Deploying Containerized Workloads to GKE Clusters

Janani Ravi
CO-FOUNDER, LOONYCORN

www.loonycorn.com

Overview

Applications deployed to containers

Service and ingress objects

Volume abstractions for shared state

Deploy attested containers using binary authorization

Demo

Define a custom Docker container

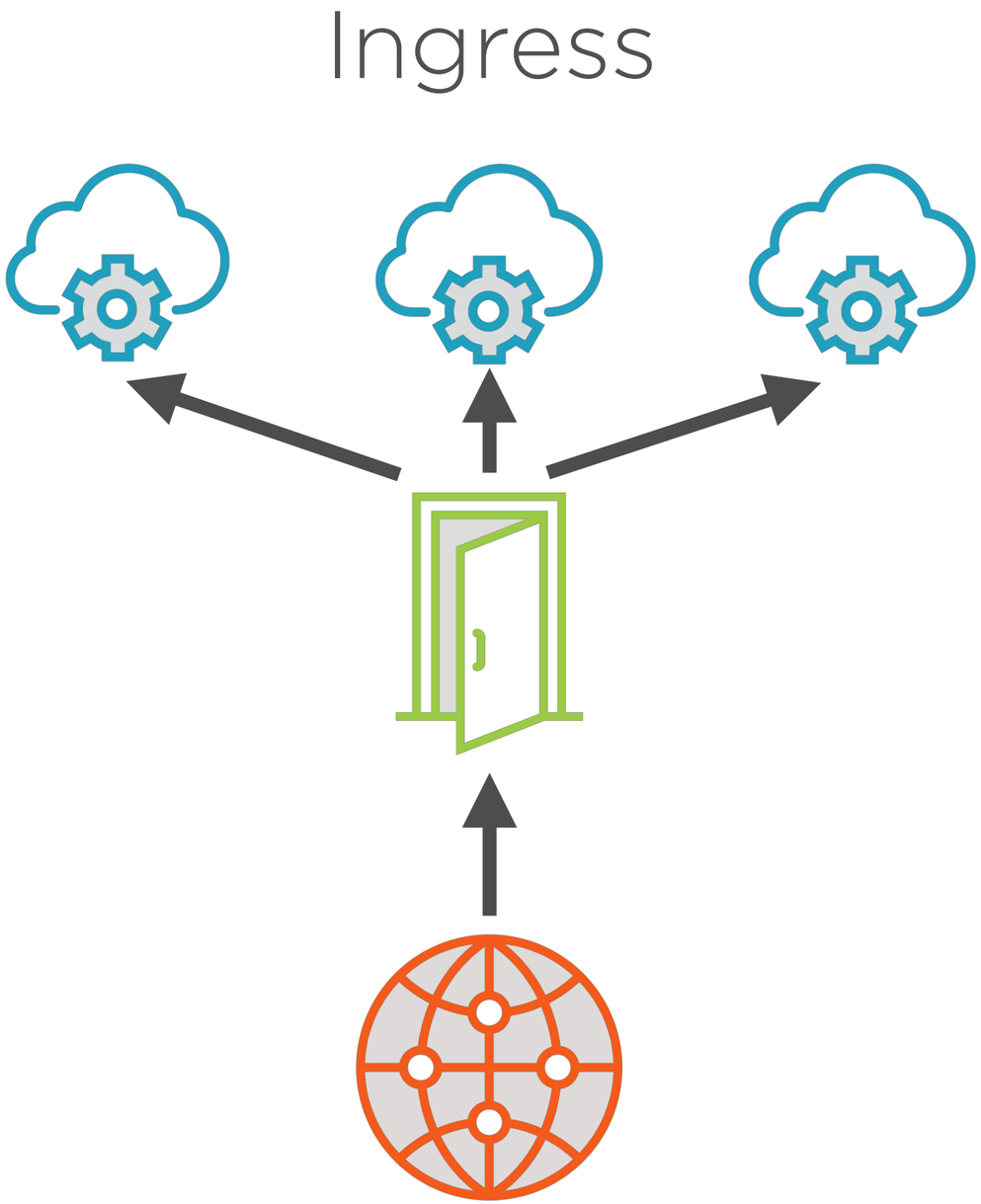
Deploy it on a Kubernetes cluster

Expose it as a service

Demo

Configure ingress objects on GKE

With multiple services it makes sense to have rules defined using an ingress object



Demo

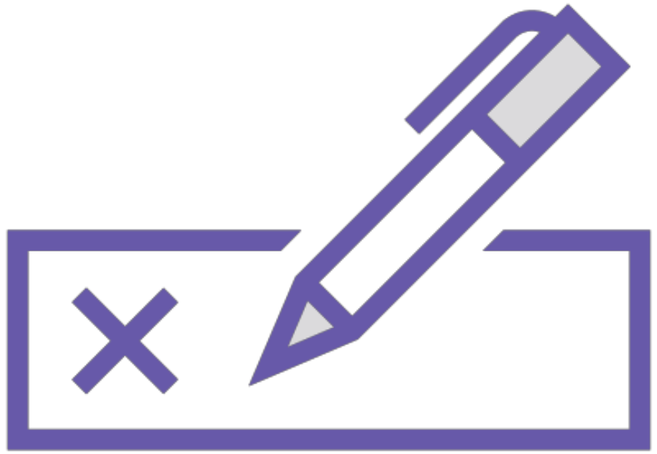
Deploy multiple services to run a WordPress site

Configure persistent storage using PersistentVolumeClaims

Binary Authorization

Binary Authorization

A deploy-time security control that ensures only trusted container images are deployed on Google Kubernetes Engine



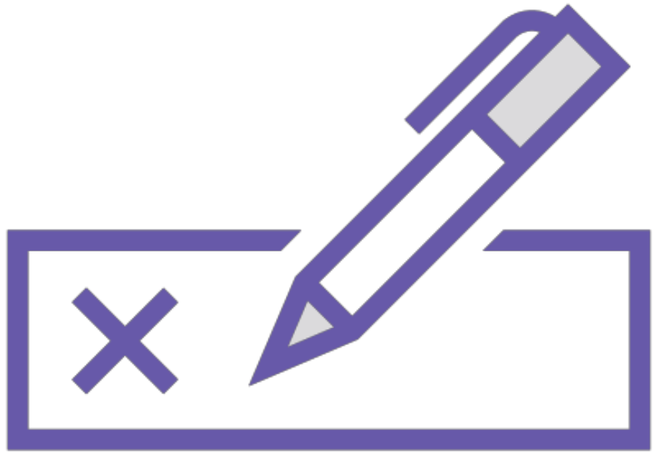
Binary Authorization

Require images to be signed by trusted authorities

Signing must occur during development

Signature validation during deployment

Binary Authorization



Reduces risk of malicious or unintended code in production

Integrates with Google Container Registry vulnerability scanning

Google Container Registry

Secure, private Docker registry

Automatic builds, deployments

- Commit code from GitHub, Cloud Source Repositories, BitBucket
- Deploy to GKE, App Engine, Cloud Functions, Firebase

