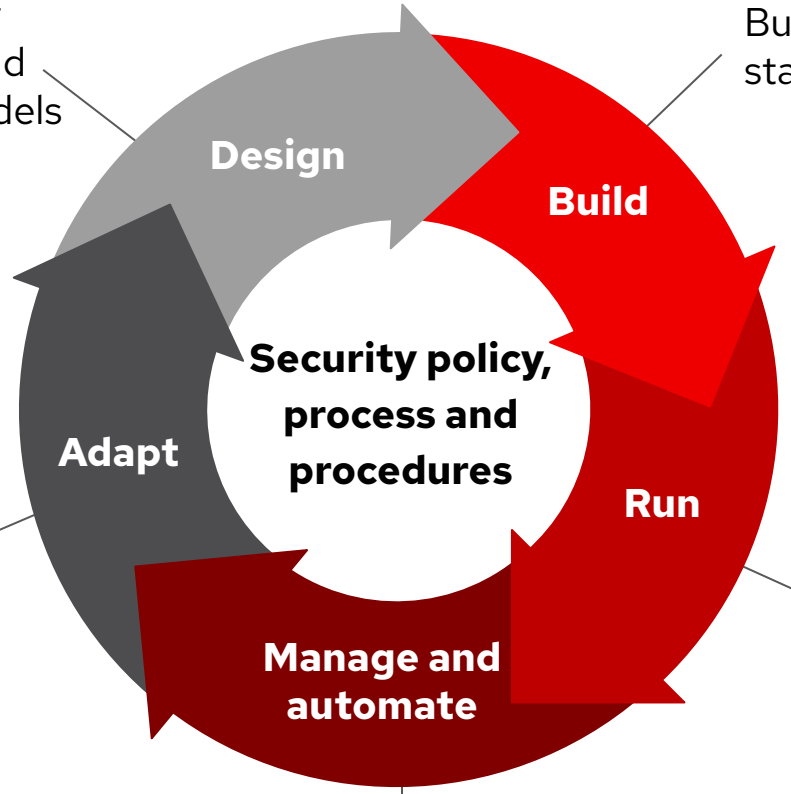
Red Hat
OpenShift

OpenShift Security &
The usage of PKI Infrastructures

Built in security across the portfolio

Security must be continuous and holistic



Identify security requirements and governance models

Built-in from the start; not bolted-on

Deploy to trusted platforms with enhanced security capabilities

Automate systems for security and compliance

Revise, update, remediate as the landscape changes

FedRAMP

NIST National Institute of Standards and Technology U.S. Department of Commerce

CIS Center for Internet Security

National Cyber Security Centre

PCI Security Standards Council

HIPAA Health Insurance Portability & Accountability Act

Red Hat | IBM

Considerations for Securing Containers and Kubernetes

NIST 800-190

"Use container-specific host OSs instead of general-purpose ones to reduce attack surfaces."

CNCF Kube Security Audit

"...the underlying hosts, components, and environment of a Kubernetes cluster must be configured and managed. This management has a direct impact on the capabilities of the cluster..."

Gartner Market Guide for Cloud Workload Protection

"The best way to secure these rapidly changing and short-lived workloads is to start their protection proactively in the development phase ..."

"Replace antivirus (AV)-centric strategies with a "zero-trust execution"/default deny/application control approach to workload protection where possible...."

Sources

NIST Special Publication 800-190 Application Container Security Guide
CNCF Cloud Native Security Whitepaper
Kubernetes Security Whitepaper, Trail of Bits, May 31, 2019
Gartner: Market Guide for Cloud Workload Protection Platforms, ID G00356240, April 8, 2019

