Edgeless Systems

# Attested TLS in Contrast

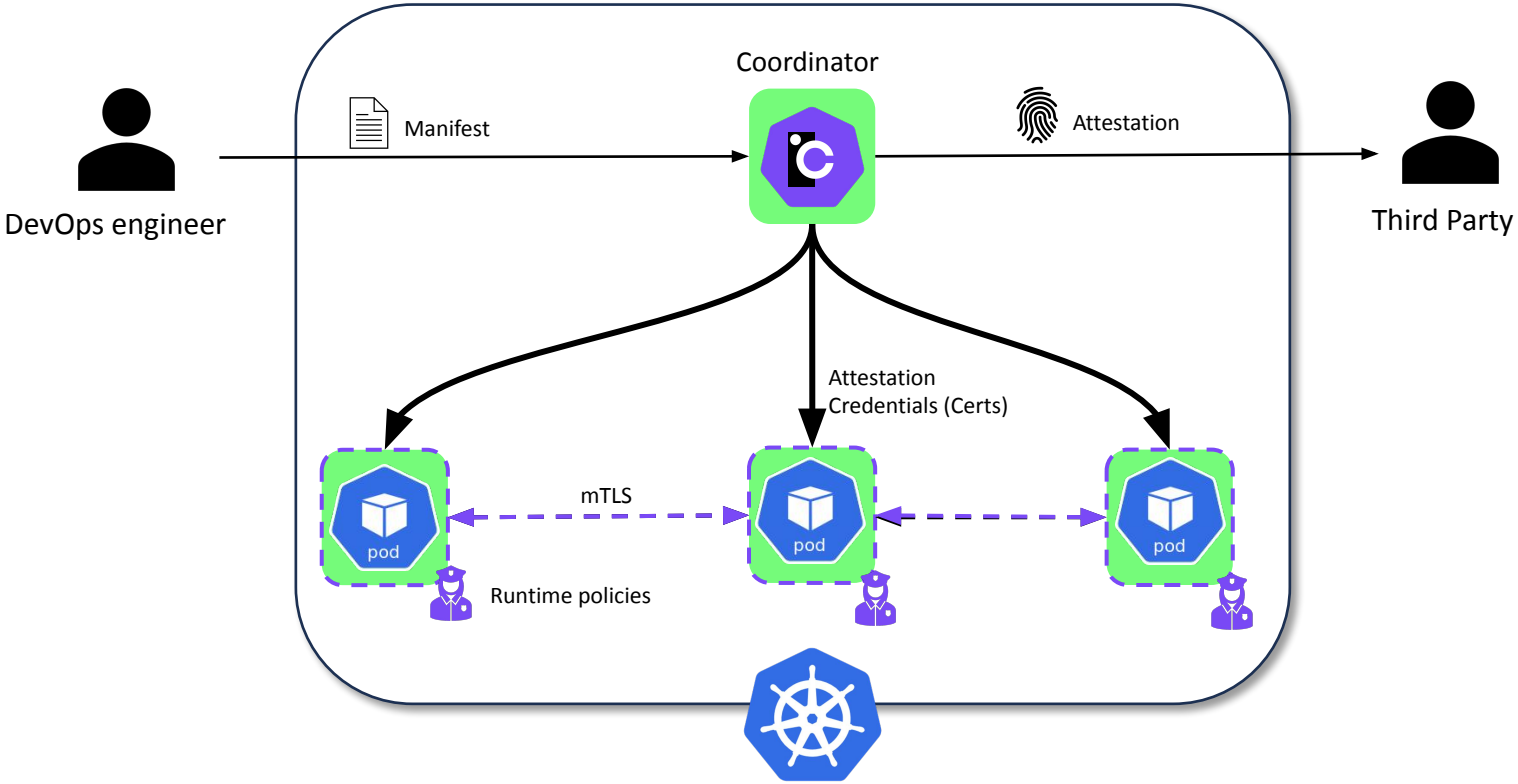
March 11, 2025 Markus Rudy (@burgerdev) CCC-Attestation SIG Meeting