Binary Authorization Process

Configure Policy

Set of rules that govern image deployment

Default and cluster-specific rules, exempt images

Sign Container Image

Create Attestation

Digitally signed record with full path to image

Set up Attestor

Entity that signs off that due process followed

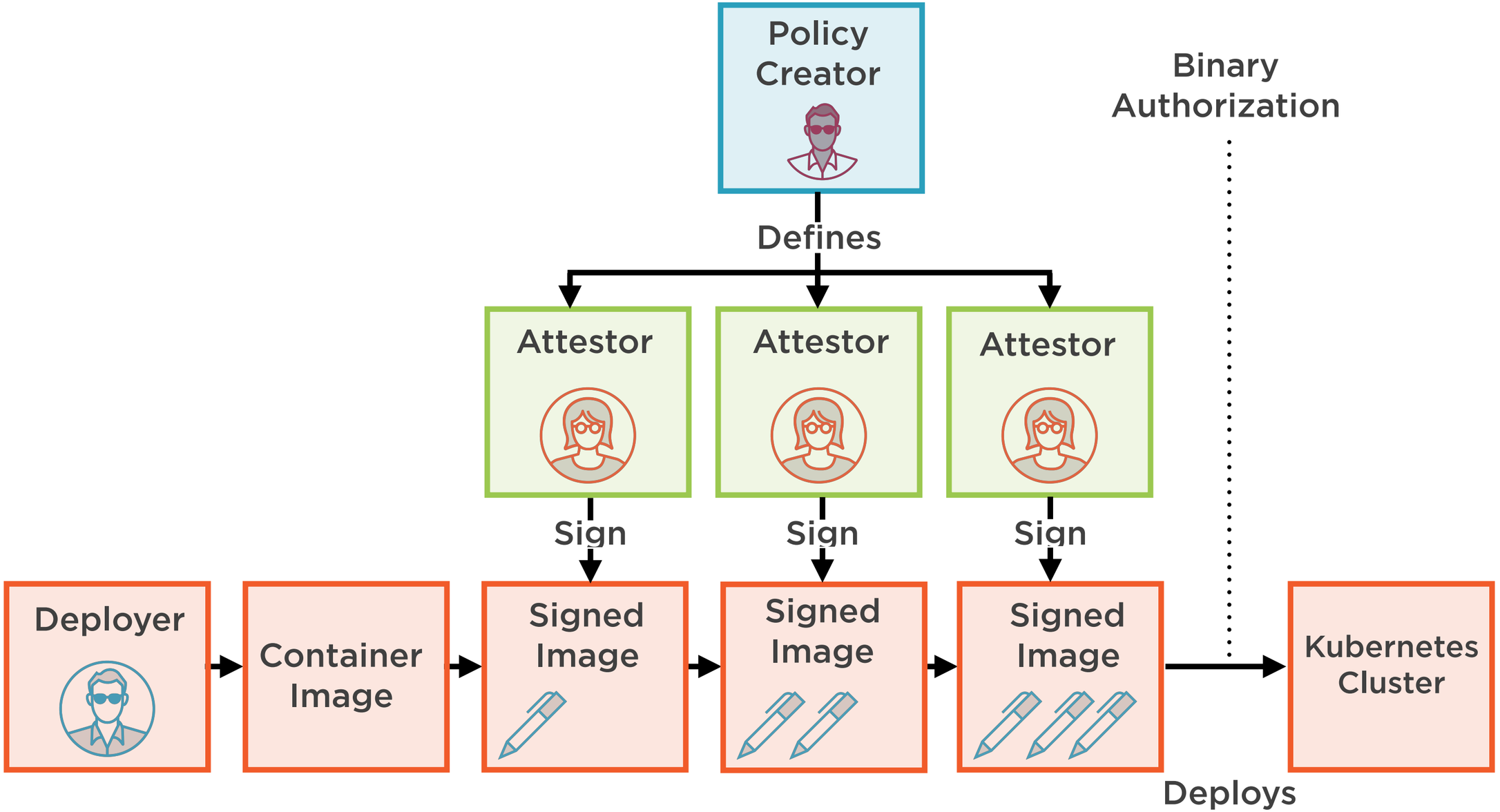
Human, or build-and-test system, with public key

