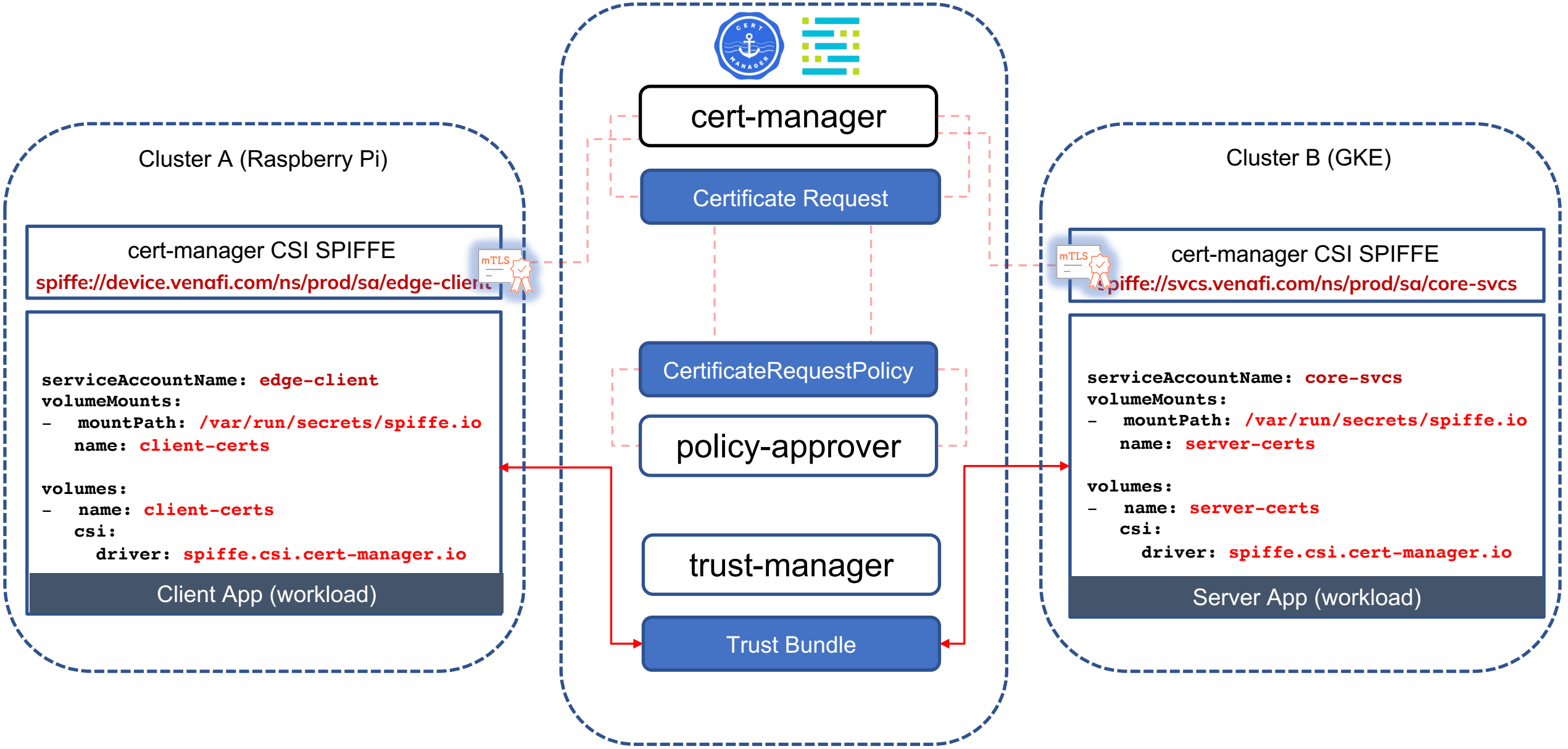
https://cert-manager.io/docs/projects/approver-policy/

The Solution !