Edgeless Systems

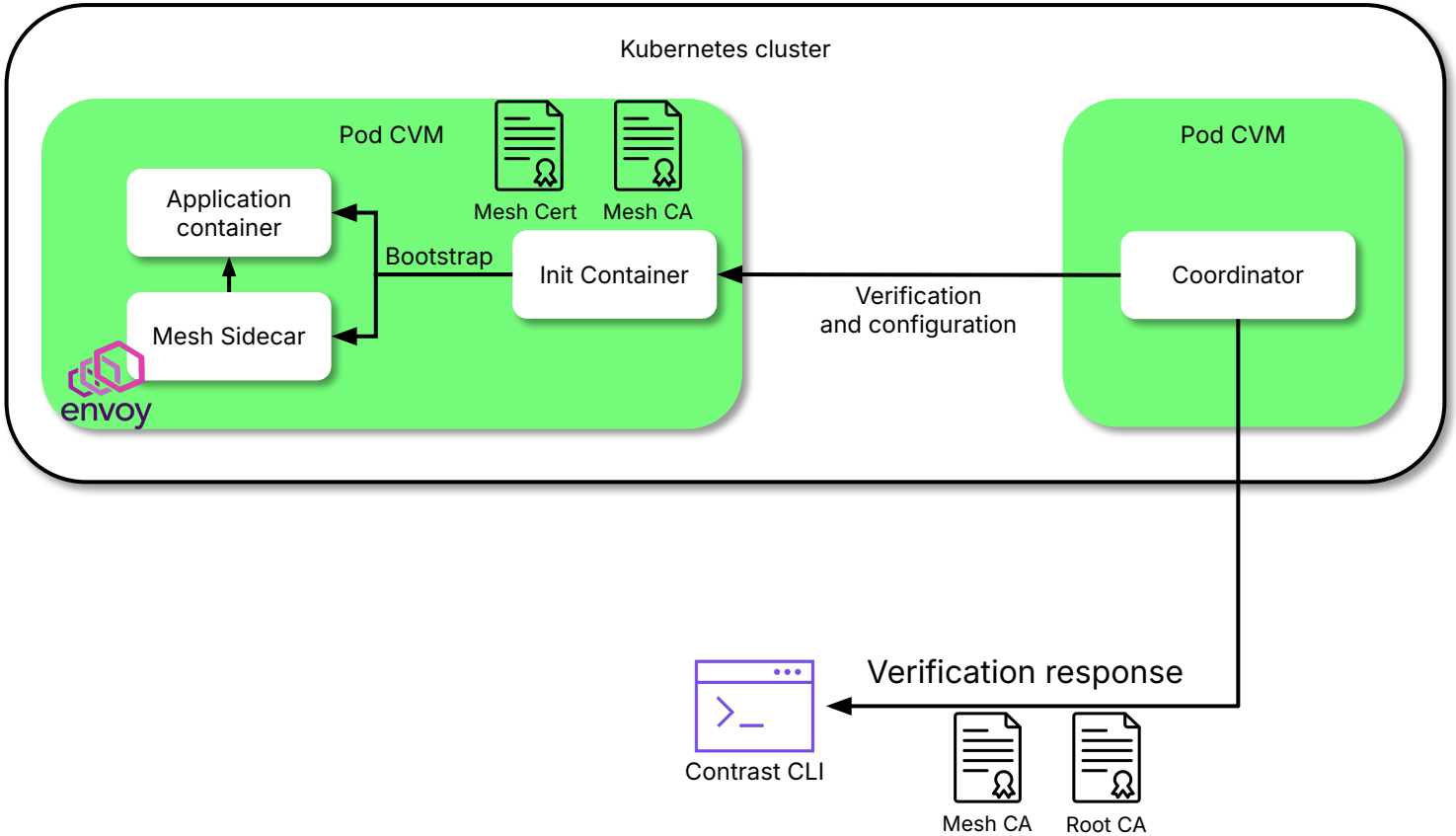
# 01 Contrast

A distribution of Confidential Containers

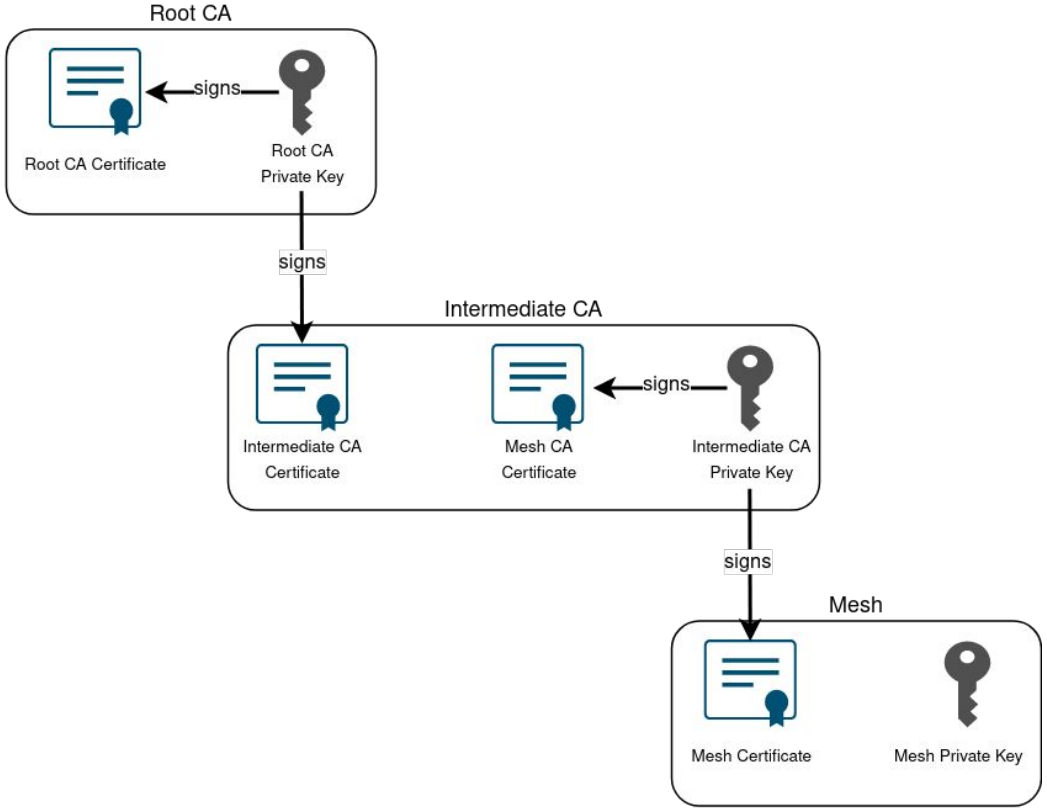
# What is Contrast?