Deploy Container Image

As usual

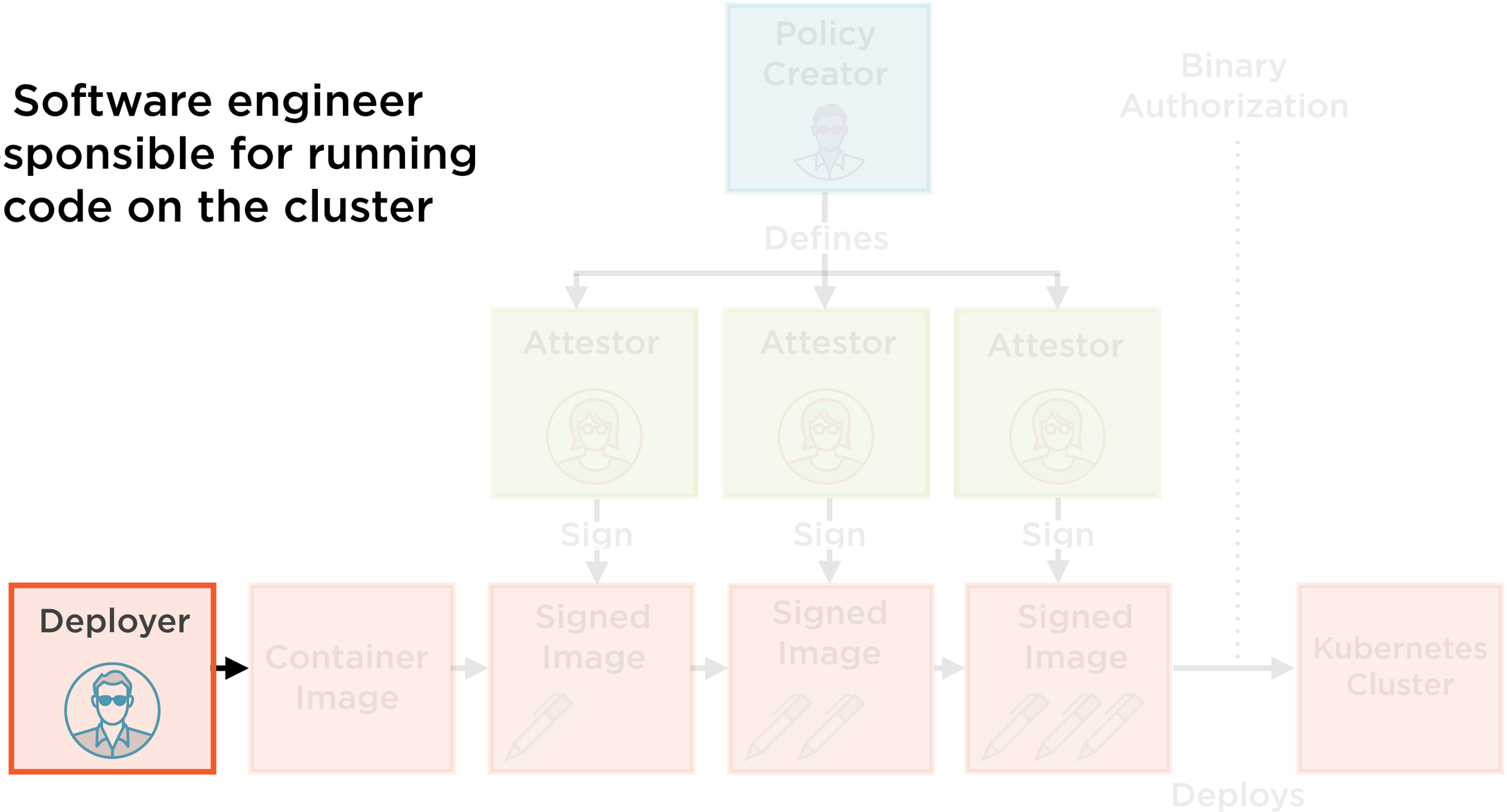
No different than regular process

Binary Authorization Process



Binary Authorization Process

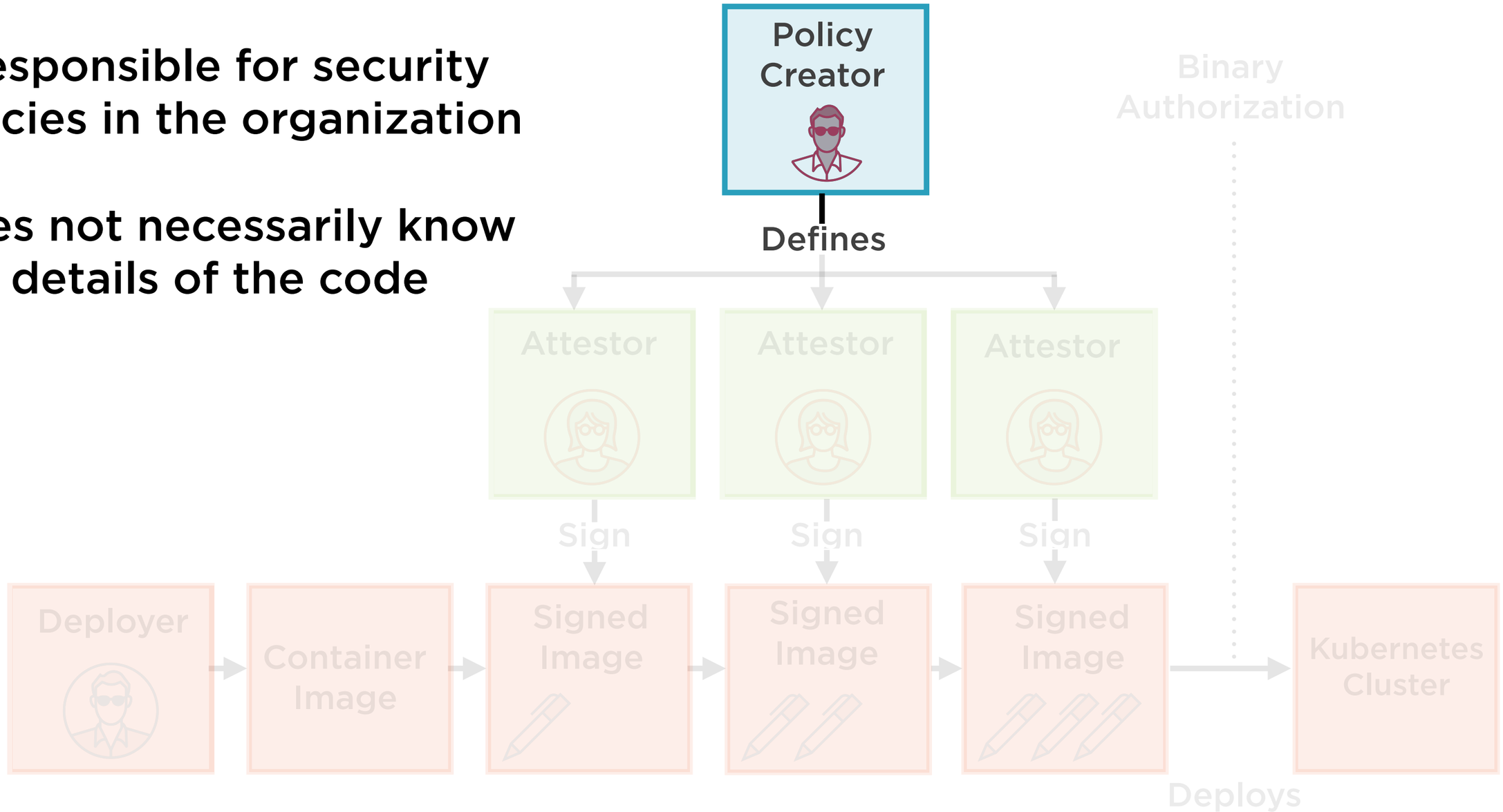
Software engineer responsible for running code on the cluster



Binary Authorization Process

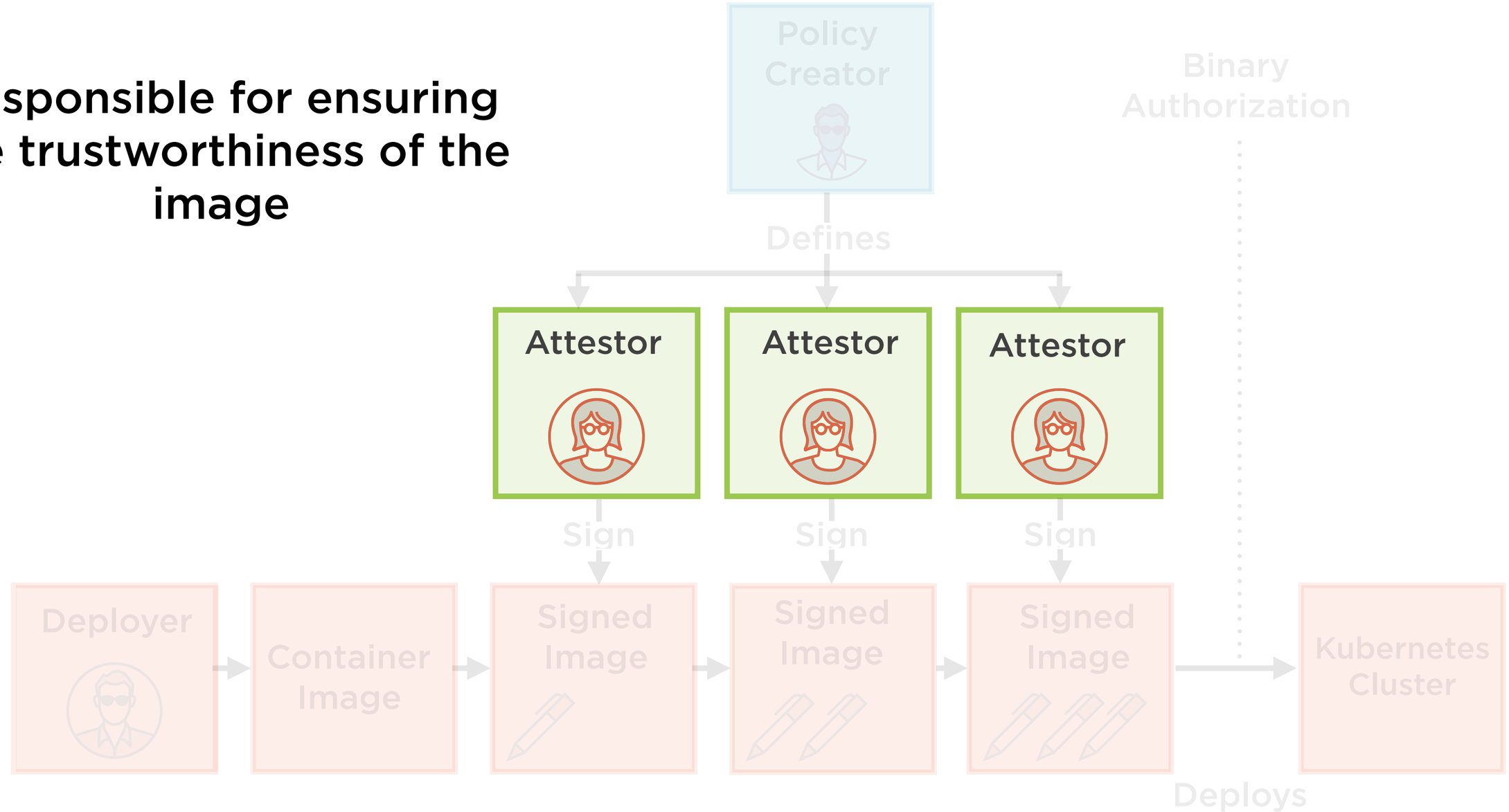
Responsible for security policies in the organization