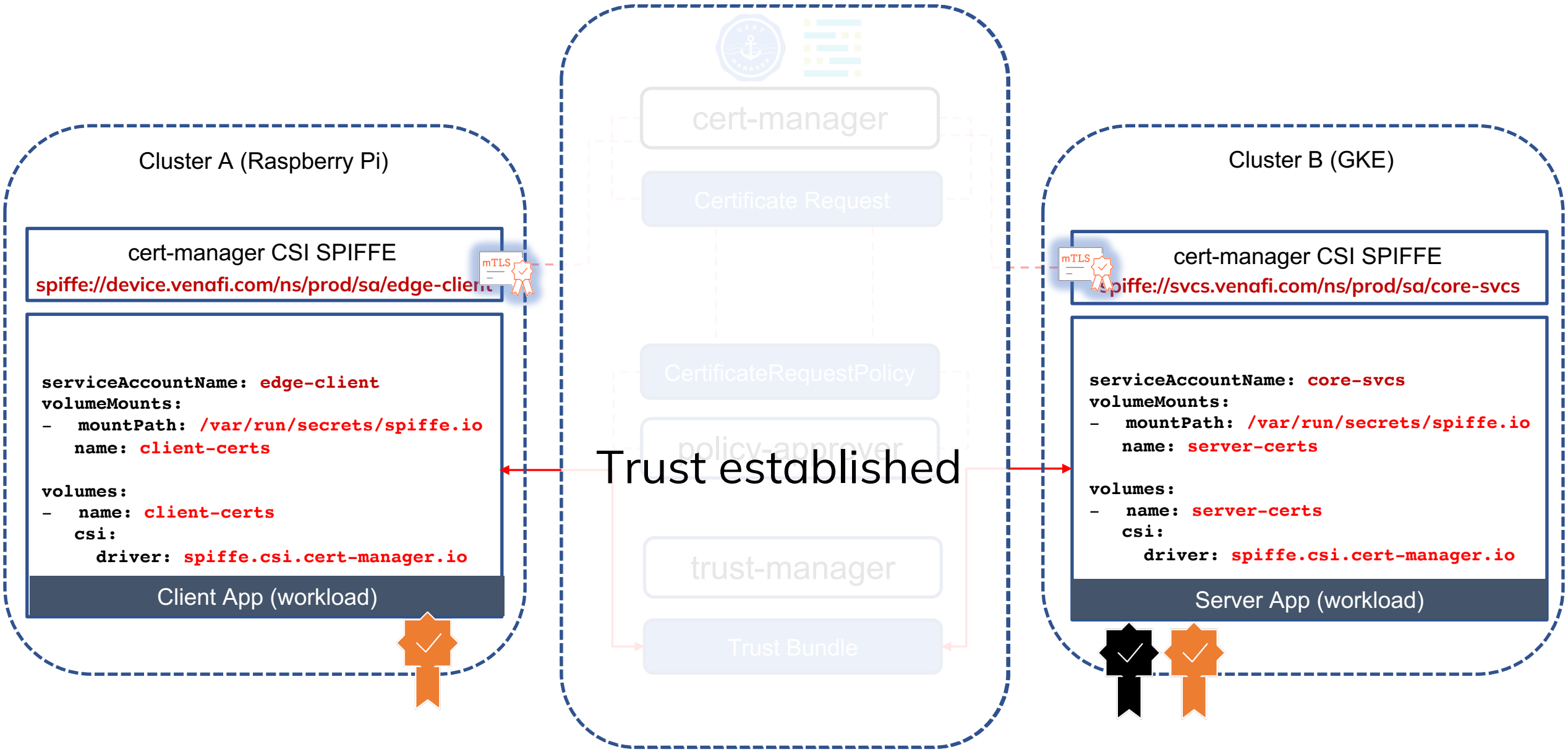


1. Pod scheduled to a Node
2. NodePublishVolume, Make & Mount Volume
3. Generate Private Key & CSR
4. Certificate Reconciliation, Policy Approved , Signed certificate obtained along with trust bundles
5. Signed certificate and private key along with CA's defined in trust-manager Bundle written to node and mounted to the pod's file system
6. CSI Driver SPIFFE tracks X509.SVID's and automatically renews them
7. NodeUnPublishVolume on pod termination,