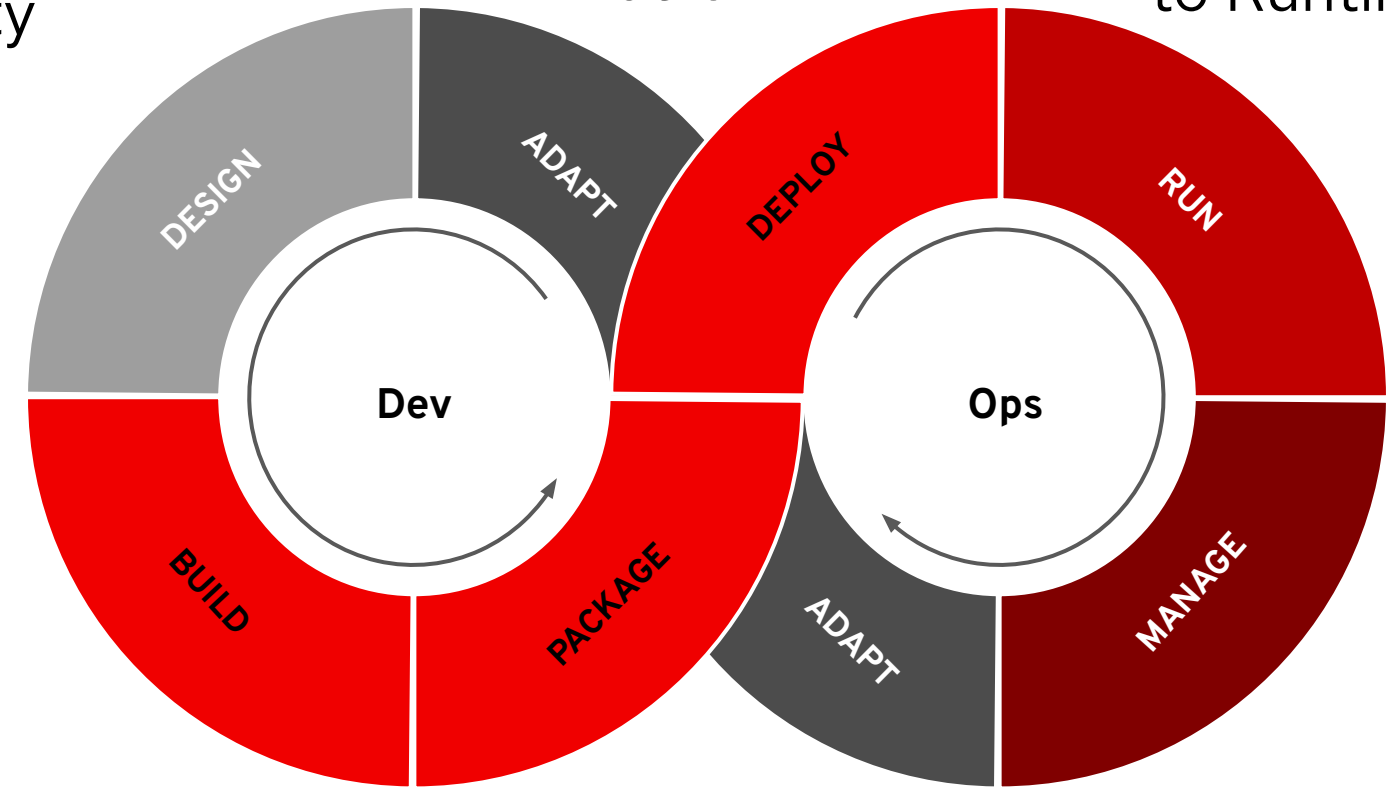
Red Hat

Containers and Kubernetes need DevSecOps

Control Application Security

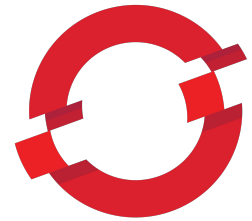
Protect the Platform

Detect & Respond to Runtime Threats



Red Hat contributions to Kubernetes

RBAC Authorization | Stateful Sets | Init Containers | Rolling Update Status | Pod Security Policy Limits | Memory based Pod Eviction | Quota Controlled Services | 1,000+ Nodes | Dynamic PV Provisioning | Multiple Schedulers | SECCOMP | Audit | Job Scheduler | Access Review API | Whitelisting Sysctls | Secure Cluster Policy | Evict Pods Disk IO | Storage Classes | Azure Data Disk | etcdv3 | RBAC API | Auth to kubelet API | Pod-level cGroups QoS | Kublet Eviction Model | RBAC | Storage Class | CustomResourceDefinitions | API Aggregation | Encrypted secrets in etcd | Limit Node Access | HPA Status Conditions | Network Policy | CRI Validation Test Suite | Local Persistent Storage | Audit Logging |



OPENSHIFT

Build: Control application security
Shift Security left

Best practices

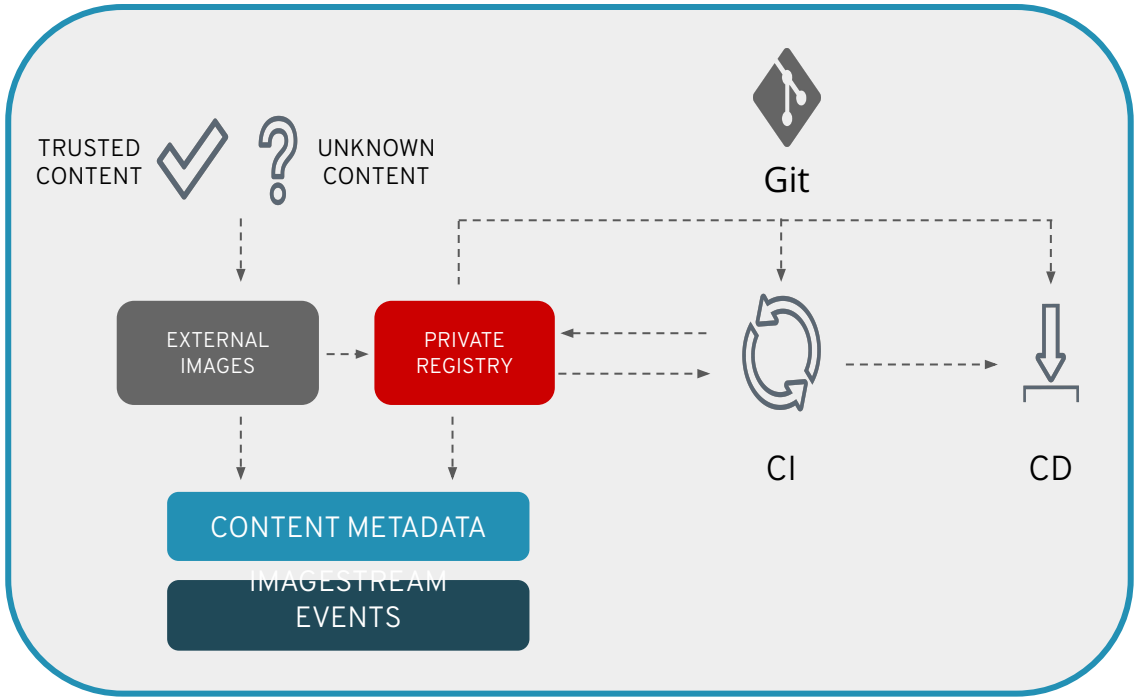
Red Hat UBI
- Use trusted sources for external content such as base images

Quay
- Use a trusted private registry to manage supply chain risk

OCP Pipelines
- Automate your CI/CD pipeline to enable rapid updates

Quay scanner (registry)
Code Ready (IDE)
ACS scanner (CI)
KubeLinter (CI)
- Integrate security tools / gates in your pipeline to identify
  - Known vulnerabilities
  - Application misconfigurations

ACM
- Use policy-based deployment tools to manage application placement (e.g. locality)