Does not necessarily know details of the code



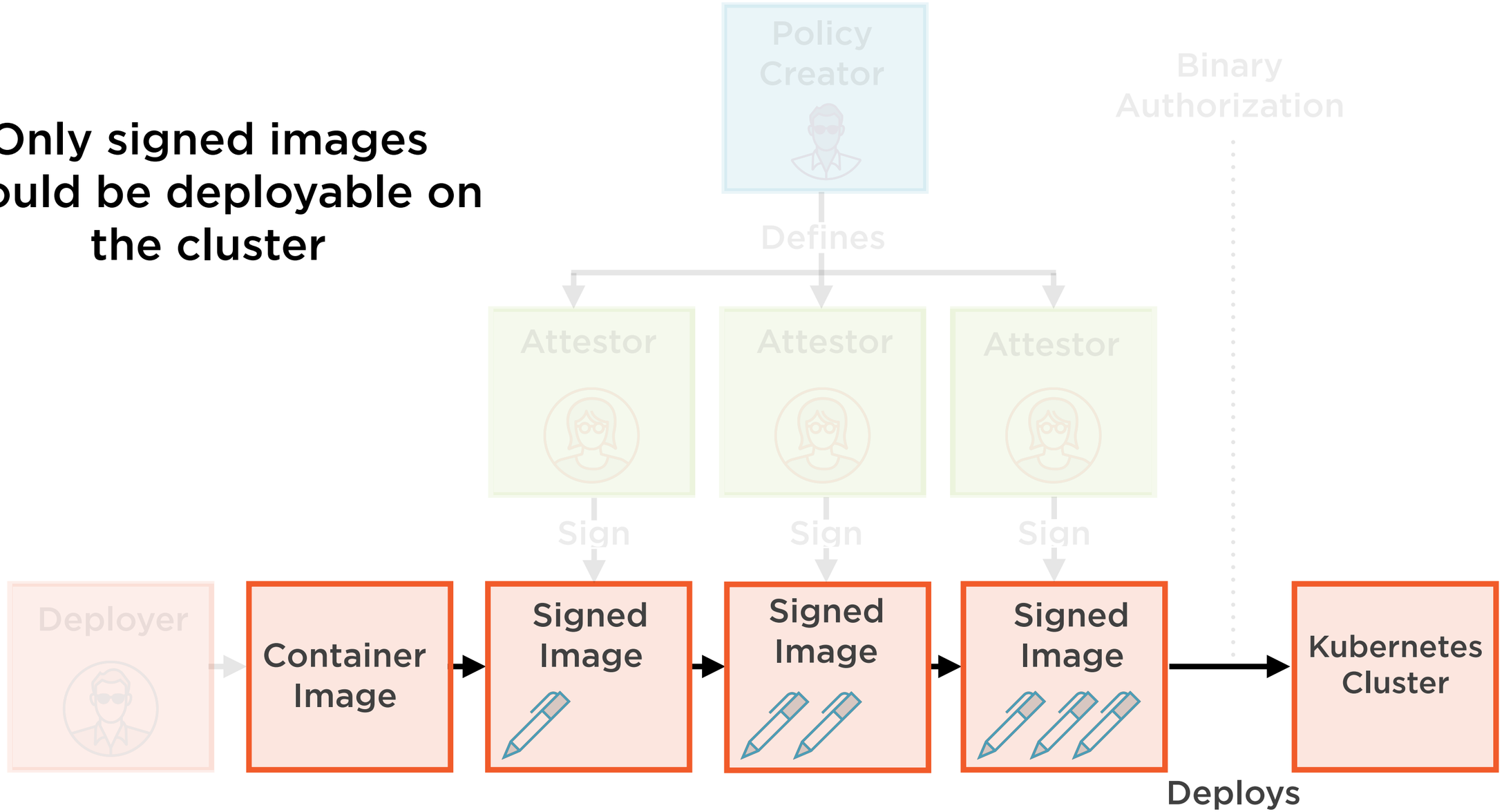
Binary Authorization Process

Responsible for ensuring the trustworthiness of the image



Binary Authorization Process

Only signed images should be deployable on the cluster



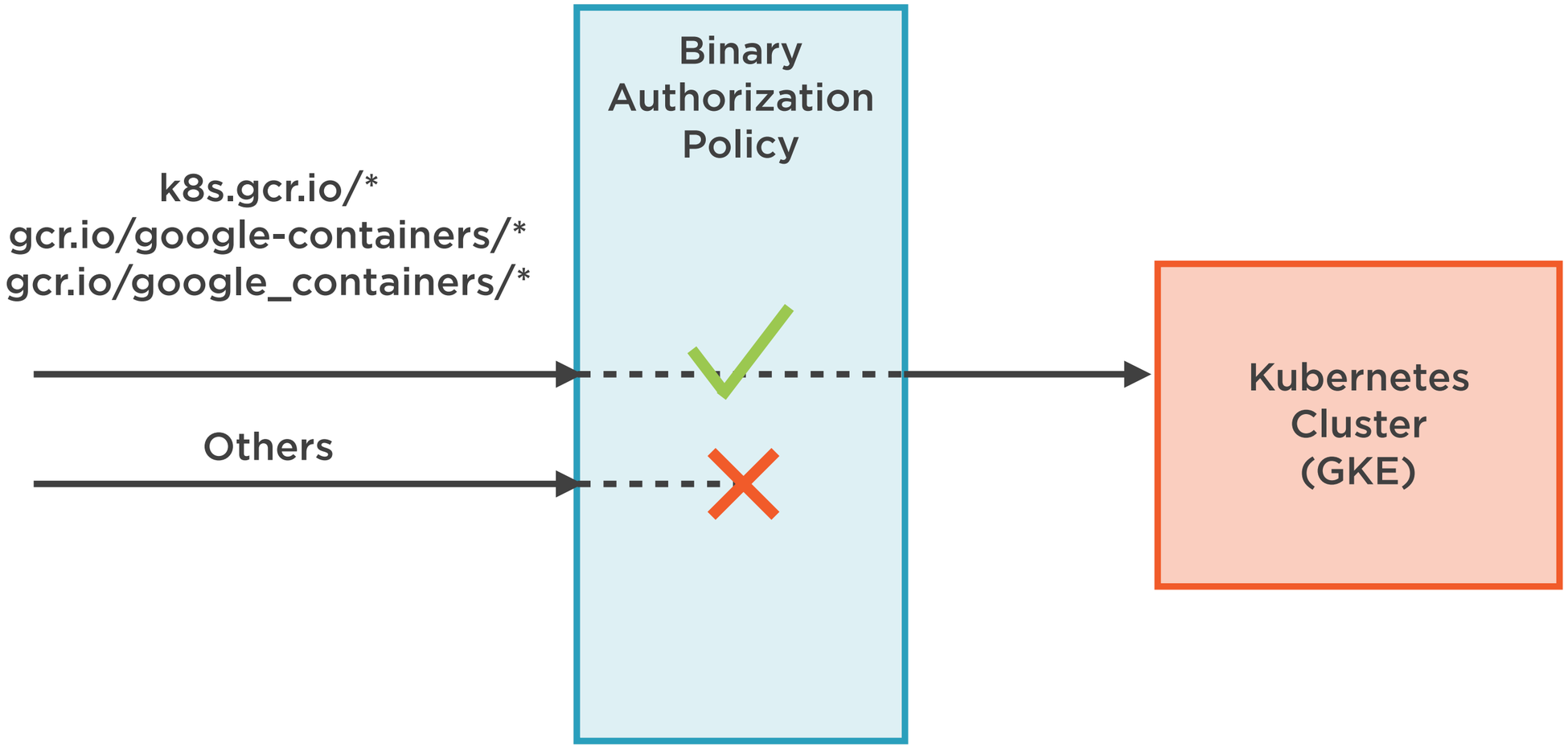
Binary Authorization Process

Configure Policy

Set of rules that govern image deployment

Default and cluster-specific rules, exempt images

Configure Policy



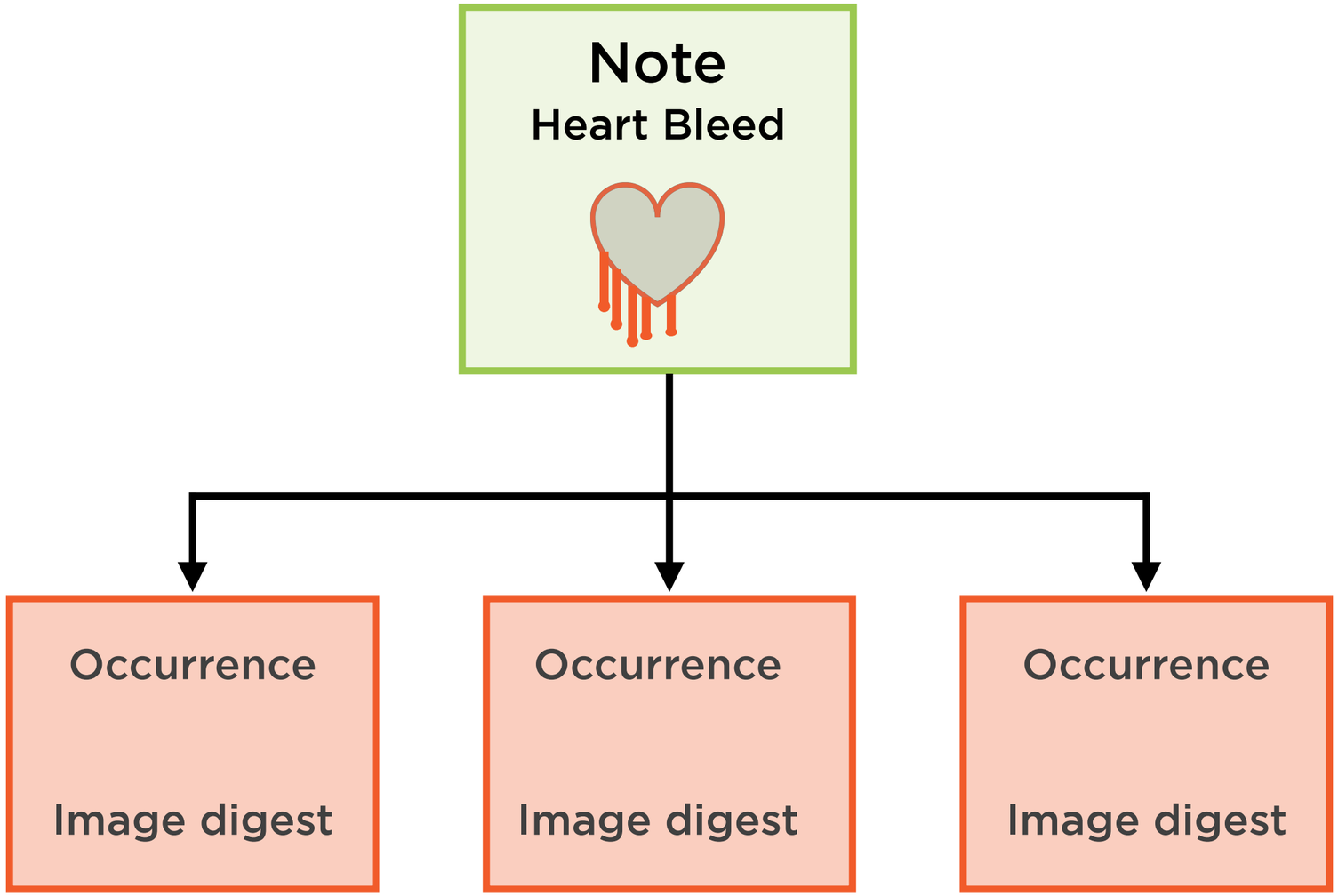
Container Analysis API

Allows association of metadata with container images

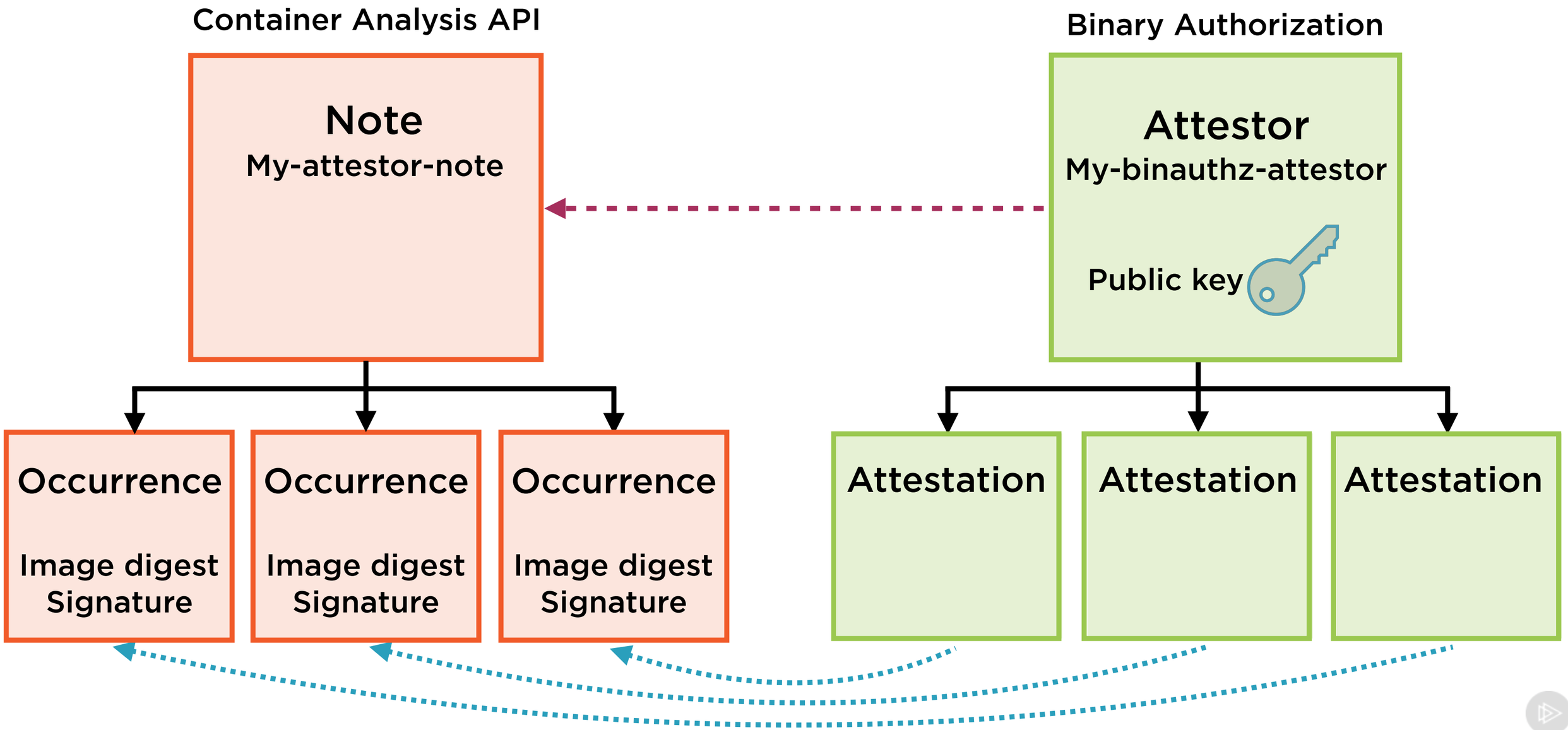
Note: A general piece of metadata

Occurrence: An instance of a note associated with a container

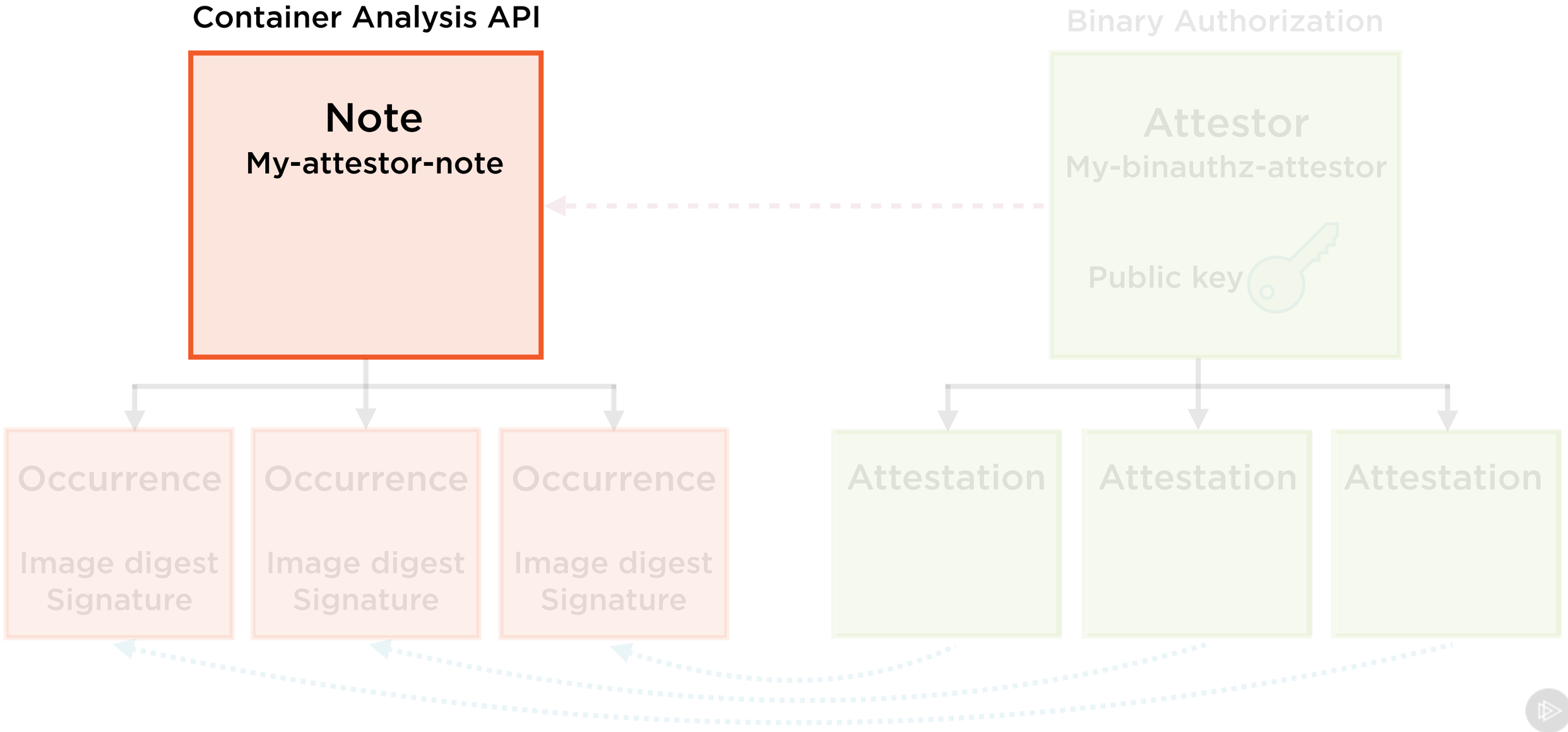
Container Analysis API



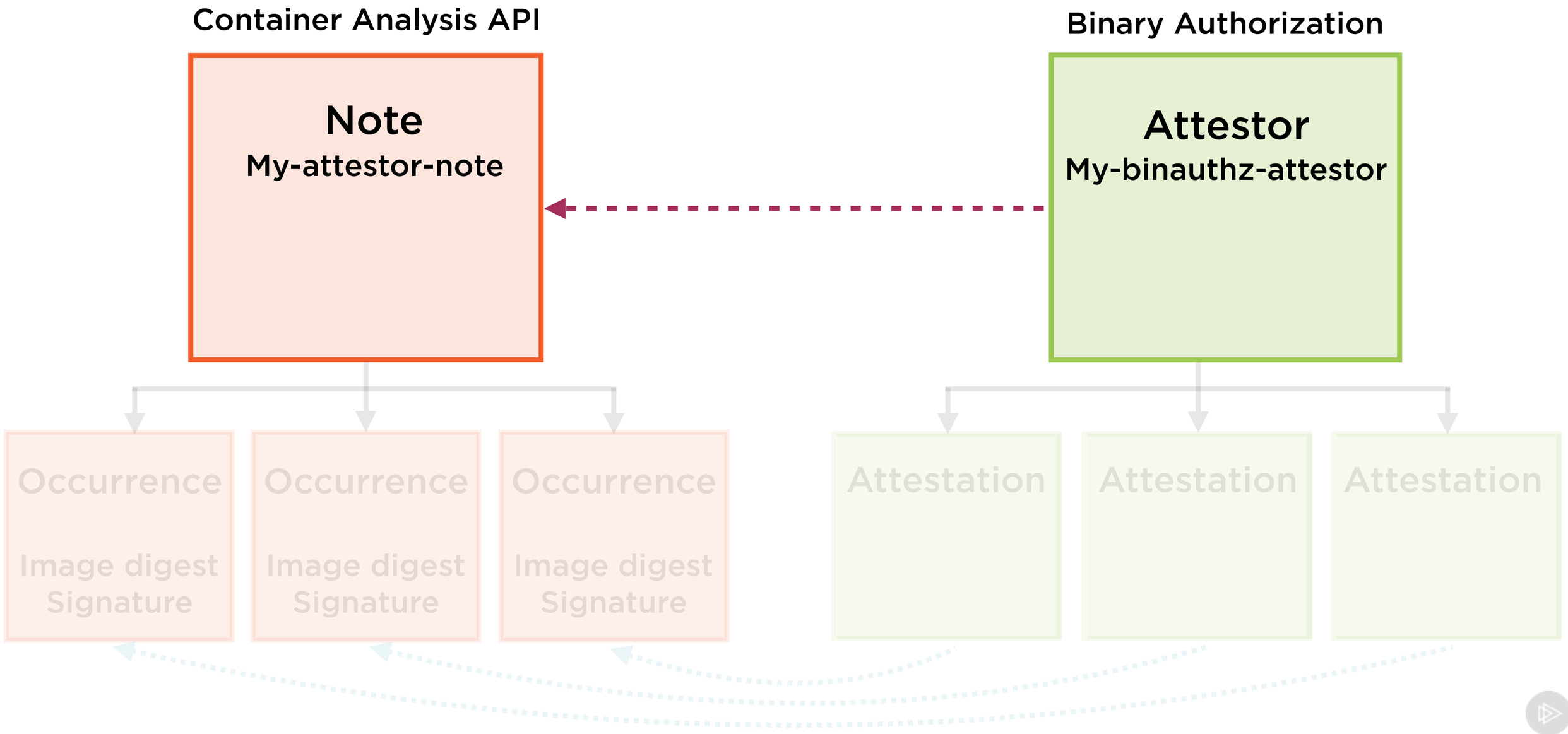
Container Analysis API



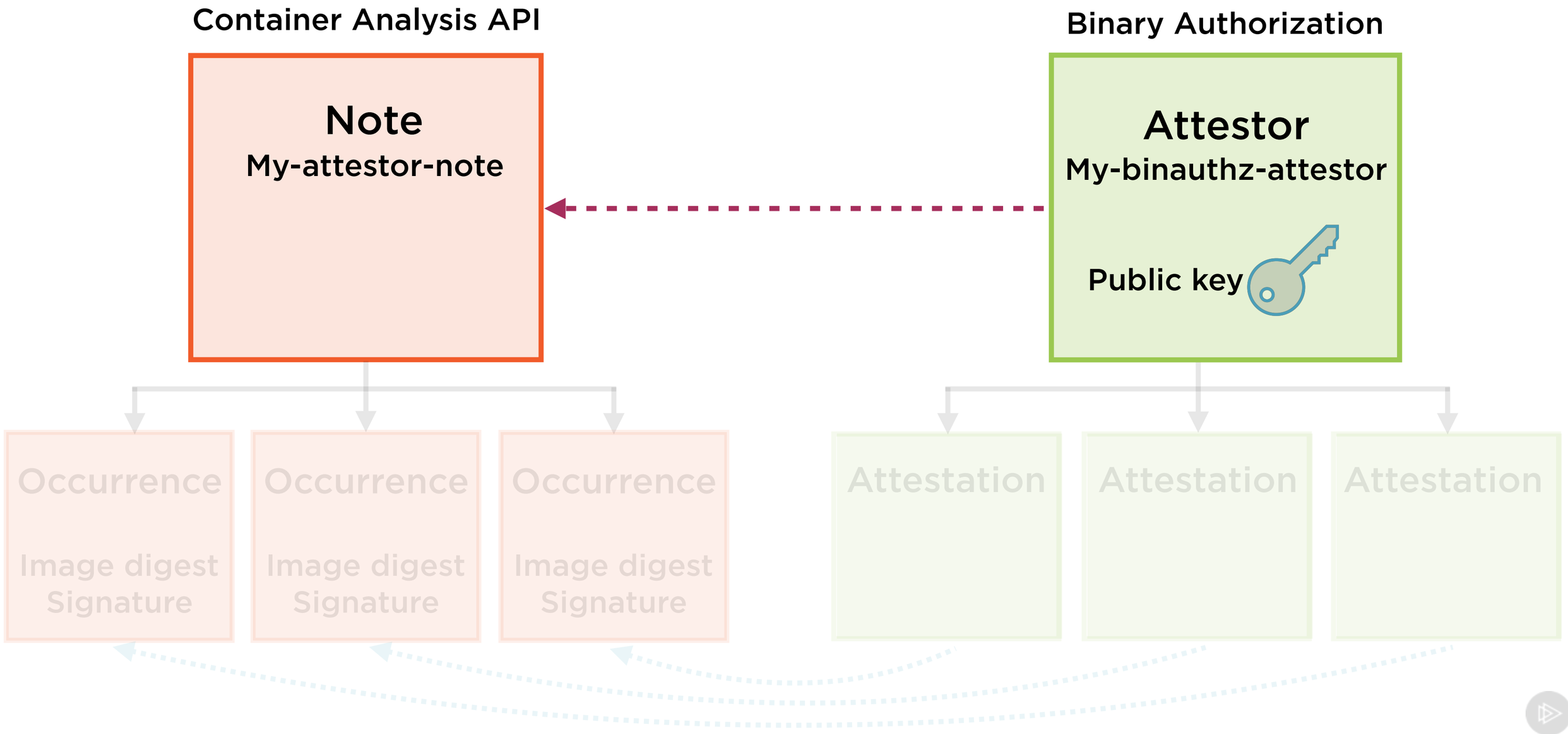
Container Analysis Note



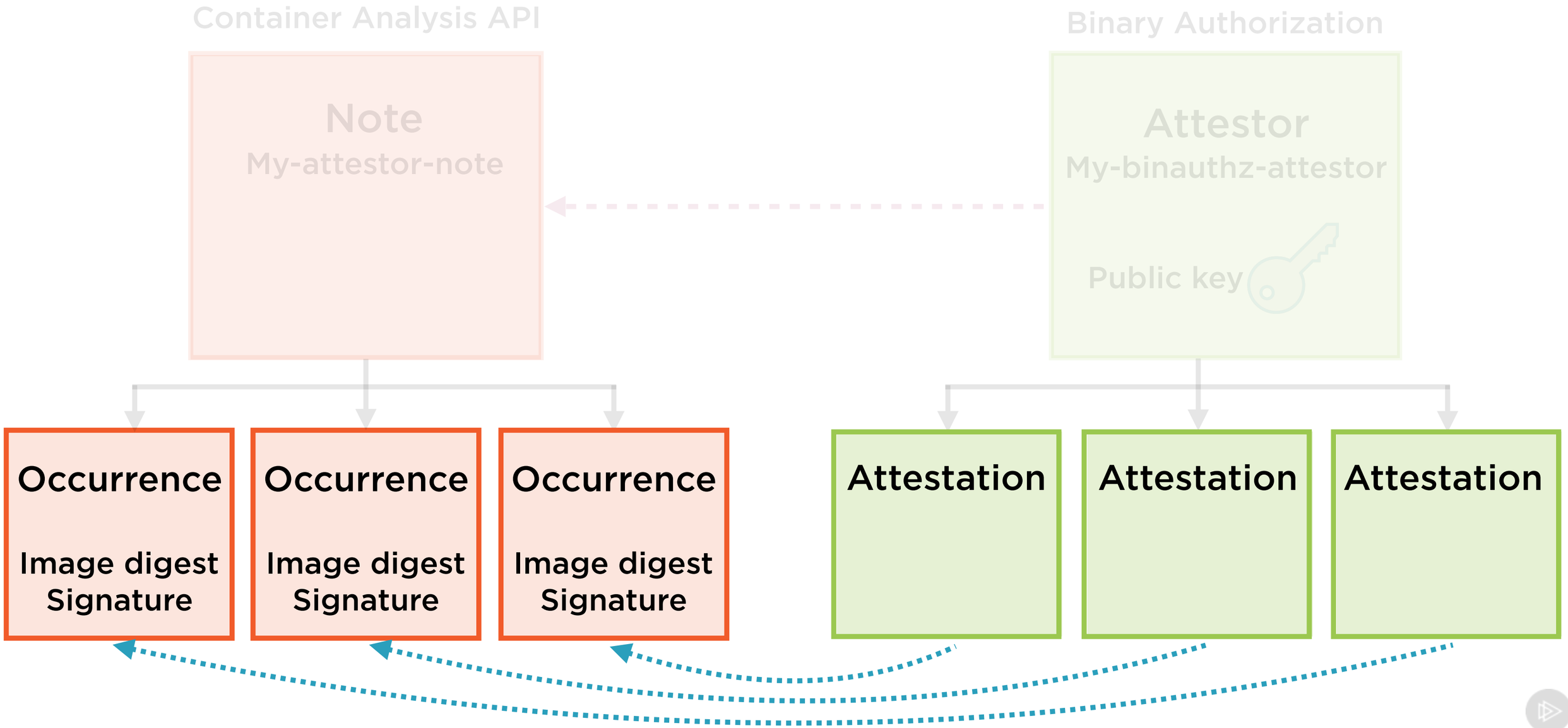
Note Represents an Attestor



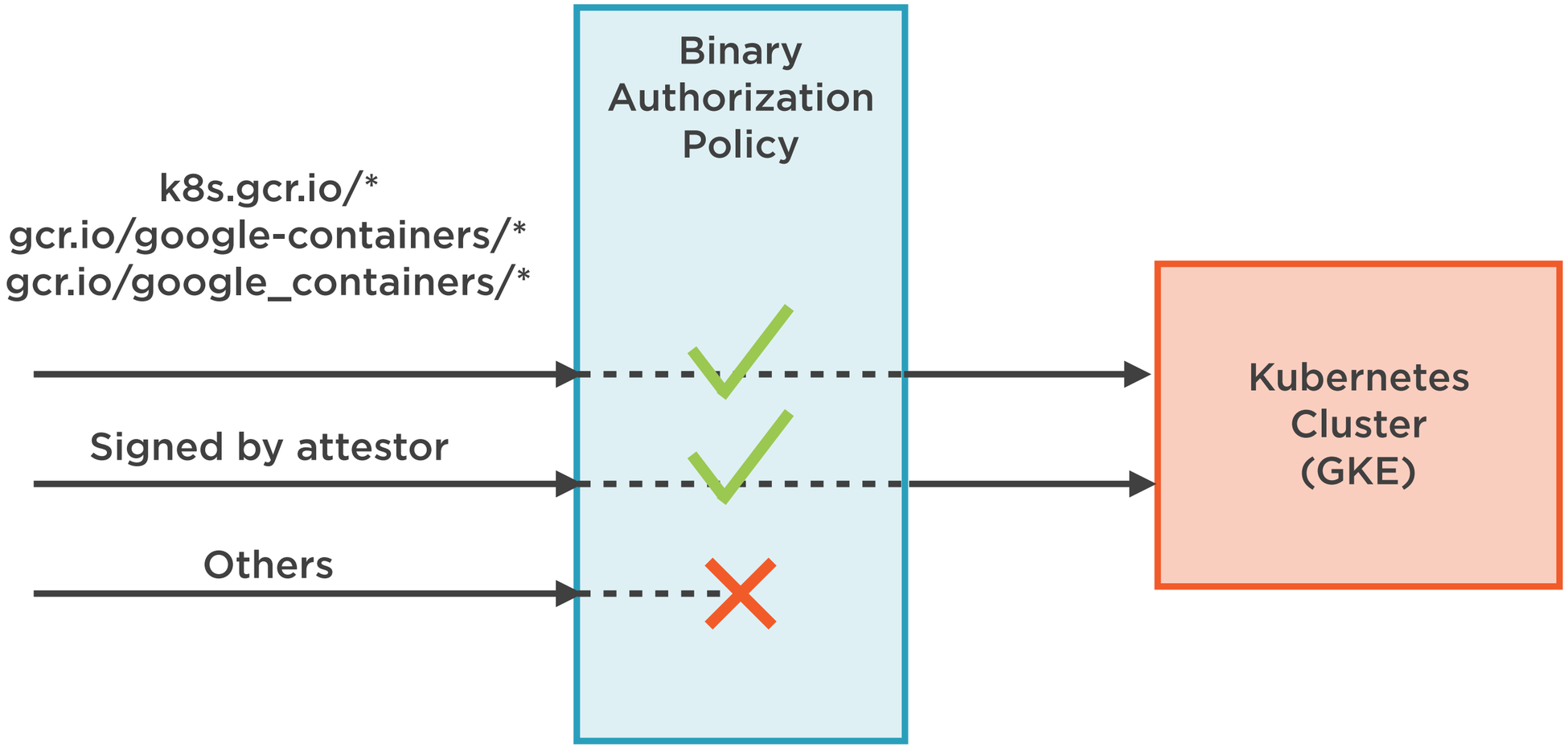
Attestor Uses Public Keys for Attestations



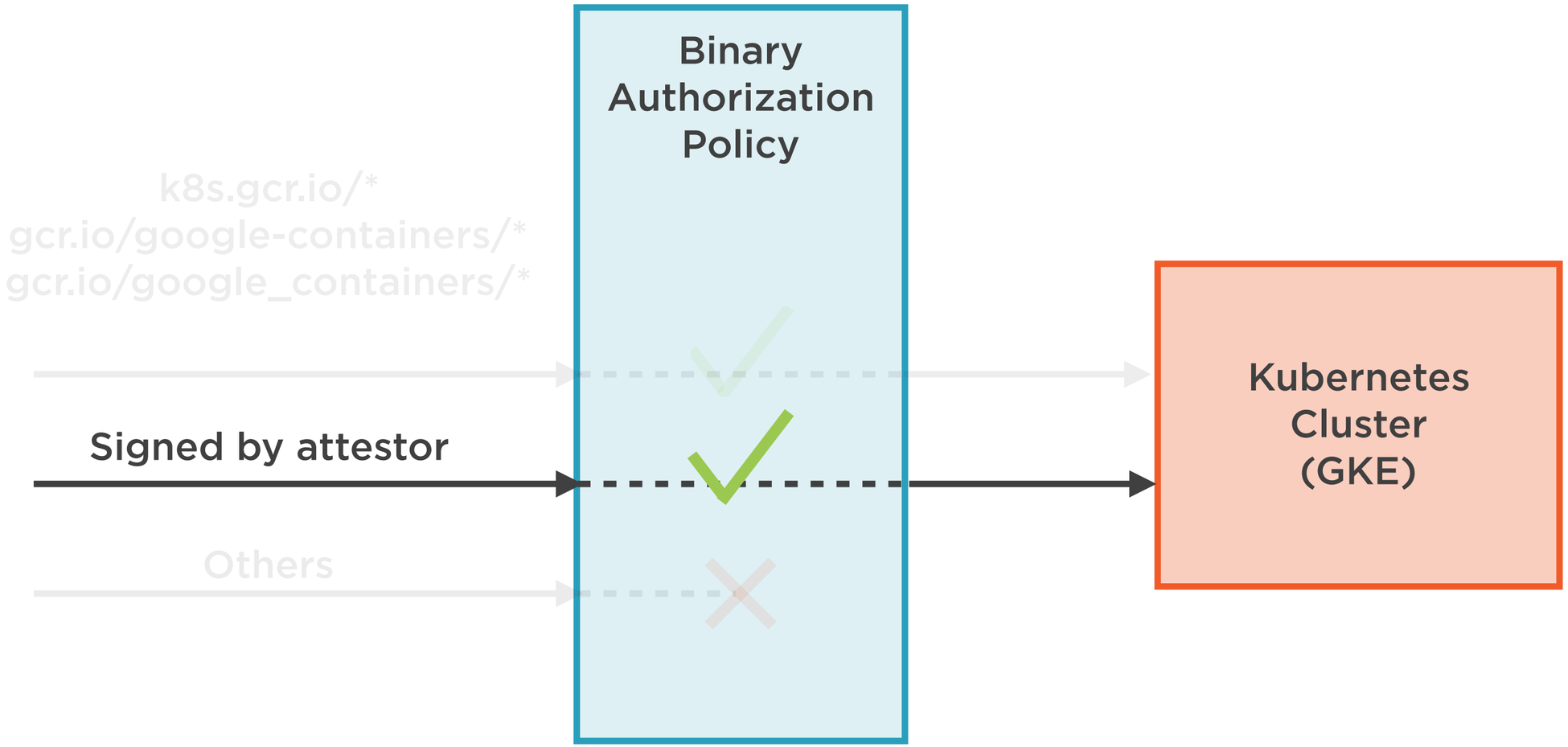
Attestation is an Occurrence



Allow Attested Images on Cluster



Allow Attested Images on Cluster



Demo

Use binary authorization to secure deployments on the Kubernetes cluster

Summary

Applications deployed to containers

Service and ingress objects

Volume abstractions for shared state

Deploy attested containers using binary authorization