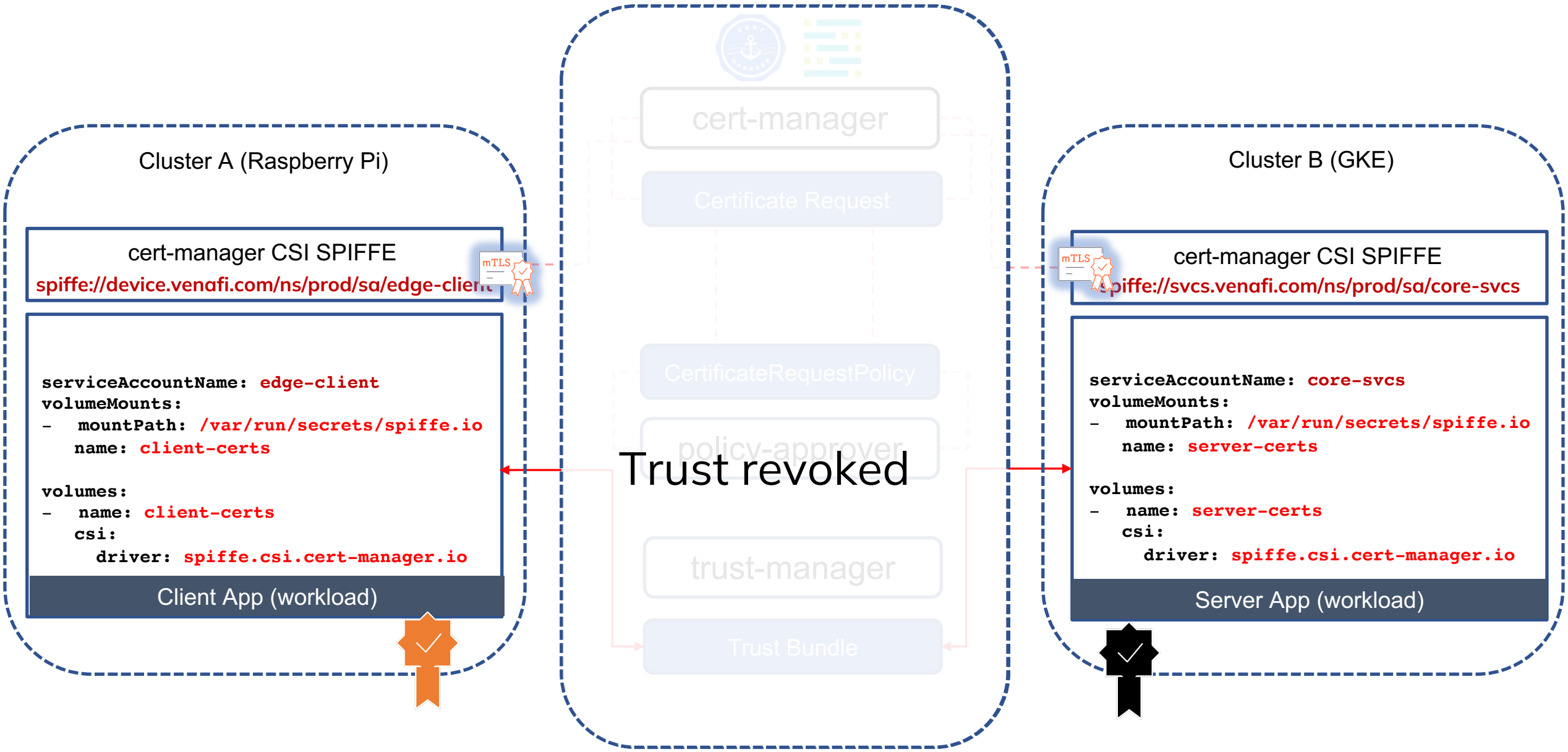
Demo Architecture



Demo Architecture



Demo Architecture



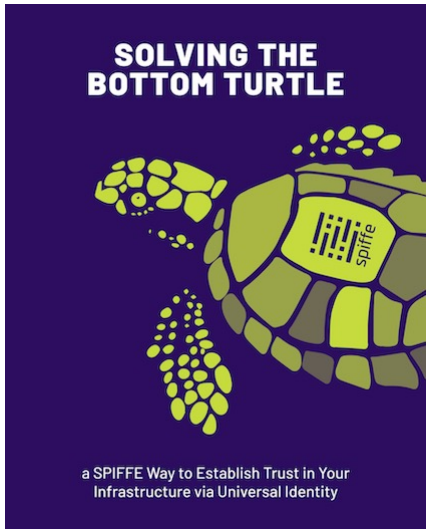
More details / links / contacts

KubeCon CloudNativeCon North America 2022

Modern workload identity with SPIFFE

https://www.jetstack.io/blog/workload-identity-with-spiffe-trust-domains

Software Engineer
Jetstack, a Venafi Company



https://spiffe.io/book/

cert-manager CSI driver for SPIFFE

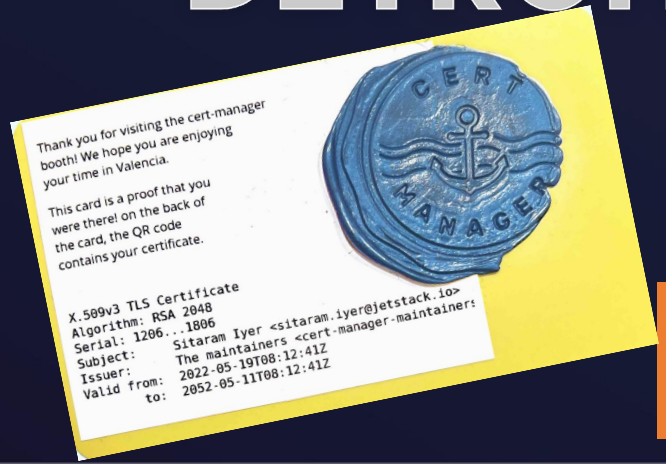
https://github.com/cert-manager/csi-driver-spiffe

Staff Software Engineer
Jetstack, a Venafi Company

Secure edge workloads with cert-manager and SPIFFE

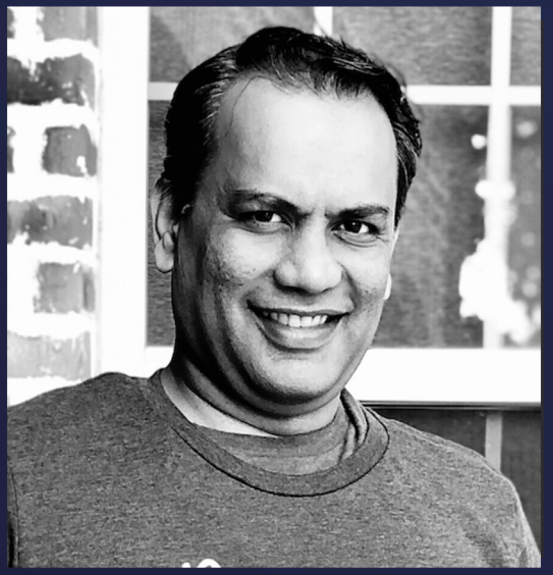
KubeCon | CloudNativeCon
North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022

KubeCon | CloudNativeCon
North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022



See you at booth #S115 and the cert-manager kiosk #22

Riaz Mohamed
Global Security Architect
Venafi /Jetstack



Sitaram IYER
Senior Director, Cloud Native Solutions
Venafi /Jetstack

Where do we go from here?

- Model / Rules driven revocation
- Trust distribution (automation) across trust boundaries
- A control plane to manage trust across trust boundaries

KubeCon | CloudNativeCon
North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Please scan the QR Code above to
leave feedback on this session