Red Hat

Deploy: Protect the application platform

Best practices

RHEL CoreOS
- Reduce attack surface with a container optimized operating system

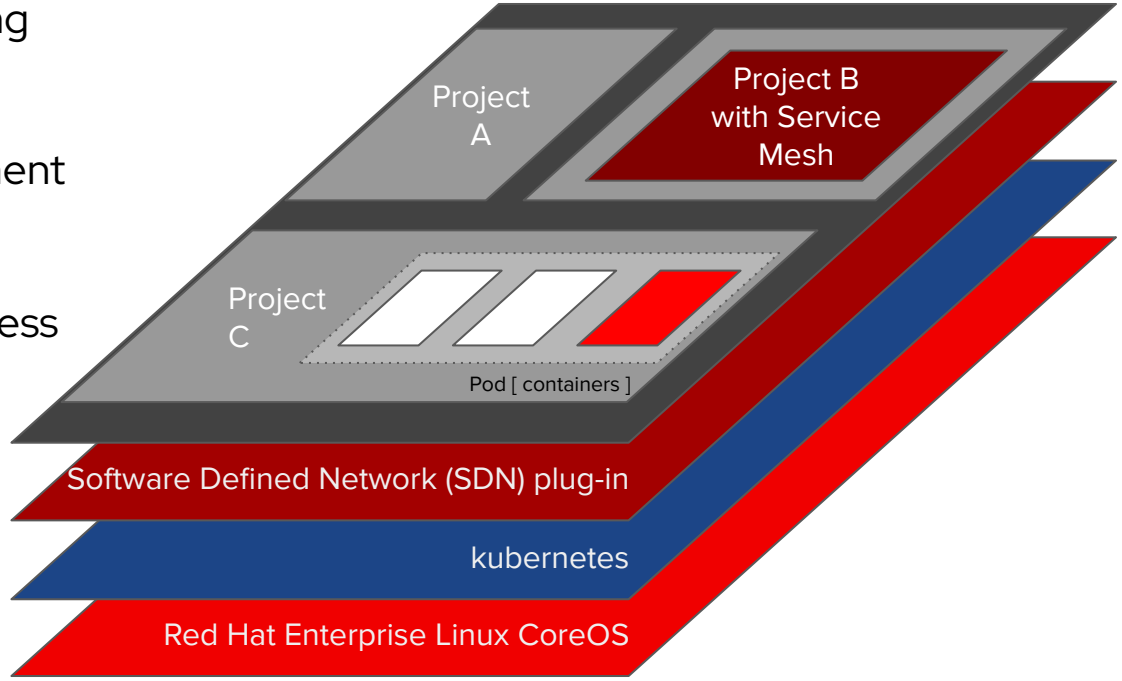
OCP Operators
ACM
- Use automated and policy-driven configuration management across your fleet

OCP RBAC
ACS to monitor
ACM to enforce
- Implement least privilege with fine-grained role based access control (RBAC)

OCP CAs
Service mesh
OCP IPSec
RHCOS NBDE
Encrypt etcd
- Encrypt platform data in transit and at rest

OCP Compliance Operator
ACS
ACM
- Use automated compliance, risk assessment and remediation solutions

OCP Security Context Constraints
ACS
- Reduce deployment risk with admission control policies that
  - Minimize admission of privileged pods, pods with host capabilities
  - Prevent admission of pods with critical vulnerabilities



Red Hat

Run: Securing the container runtime

Best practices

OCP ACS
- Minimize the impact of an attack by isolating running applications with
  - SELinux & Security Context Constraints
  - Kubernetes namespaces (Projects), RBAC
  - Network Policies for microsegmentation

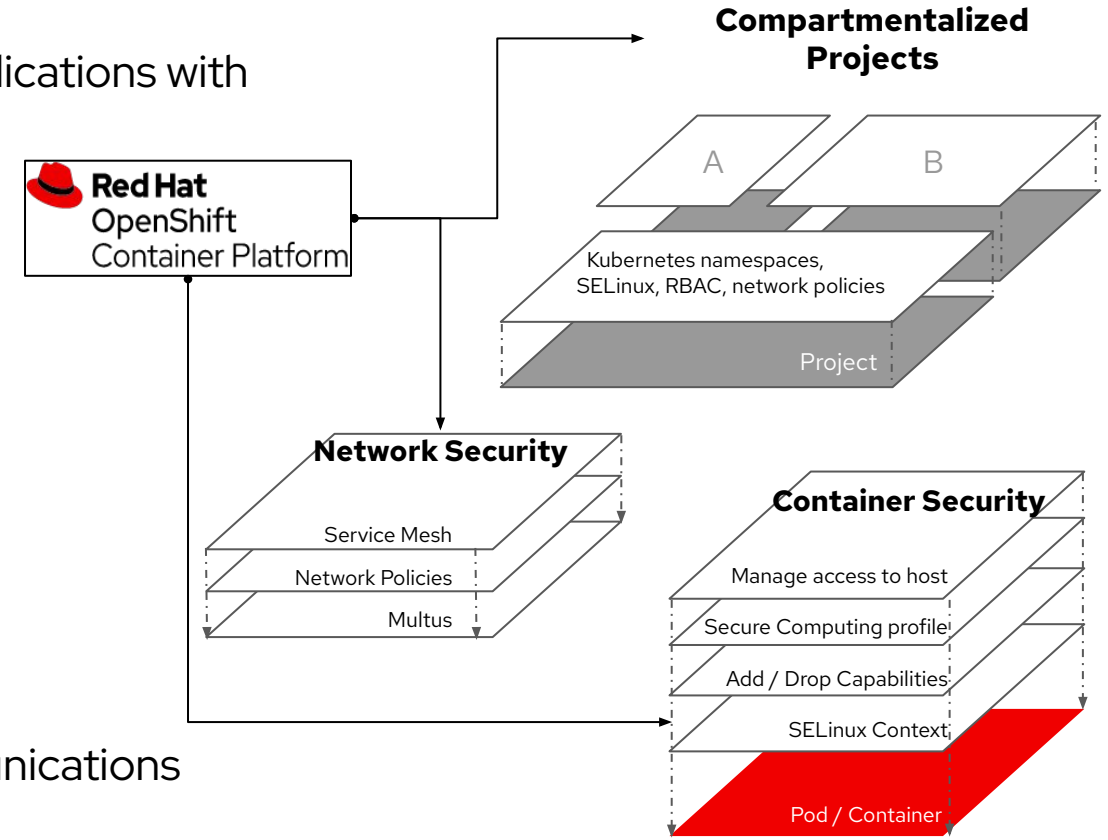
OCP ACM
- Use resource quotas to prevent resource exhaustion