# Certificates



# Certificate Chain



# Roles

| **(Human) Operator** | **Coordinator** | **Initializer** |
|---|---|---|
| In a secure environment | In a TEE | In a user workload TEE |
| ● Verifier (for Coordinator)<br>● Verifier Owner<br>● Consumes CA certificates | ● Verifier (for Initializer)<br>● Attester (towards Operator)<br>● Certificate authority<br>● Key Management Service | ● Attester (towards Coordinator)<br>● Certificate requester<br>● KMS client |

Edgeless Systems

# 02 Attested TLS

# The problem

We need to establish an encrypted channel to a server*.

- The server runs in a TEE and can produce evidence.
- The client has an appraisal policy for this evidence.
- The channel must be tied to appraised evidence.
- All server configuration is assumed to be public.

*: the situation for an attesting client is mostly the same

# The problem - cont’d

Additional constraints:

- Verify evidence before using the channel.
- Use standard protocols and algorithms.

# The problem - cont’d

Not a problem (for us):

- Interoperability/Standardization
- Middle boxes*

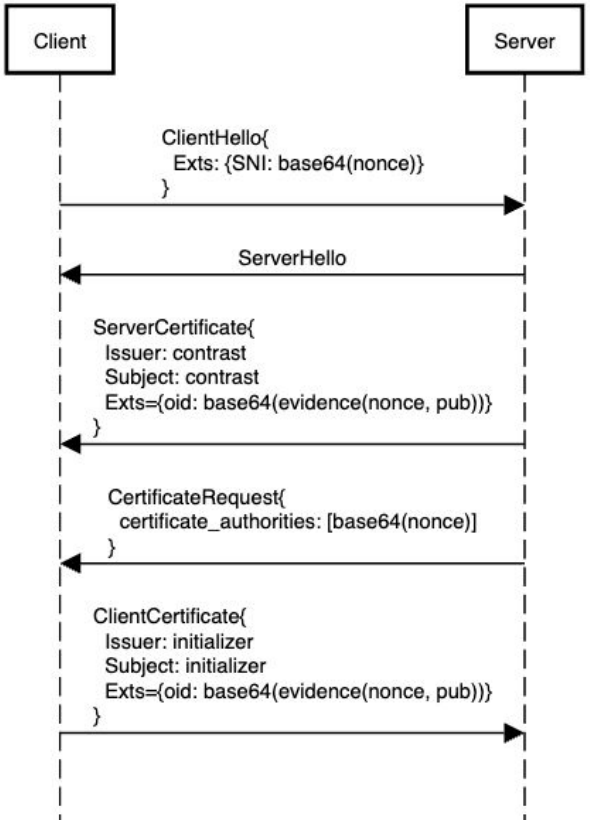
# High-level design

- Use TLS with self-signed, ephemeral keys.
- Find extension points to transmit attestation data.
- Include TLS channel state in evidence.
- Use hooks from the TLS library to produce evidence.

# TLS extension points

- X.509 certificates support arbitrary extensions!
- But:
  - Server cert is sent immediately after ClientHello.
  - Evidence creation needs a nonce from the client.
  - ClientHello has extensions, but they are not accessible.
- Idea: reuse an existing extension!
  - Server Name Indication (SNI)

# Attested TLS handshake



# Verification goals

| **Verification goal** | **Achieved by** |
| --- | --- |
| Peer possesses private key for channel. | Successful TLS handshake |
| Evidence was created for this channel. | Verifier-supplied nonce in evidence |
| Evidence was created by this peer. | Peer’s public key in evidence |
| Peer created the key inside the TEE. | Appraisal of remaining evidence (workload integrity) |