OpenShift Security
The usage of PKI Infrastructures

We start at 13:00

Stronger Platform Security
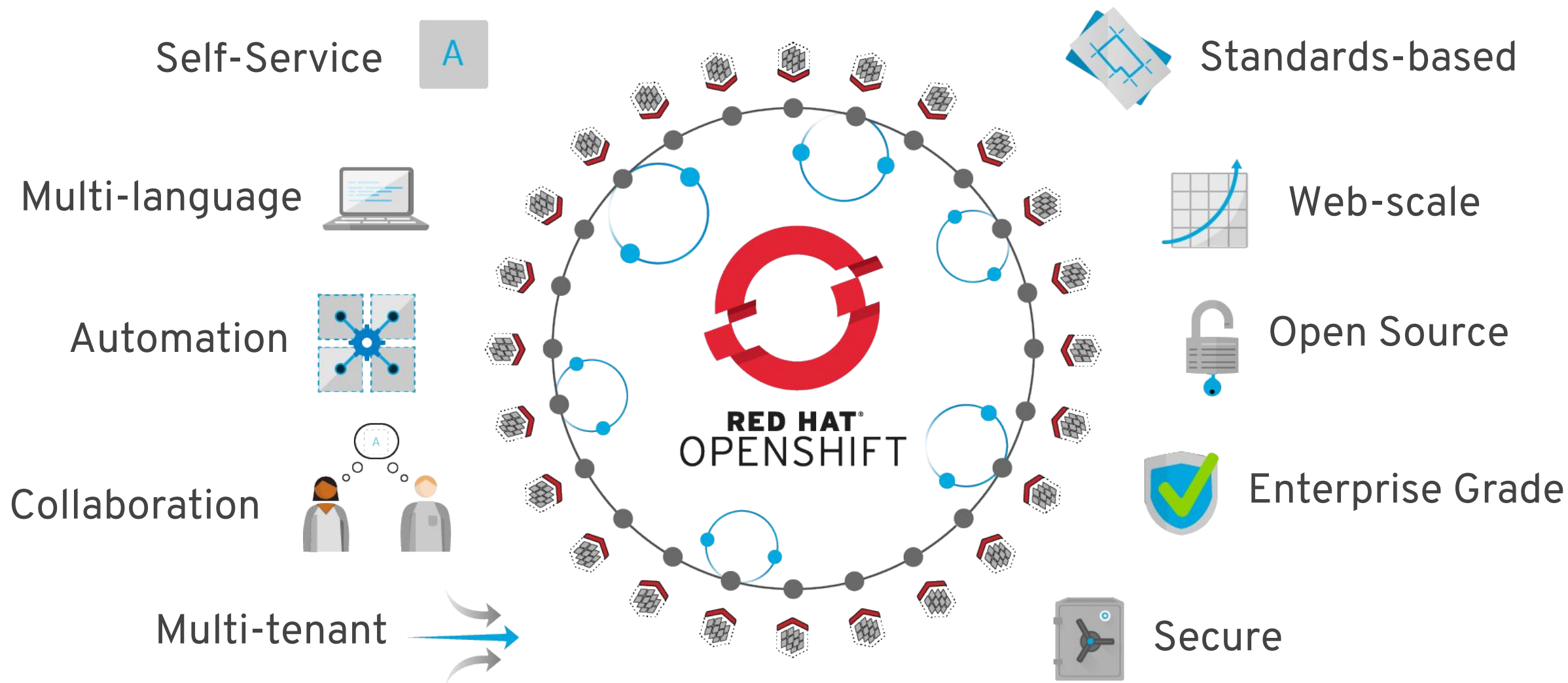
Defense in Depth

CONTROL
Application Security

DEFEND
Infrastructure

EXTEND

- FIPS Compliance

- Encrypt etcd datastore

- RHEL CoreOS network bound disk encryption

- Private clusters with existing VPN / VPC

- Internal ingress controller

- Ingress Cipher & TLS Policy Configuration

- Log forwarding (tech preview)

2

Red Hat

Value of OpenShift

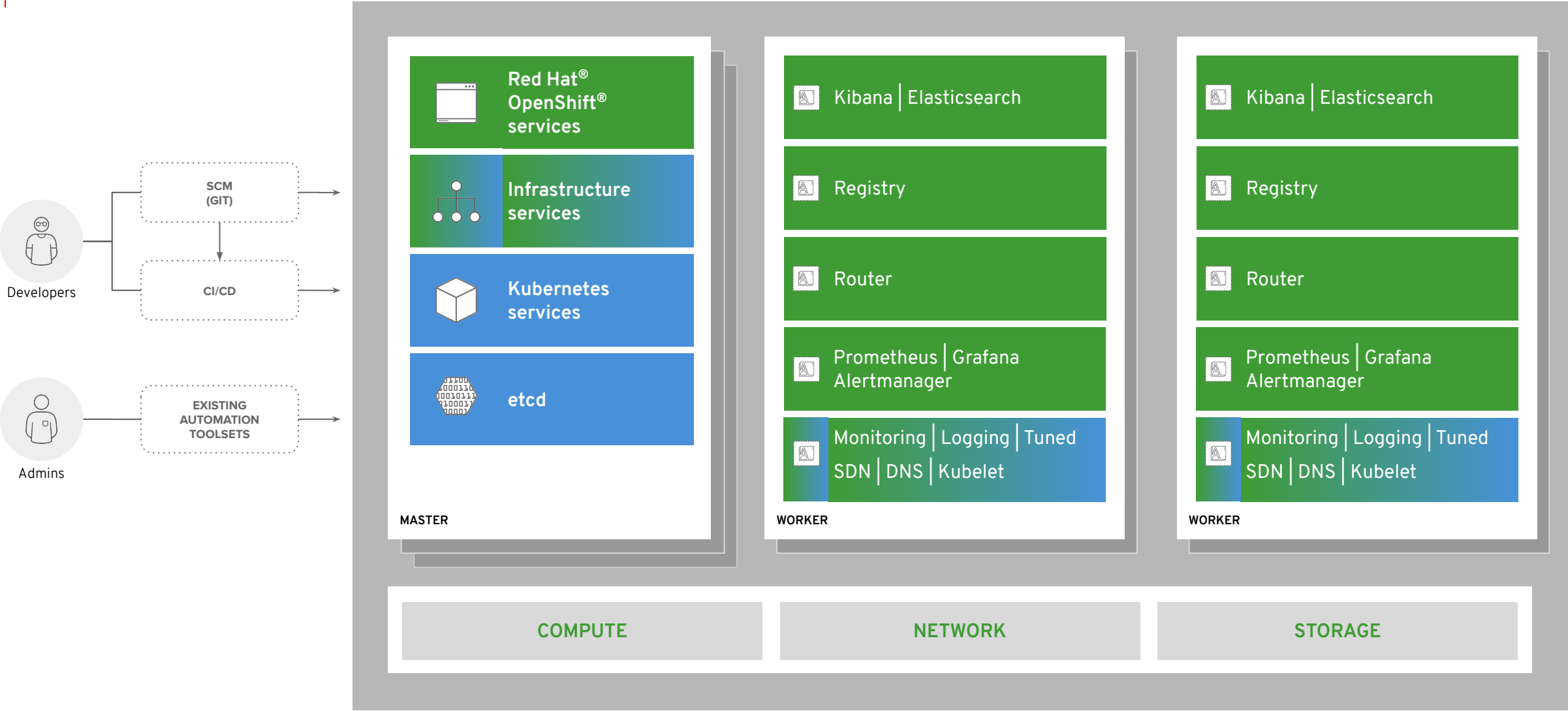| Monitoring, Logging, Registry, Router, Telemetry	Service Mesh, Serverless, Middleware/Runtimes, ISVs	Dev Tools, CI/CD, Automated Builds, IDE
Cluster Services	**Application Services**	**Developer Services**

Automated Operations

Kubernetes

Red Hat Enterprise Linux | RHEL CoreOS

Best IT Ops Experience   CaaS ⟷ PaaS ⟷ FaaS   **Best Developer Experience**

Red Hat

Developers

SCM (GIT)

CI/CD

Admins

EXISTING AUTOMATION TOOLSETS

MASTER

Red Hat® OpenShift® services

Infrastructure services

Kubernetes services

etcd

WORKER

Kibana | Elasticsearch

Registry

Router

Prometheus | Grafana Alertmanager

Monitoring | Logging | Tuned
SDN | DNS | Kubelet

WORKER

Kibana | Elasticsearch

Registry

Router

Prometheus | Grafana Alertmanager

Monitoring | Logging | Tuned
SDN | DNS | Kubelet

COMPUTE

NETWORK

STORAGE

Red Hat

PKI in OpenShift

Secure OCP Infrastructure → Secure OCP Internal Communication → Encrypt Workload Communication
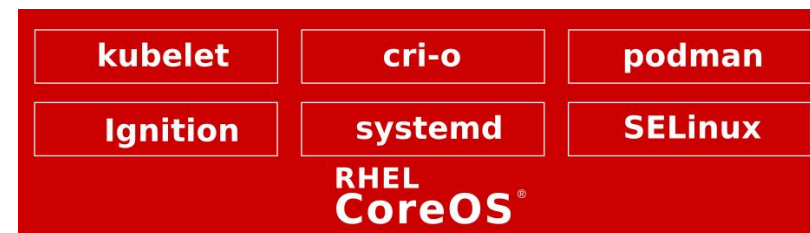
Red Hat Enterprise Linux CoreOS

4.3 Image Availability: (* = new)

- OpenStack
- GCP
- Azure

- Amazon
- vSphere
- Bare Metal (unified x86_64 image)*
- IBM Z (DASD & FCP via z-stream)*

FIPS mode support:

- Enforces FIPS validated ciphers for node-level cryptography
- Configurable at install/provisioning

Network Bound Disk Encryption:

- Provides encryption for local storage
- Addresses disk/image theft
- Platform/cloud agnostic implementation
- TPM/vTPM (v2) and Tang endpoints for automatic decryption

kubelet	cri-o	podman
Ignition	systemd	SELinux

RHEL CoreOS®

Kmods via containers:

- A framework to build and load 3rd party kmods
- Viable for drivers unsuitable for the SRO

Product Manager: Ben Breard   Generally Available   **Red Hat**

OpenShift 4 Fips 140-2 Compliant Cluster

FIPS ready Services
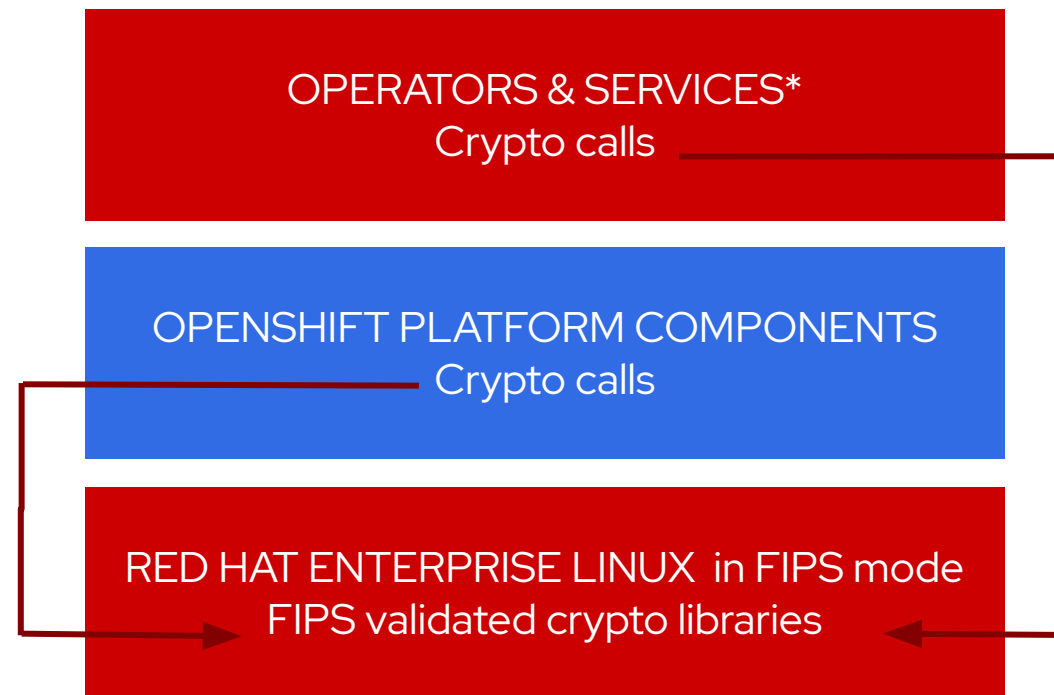
- When built with RHEL 7 base image

OpenShift calls FIPS validated crypto

- When running on RHEL in FIPS mode, OpenShift components bypass go cryptographic routines and call into a RHEL FIPS 140-2 validated cryptographic library
- This feature is specific to binaries built with the RHEL go compiler and running on RHEL

RHEL CoreOS FIPS mode

- Configure at install to enforce FIPS validated ciphers for node-level cryptography
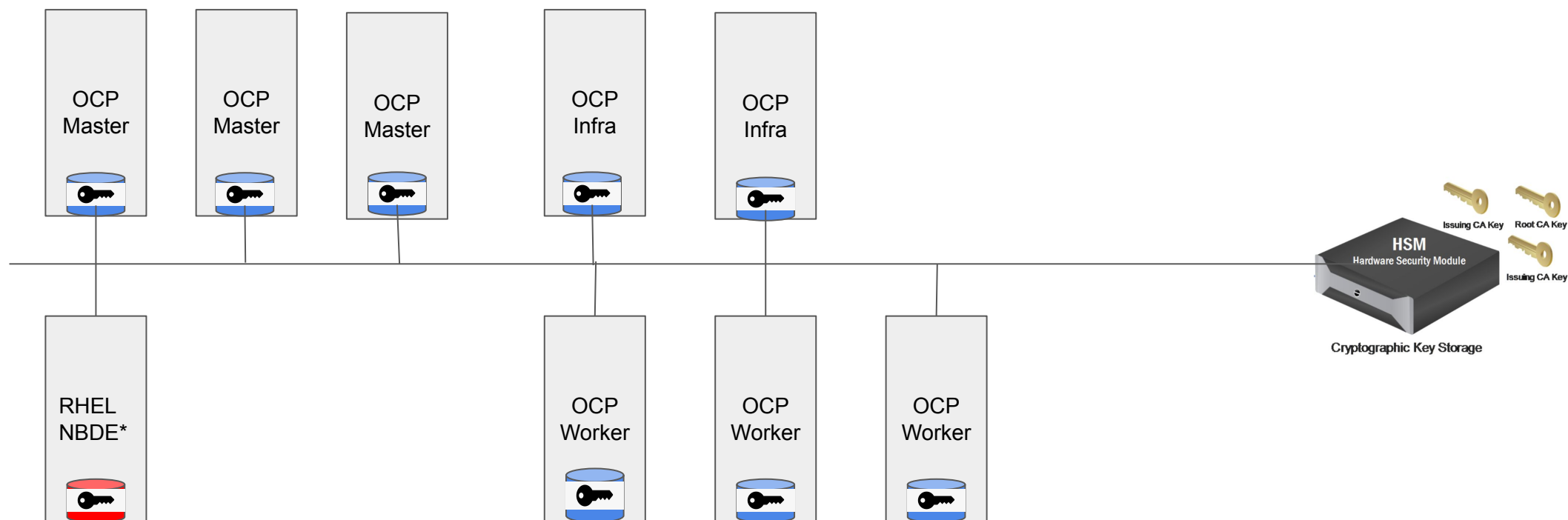
Note: products are not FIPS validated, only libraries.

OPERATORS & SERVICES*
Crypto calls

OPENSHIFT PLATFORM COMPONENTS
Crypto calls

RED HAT ENTERPRISE LINUX in FIPS mode
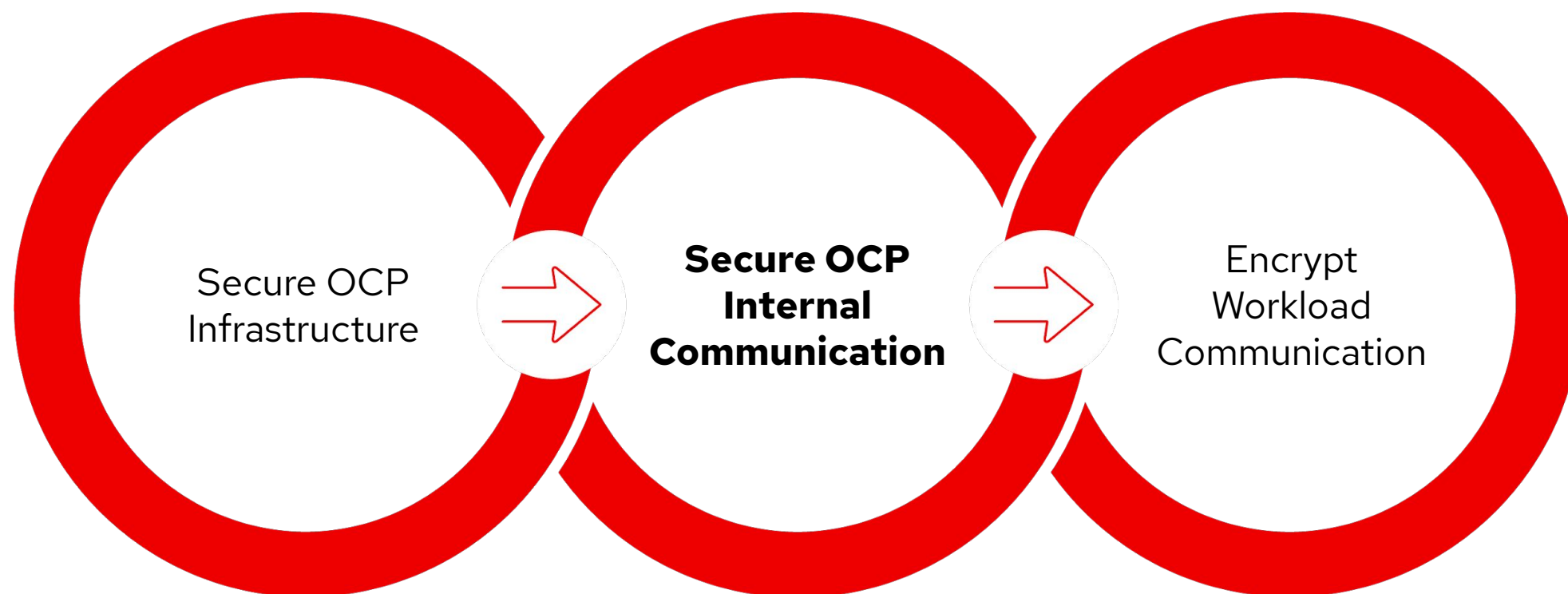FIPS validated crypto libraries

*When built with RHEL base images

More about RHEL go and FIPS 140-2

Encrypting the Disk of the OCP Nodes

*Network bound disk encryption (Clavis & Tang)

# PKI in OpenShift

Secure OCP Infrastructure → **Secure OCP Internal Communication** → Encrypt Workload Communication

OpenShift 4 etcd Encryption

Encrypt secrets, config maps...

- Encryption of the etcd datastore is optional. Once enabled, encryption cannot be disabled.
- The aes-cbc cipher is used.
- Keys are created and automatically rotated by an operator and stored on the master node's file system.
- Keys are available as a secret via the kube API to a cluster admin.
- Assuming a healthy cluster: after enabling encryption, within a day, all relevant items in etcd are encrypted
- Backup: The etcd data store should be backed up separately from the file system with the key.
- Disaster recovery: a backup of both the encrypted etcd data and encryption keys must be available.

Red Hat® OpenShift® services

Kubernetes services

Infrastructure services
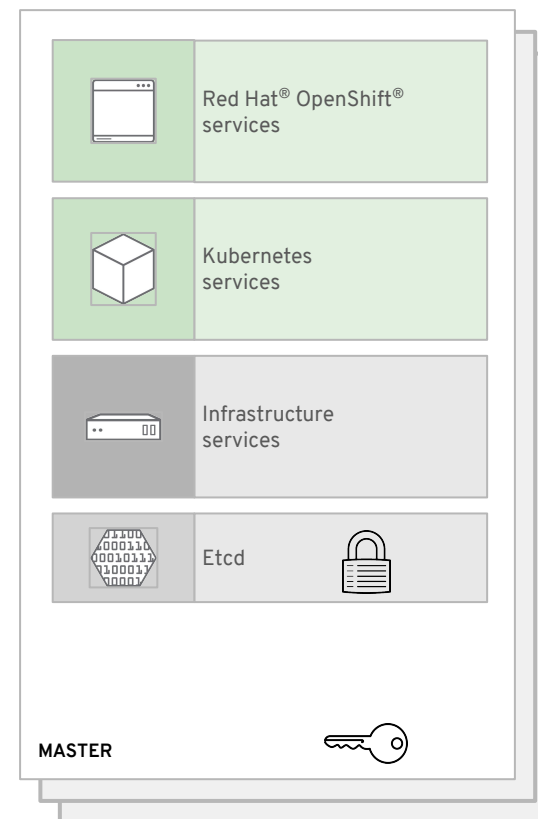
Etcd

MASTER

Certificates and Certificate Management

- OpenShift provides its own internal CA

- Certificates are used to provide secure connections to

  - master (APIs) and nodes
  - Ingress controller and registry
  - etcd

- Certificate rotation is automated

- Optionally configure external endpoints to use custom certificates
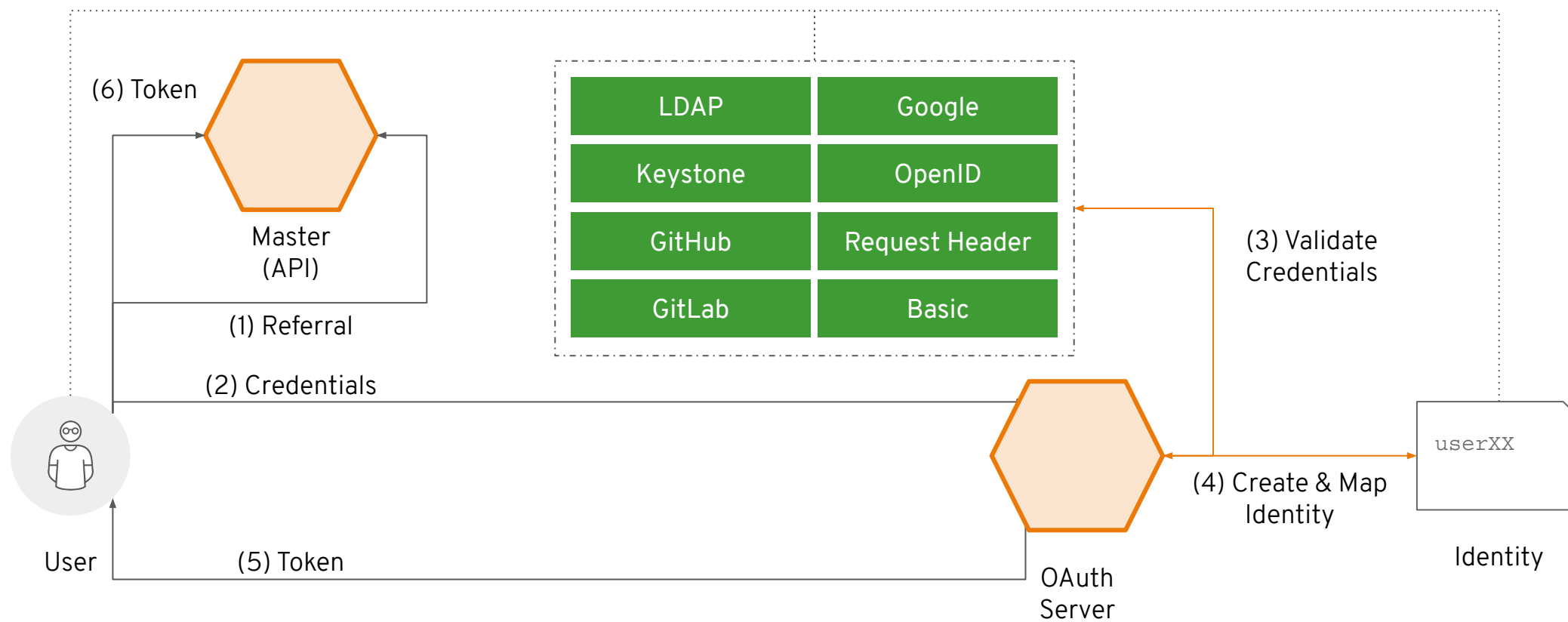
🔒✓ MASTER

🔒✓ ETCD

🔒✓ NODES

🔒✓ INGRESS CONTROLLER

🔒✓ CONSOLE

🔒✓ REGISTRY
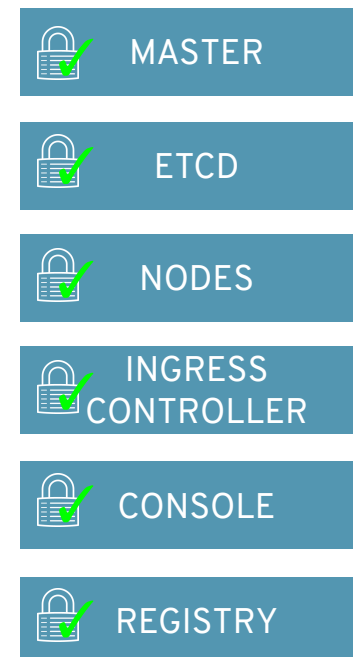
Encrypting the OCP Network traffic and the etcd Database
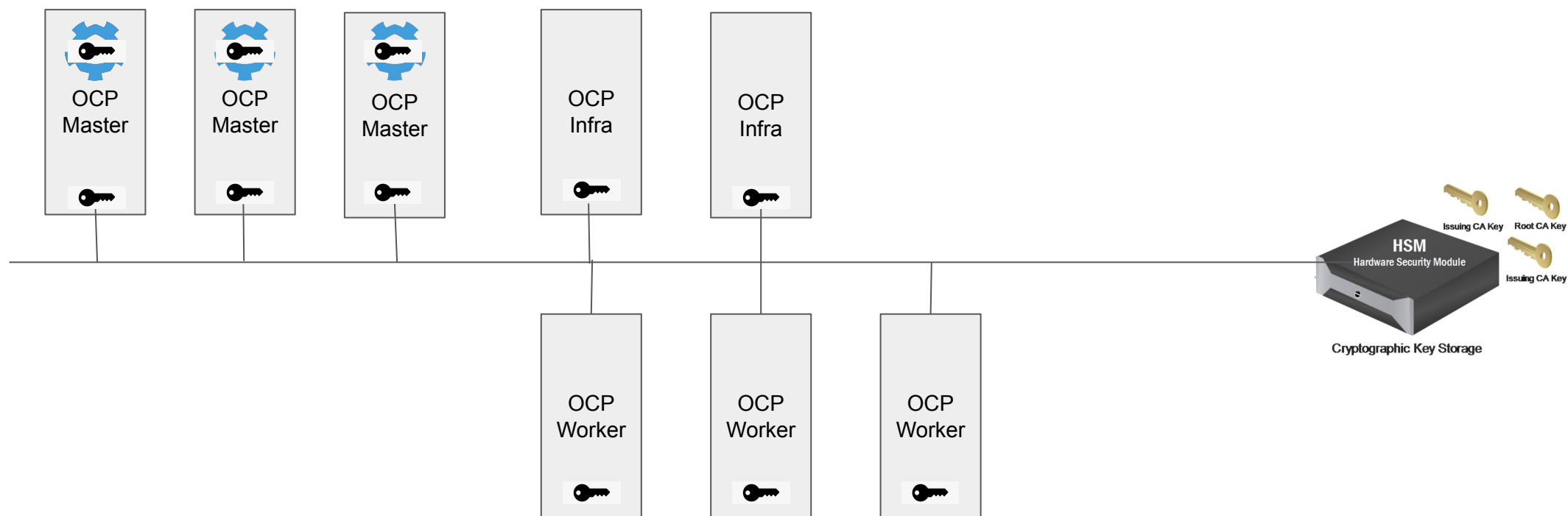
Identity and Access Management

Identity and Access Management

Fine-Grained RBAC

- Project scope & cluster scope available

- Matches request attributes (verb,object,etc)

- If no roles match, request is denied (deny by default)

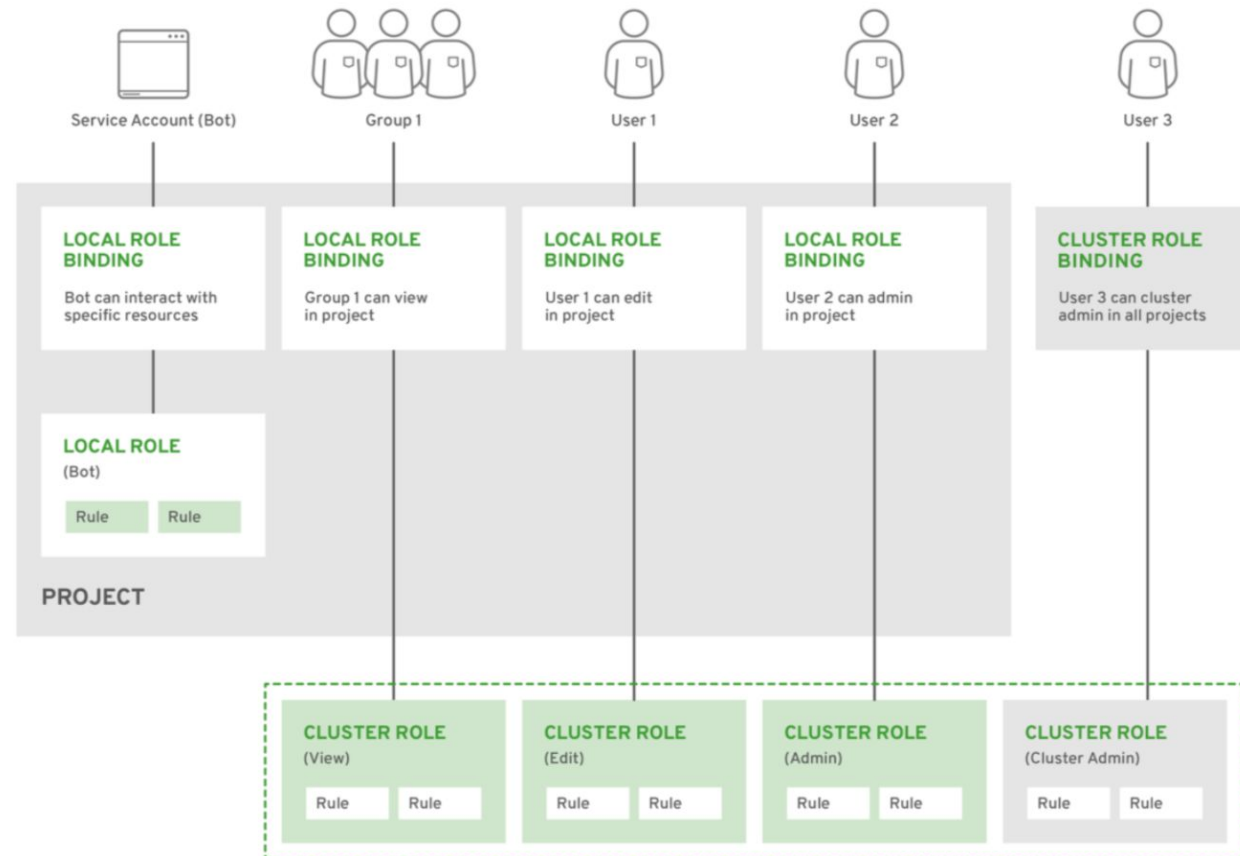- Operator- and user-level roles are defined by default
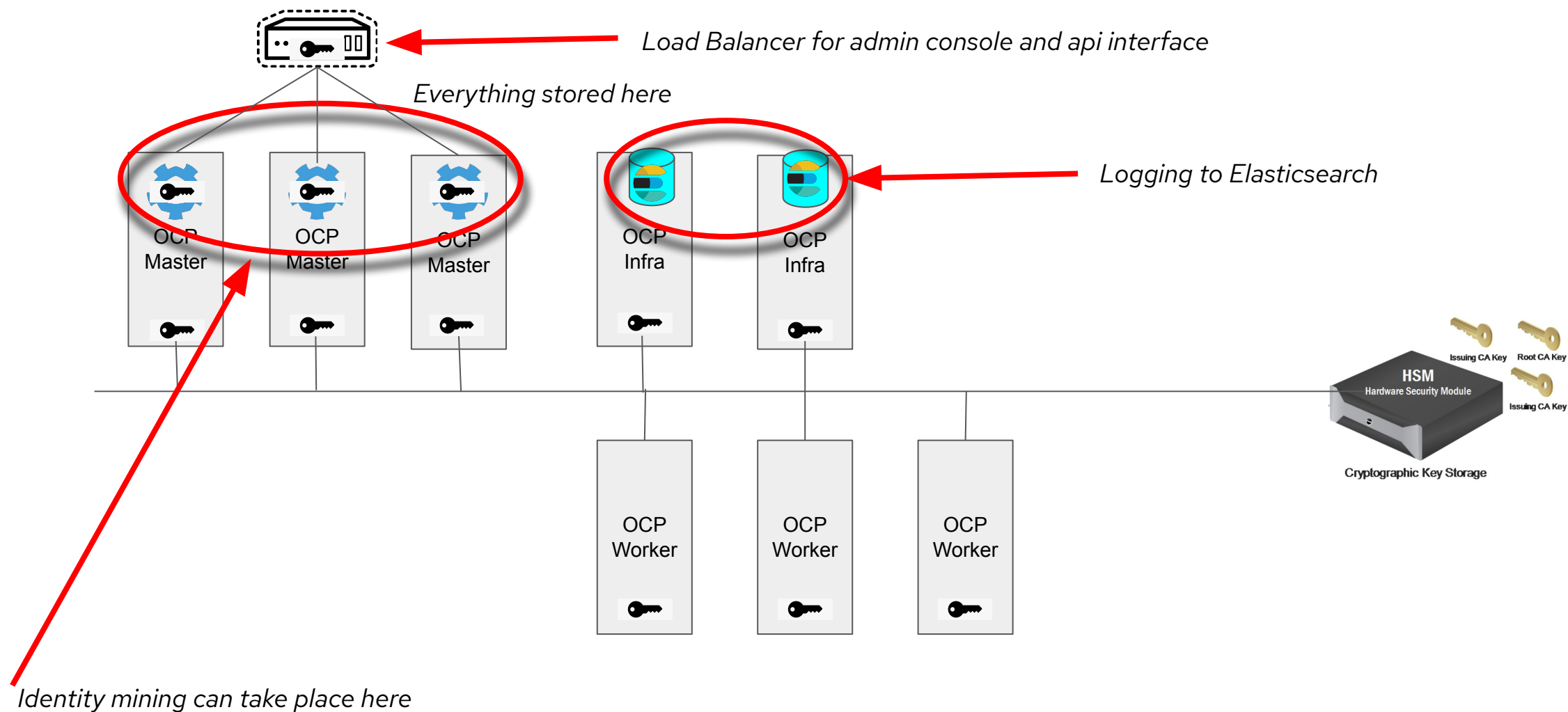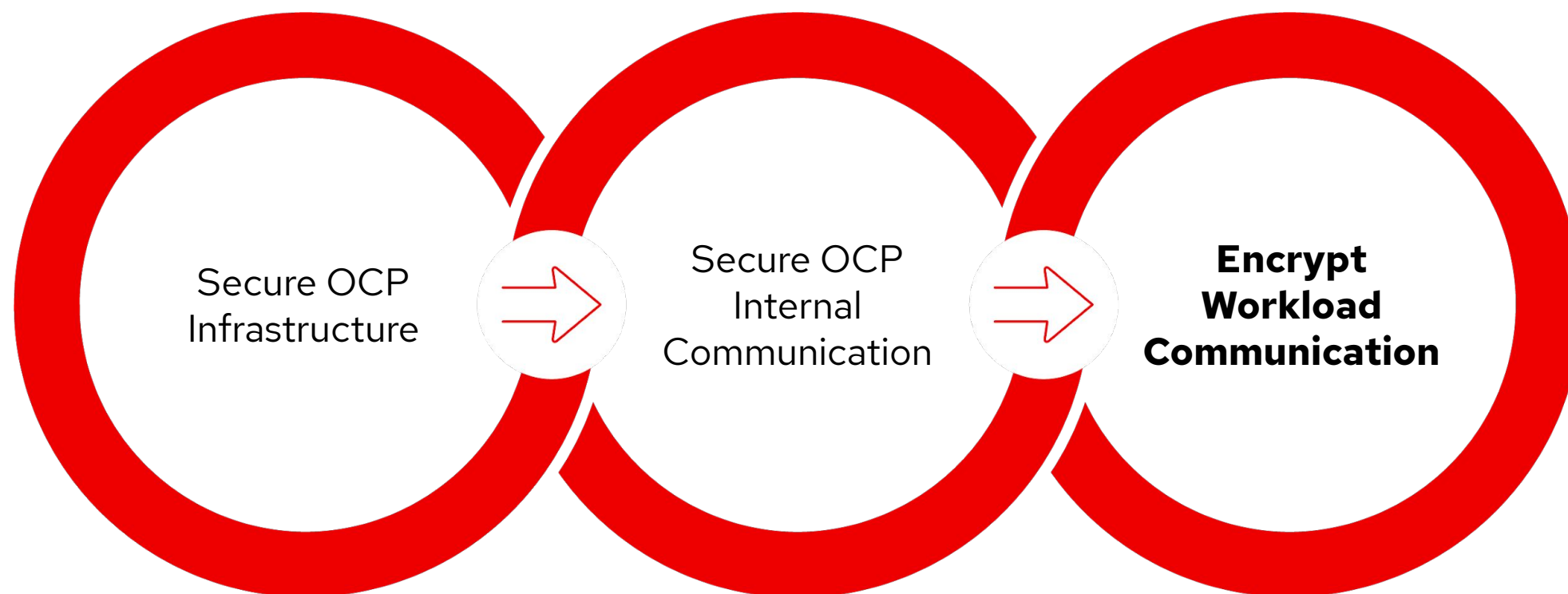
- Custom roles are supported

Figure 12 - Authorization Relationships
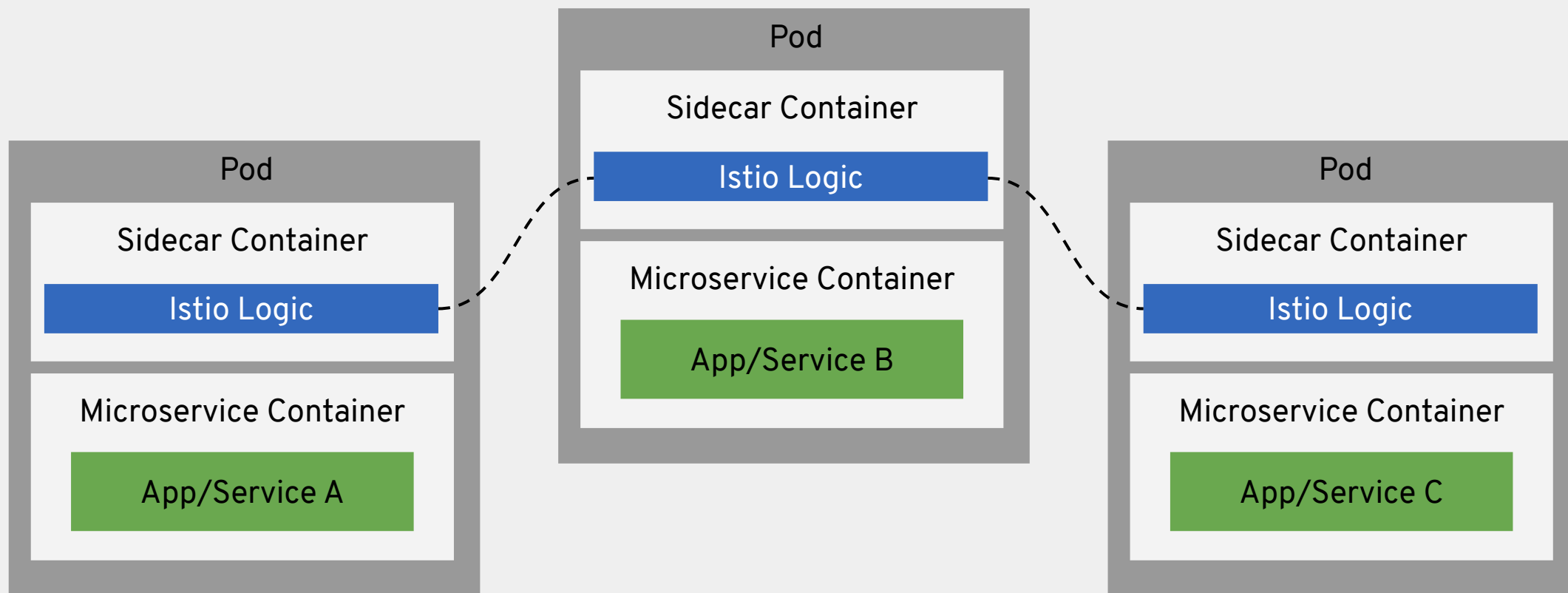
Identity Mining and SIAM Mining

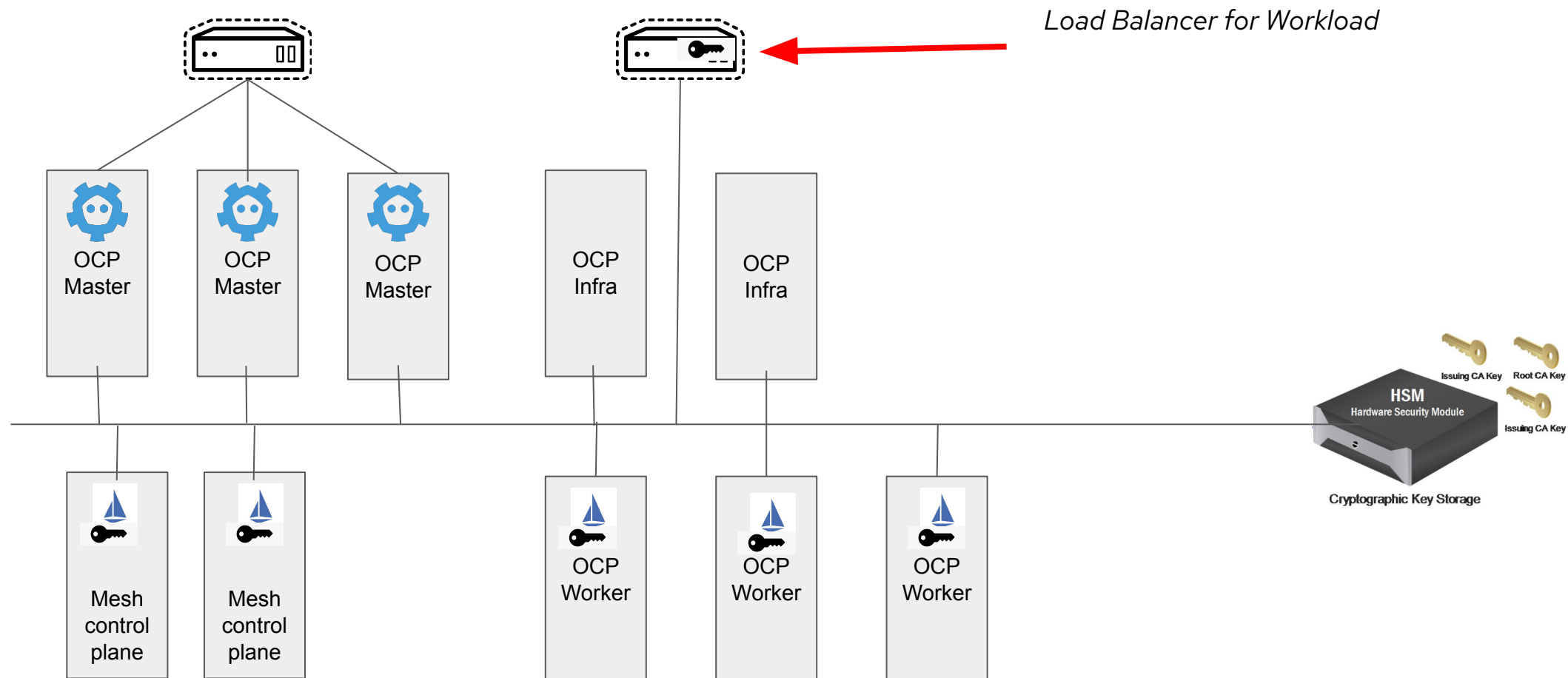
Load Balancer for admin console and api interface

Everything stored here

Logging to Elasticsearch

OCP Master

OCP Master

OCP Master

OCP Infra

OCP Infra

HSM
Hardware Security Module

Issuing CA Key   Root CA Key

Issuing CA Key

Cryptographic Key Storage

OCP Worker

OCP Worker

OCP Worker

Identity mining can take place here

PKI in OpenShift

Secure OCP Infrastructure → Secure OCP Internal Communication → **Encrypt Workload Communication**

Load Balancer for Workload
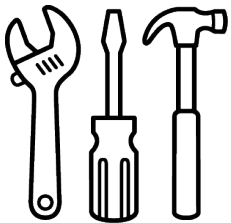
Stronger Platform Security

Defense in Depth

CONTROL
Application Security

DEFEND
Infrastructure

EXTEND

- FIPS Compliance

- Encrypt etcd datastore

- RHEL CoreOS network bound disk encryption

- Private clusters with existing VPN / VPC

- Internal ingress controller

- Ingress Cipher & TLS Policy Configuration

- Log forwarding (tech preview)

Product Manager: Kirsten Newcomer & Keith Basil

Red Hat

Thank you !

Please give me a little feedback

https://www.menti.com/z71igy9cgk

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

in   linkedin.com/company/red-hat

▶   youtube.com/user/RedHatVideos

f   facebook.com/redhatinc

🐦   twitter.com/RedHat

Red Hat | IBM