- Manage application access and protect application data
  - Red Hat Single Sign On for user management

OCP
  - Secure routes / ingress, 3Scale API Gateway
  - Service mesh to encrypt pod-to-pod traffic
  - Egress IPs / firewall

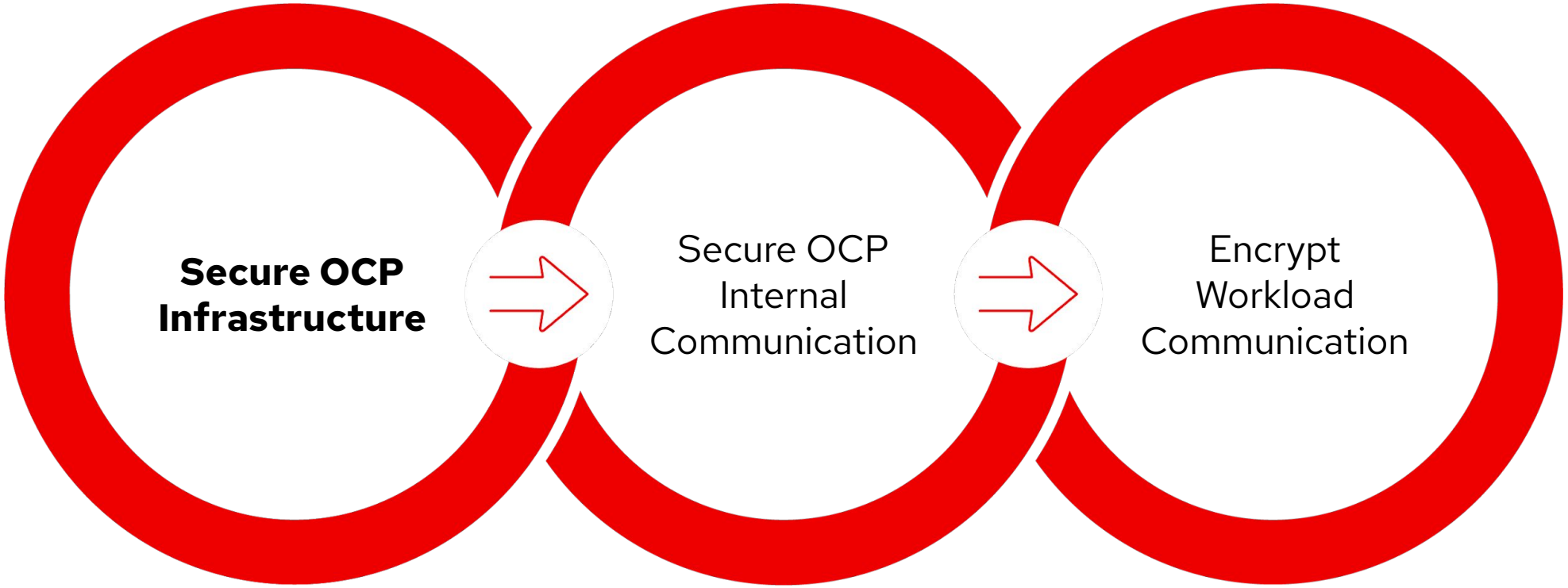
OCP ACS ACM
- Monitor application metrics, logging and network communications

ACS
- Automate threat detection and response
  - Alert or kill pods based on anomalous behavior
  - Detect privilege escalation and risky processes such as cryptomining



Red Hat

PKI in OpenShift



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

Kmods via containers:

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

OpenShift 4 Fips 140-2 Compliant Cluster

FIPS ready Services

- When built with RHEL 7 base image

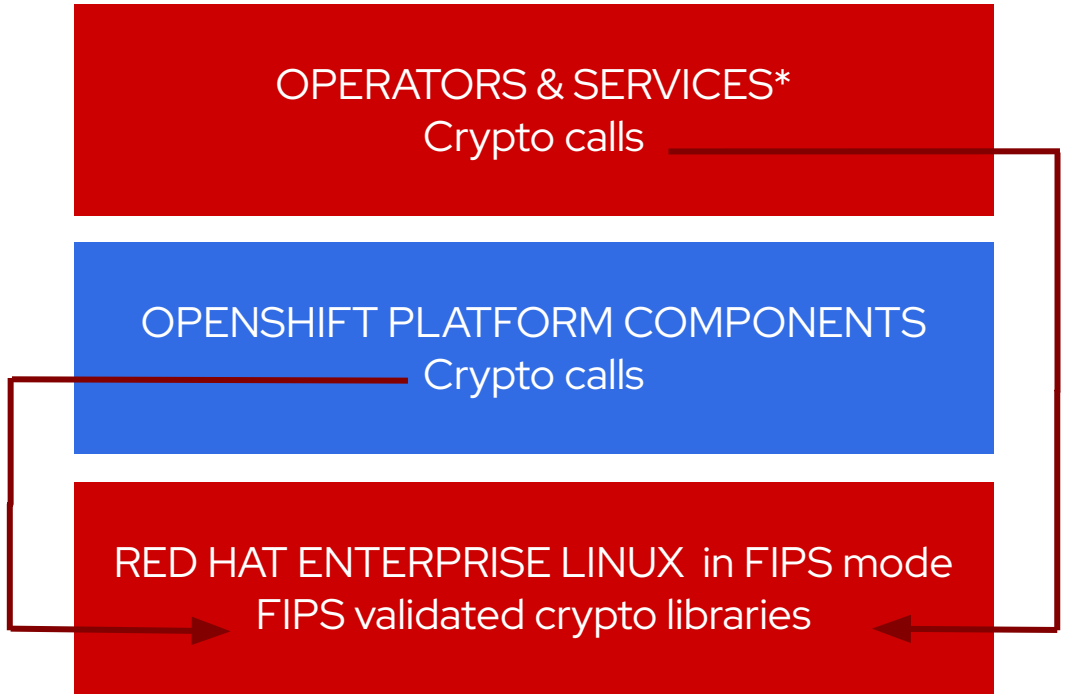
OpenShift calls FIPS validated crypto

- 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

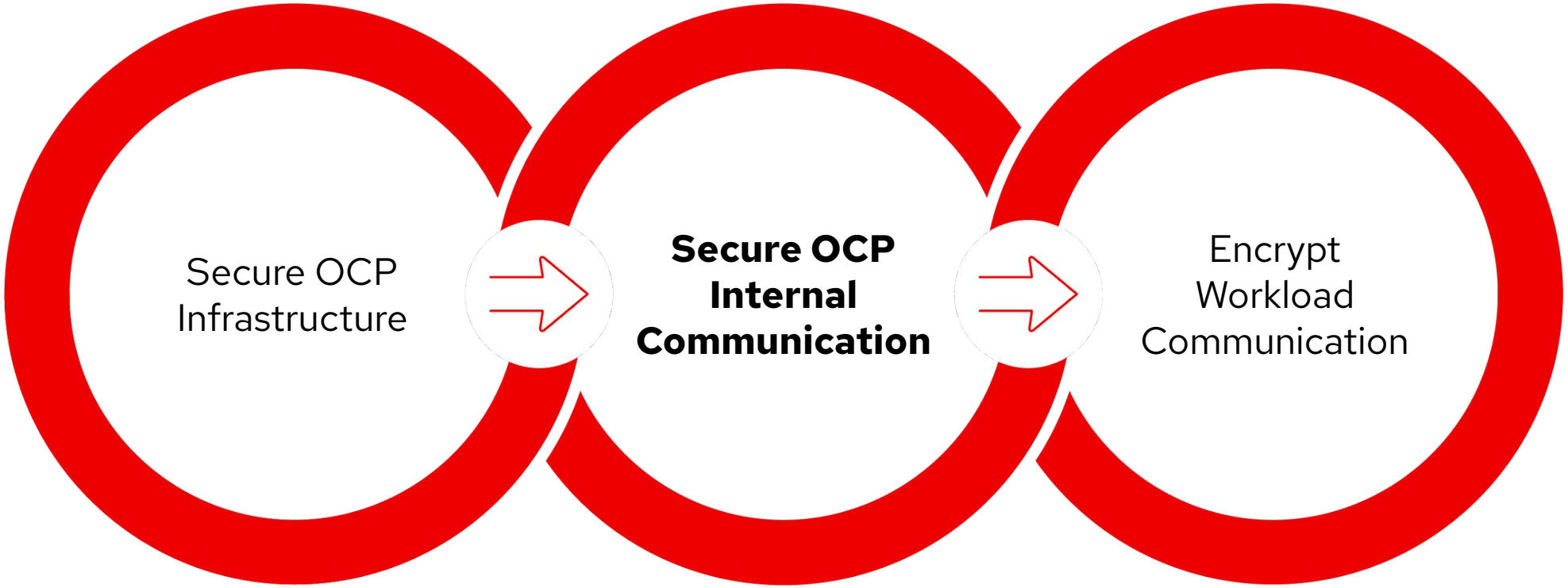
Note: products are not FIPS validated, only libraries.



*When built with RHEL base images

More about RHEL go and FIPS 140-2

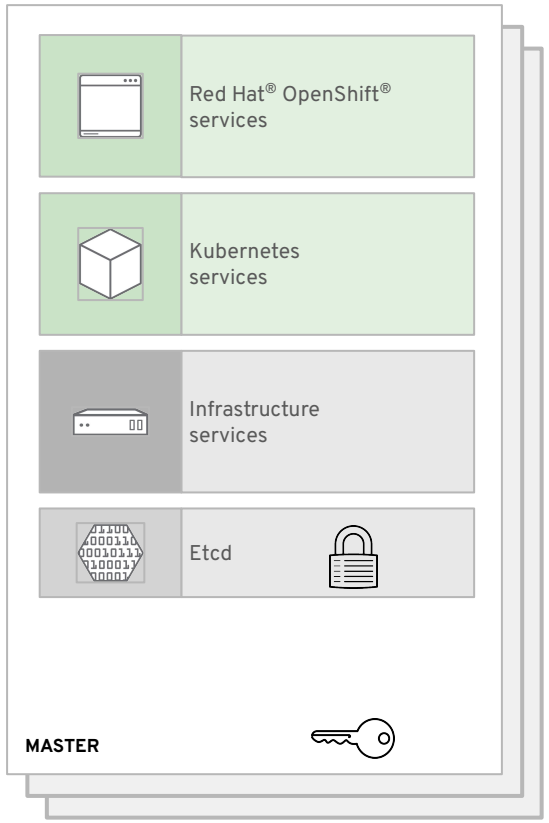
PKI in OpenShift



OpenShift 4 etcd Encryption

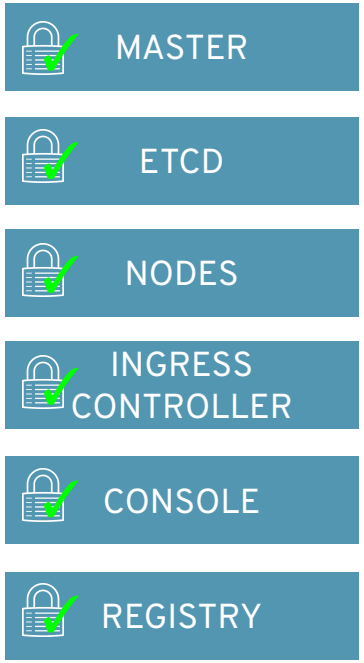
Encrypt secrets, config maps…

- 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.



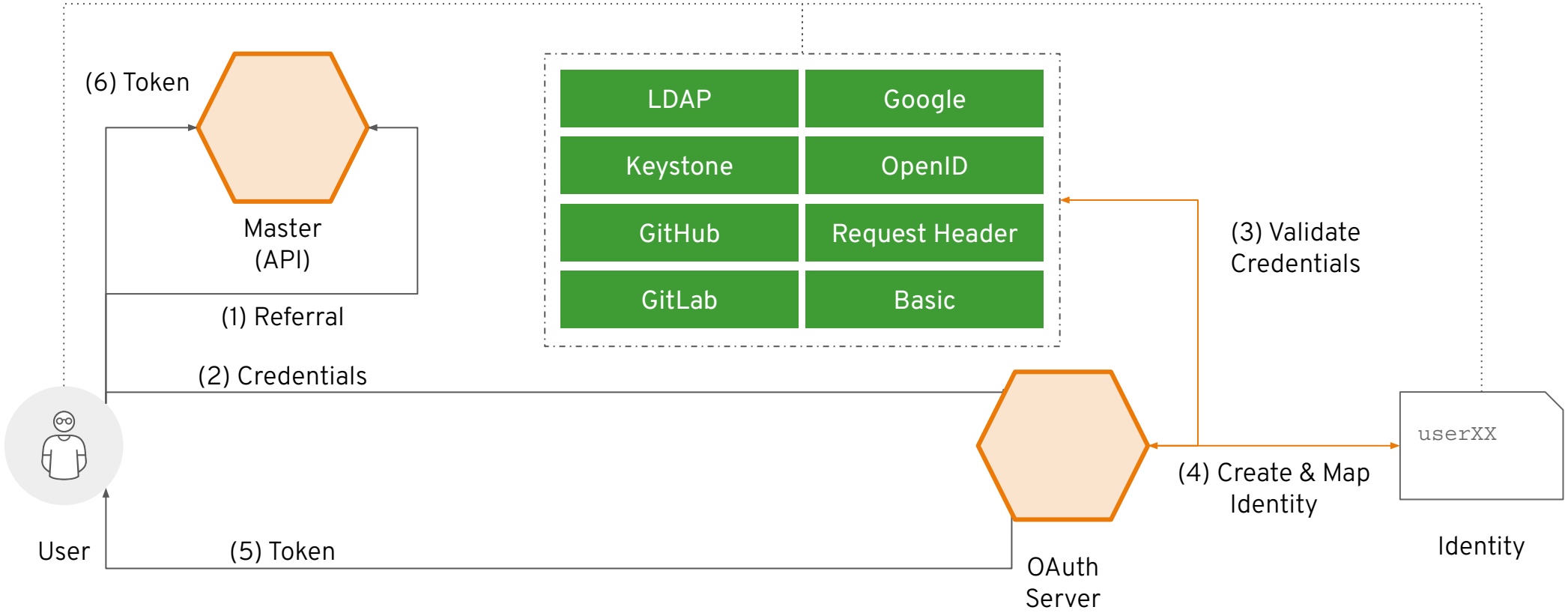
Certificates and Certificate Management

- 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



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

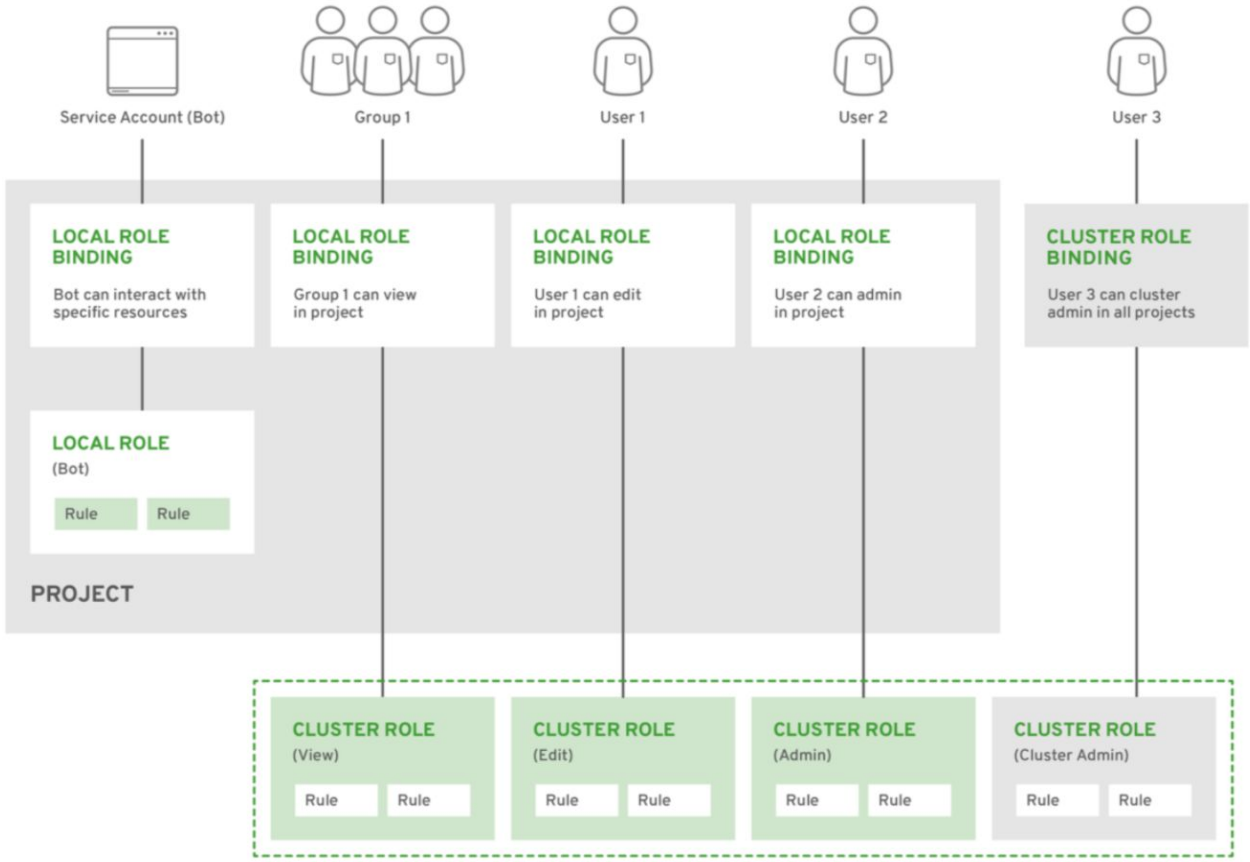
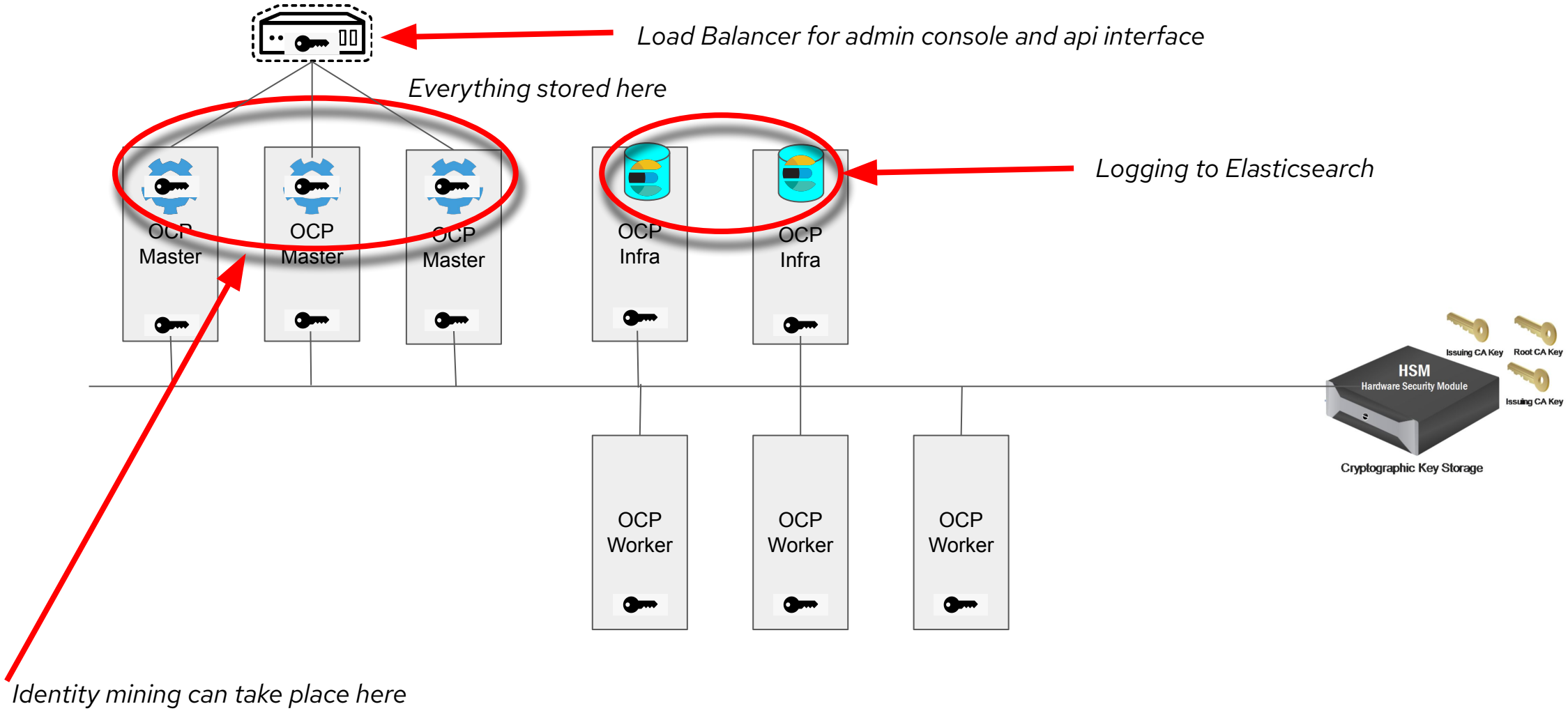


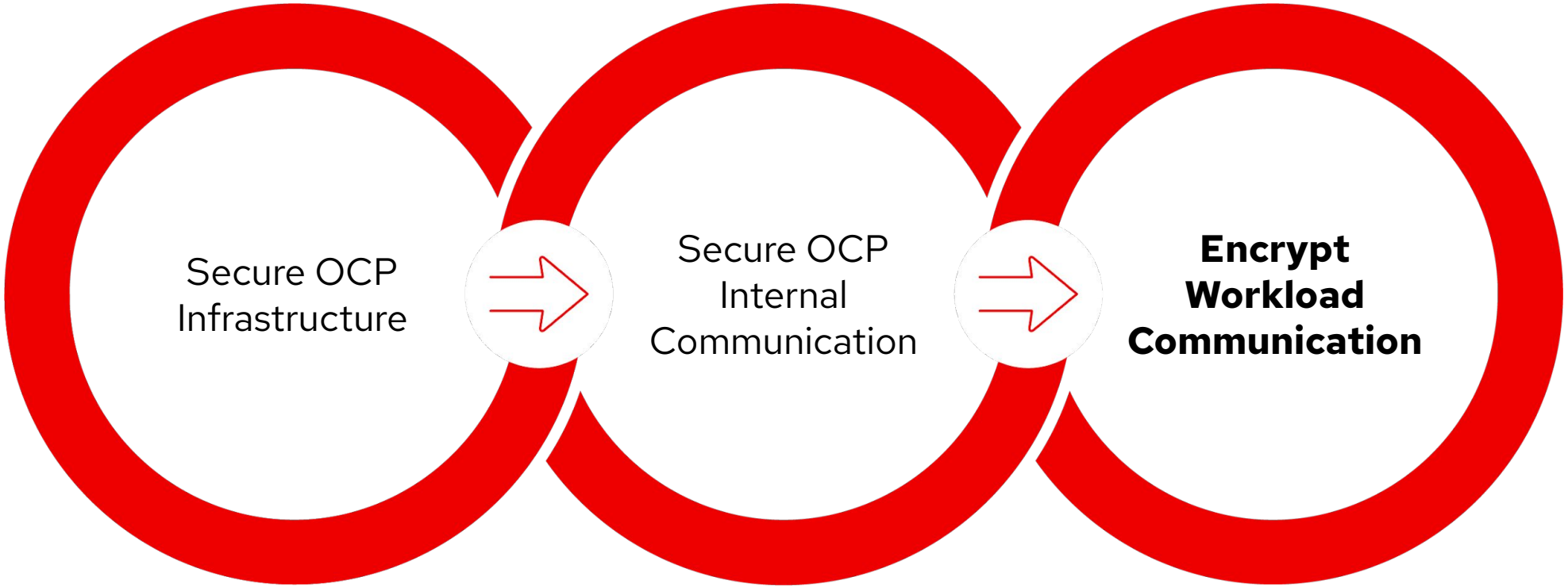
Figure 12 - Authorization Relationships

Red Hat

Identity Mining and SIAM Mining

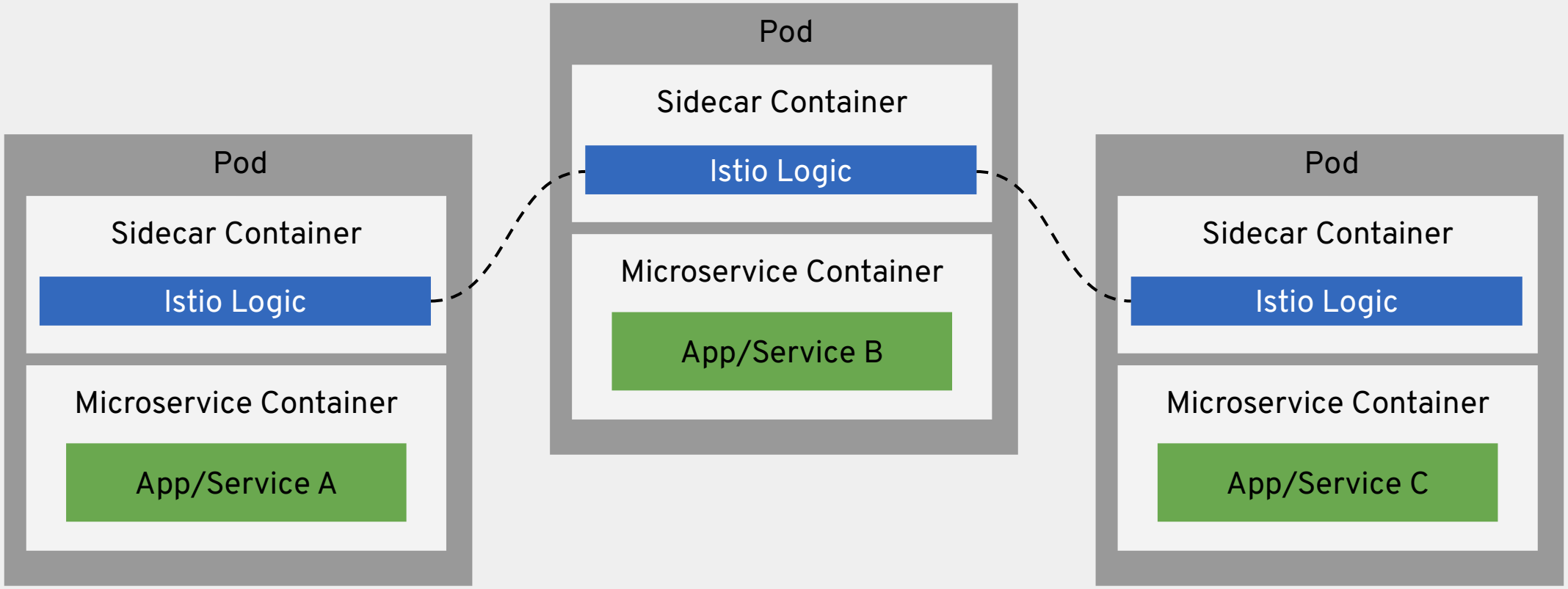


PKI in OpenShift



MICROSERVICES WITH ISTIO

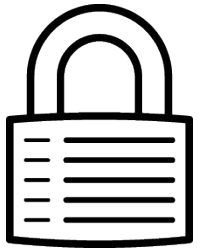
connect, manage, and secure microservices *transparently*



Red Hat

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)

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.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat