Intro to Confidential Containers

Presenter: Kautilya Tripathi

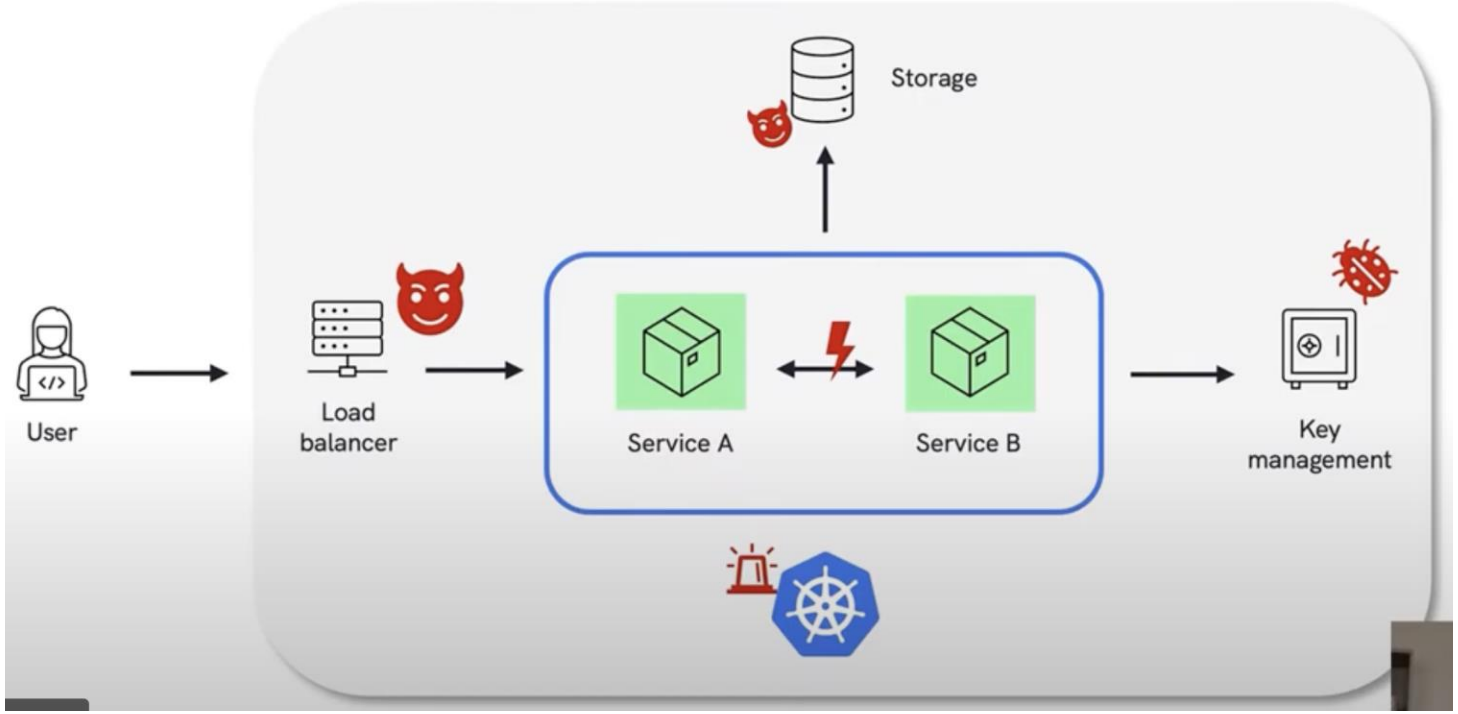
PPT: Suraj Deshmukh

About me

- Working at Microsoft under Azure team.
- Open Source Software ♡. knrt10
- Cloud Technolgies and Low level Linux
- Football(Hala Madrid!!!!(Why Casemiro why???))

State of Confidentiality

- Guarantee of data confidentiality?
- A rogue system admin peeks at the data of the customer?
- A host is compromised thus the data on it is compromised as well!



What is Confidential Computing?

Confidential Computing protects data in use by performing ***computation in a hardware-based Trusted Execution Environment****. These secure and isolated environments* ***prevent unauthorized access or modification of applications and data while in use****, thereby increasing the security assurances for organizations that manage sensitive and regulated data.*

- Data encryption at rest and in transit is a solved problem.
- CoCo implements data encryption in compute, where the memory is encrypted.
- Example applications:
    - Financial data
    - Health data
    - Personally Identifiable data

What is Confidential Containers?

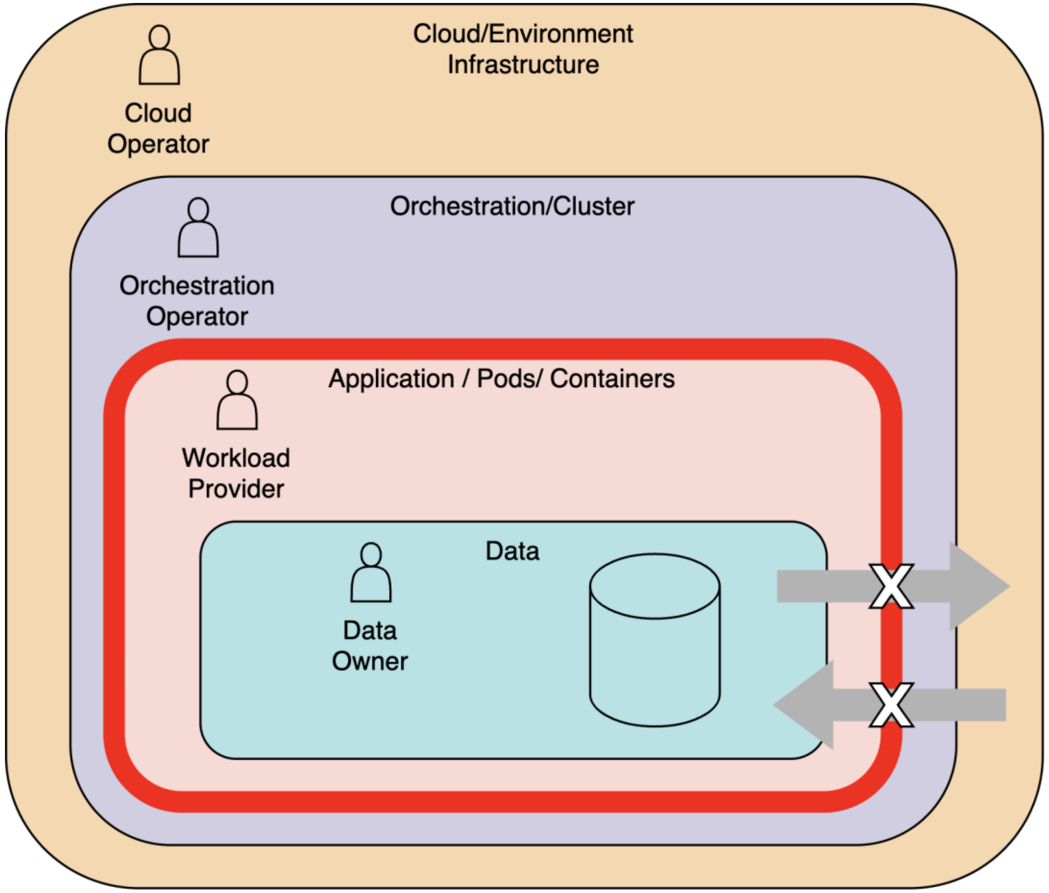
Implement Confidential Computing for the containers ecosystem.

Containers whose data, code, CPU state and memory is encrypted.

An environment that can be integrated with Kubernetes to leverage Confidential Computing.

Cloud provider is out of the Trusted Compute Base. Only user provided container is what user trusts.

Isolation vs Confidentiality



🟥 Confidential Computing Boundary

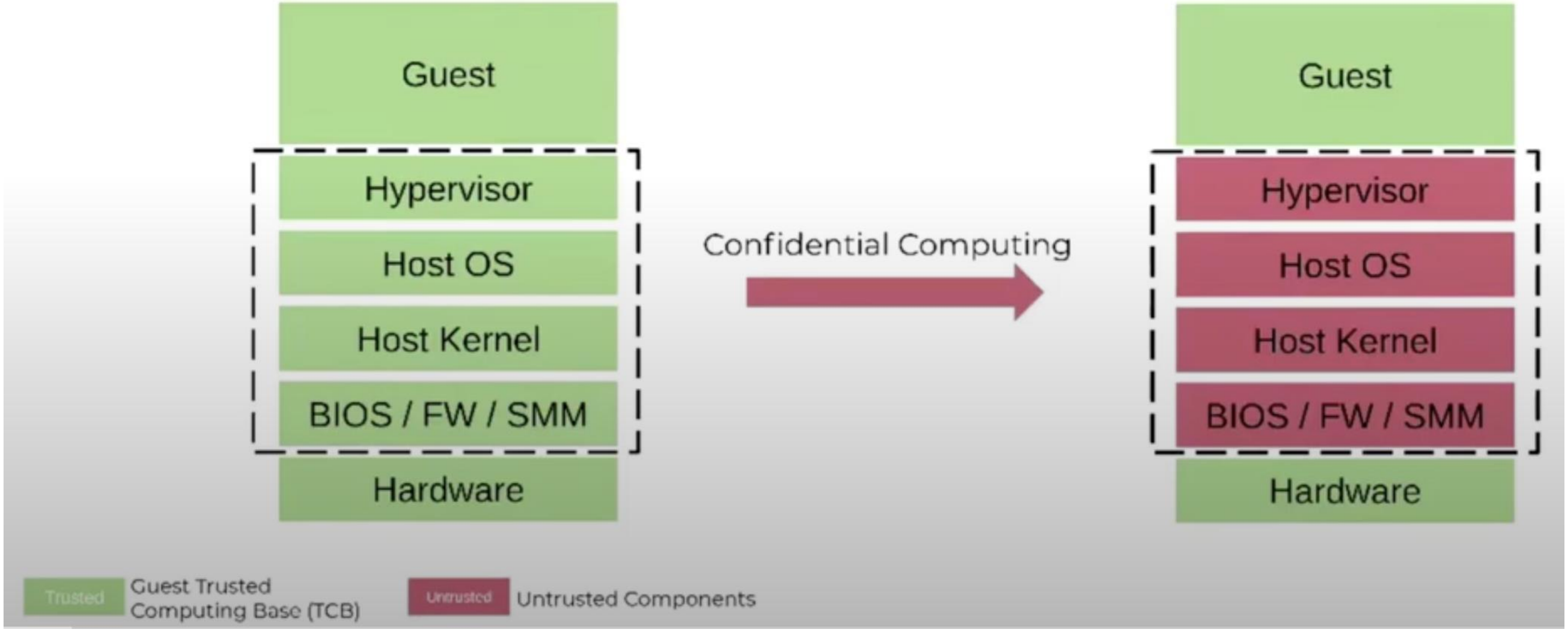
Isolation can protect the outer layers (Cloud and Cluster) from the workload code and containers

Confidentiality is the reverse and protects the code and data from the outer layers and personas.

How Kata-containers fit in this scenario?

- CoCo features implemented in processors are VM extensions.
- A VM is needed to take advantage of these features.
- To use confidential computing with Kubernetes we need a container runtime that runs as VM.
  - Enter Kata-containers!

TCB from a node perspective



Guest

Hypervisor

Host OS

Host Kernel

BIOS / FW / SMM

Hardware

Confidential Computing

Guest

Hypervisor

Host OS

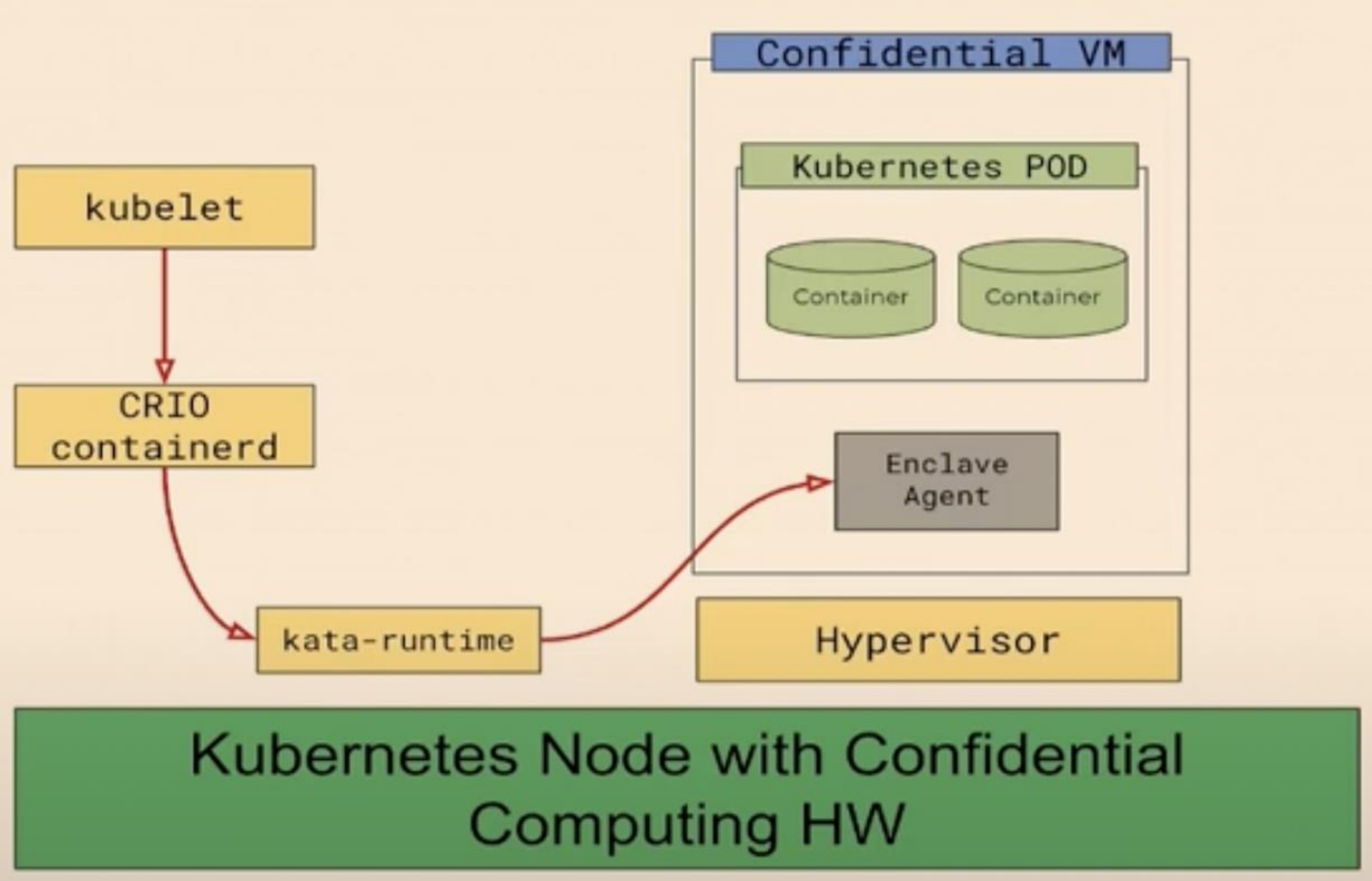
Host Kernel

BIOS / FW / SMM

Hardware

Trusted Guest Trusted Computing Base (TCB)

Untrusted Untrusted Components



kubelet

CRIO containerd

kata-runtime

Confidential VM

Kubernetes POD

Container

Container

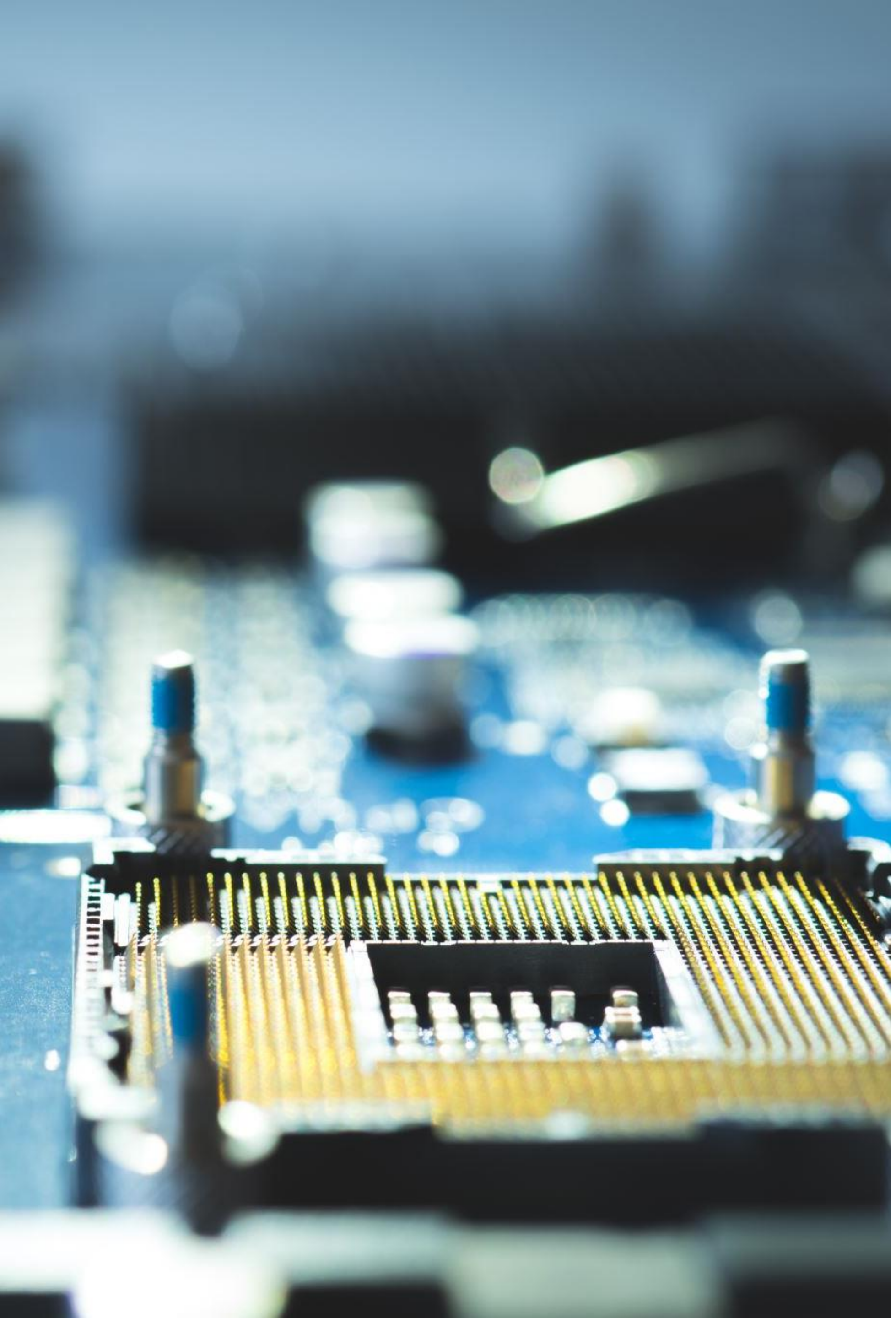
Enclave Agent

Hypervisor

Kubernetes Node with Confidential Computing HW

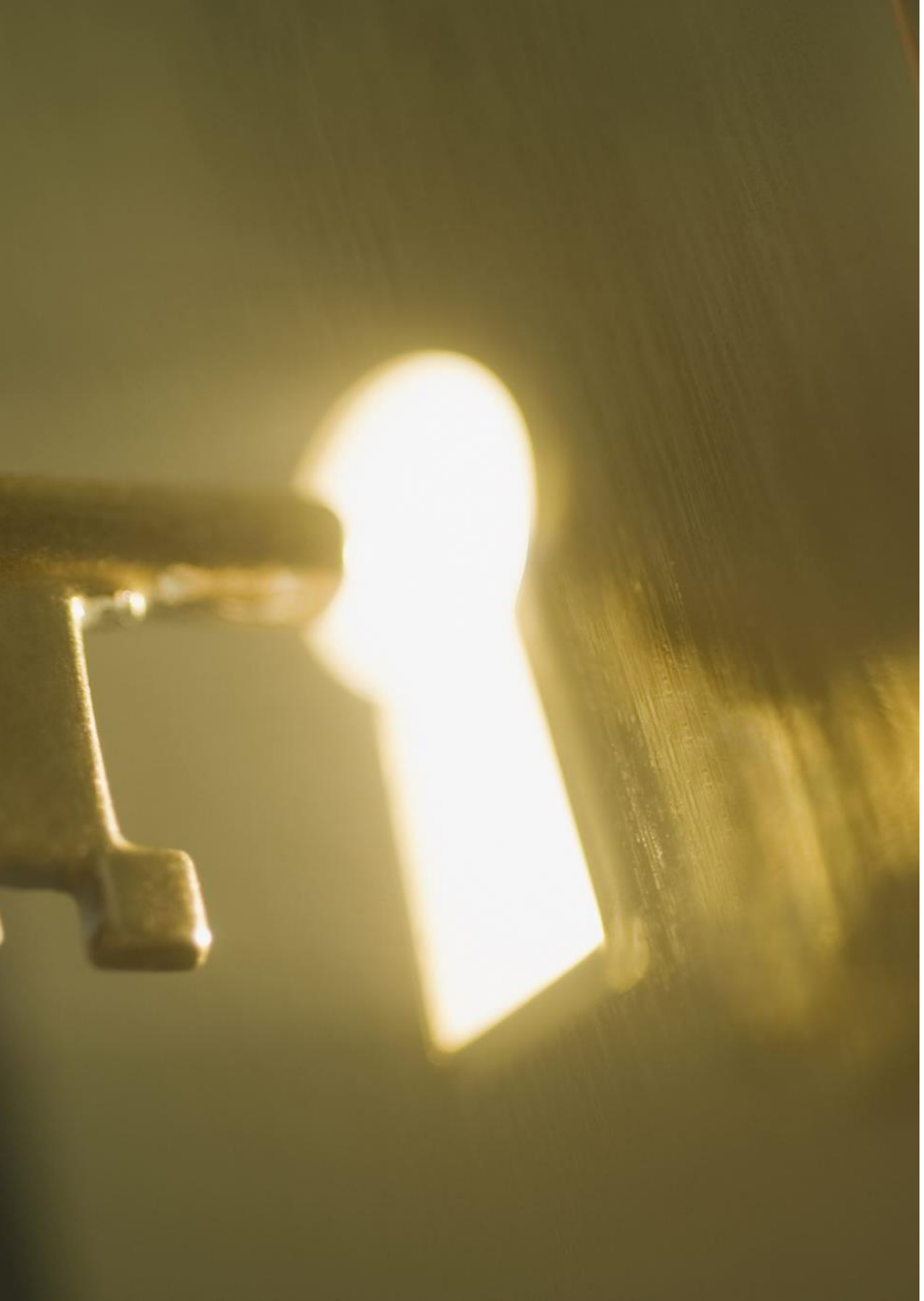
Enclave Stack

- Enclave stack is all the software needed to run a VM used for direct measured boot.
- Direct boot relies on OVMF(open VM firmware) package.
- It sets a piece of firmware binary to store hashes of:
  - Initrd
  - Kernel
  - Command line
- When QEMU boots a VM, it hashes each of these components and injects the hashes into the firmware binary. In a direct boot OVMF receives each of these components from the HV via the **fw_config** interface.
- HV is untrusted, but Firmware binary is measured.



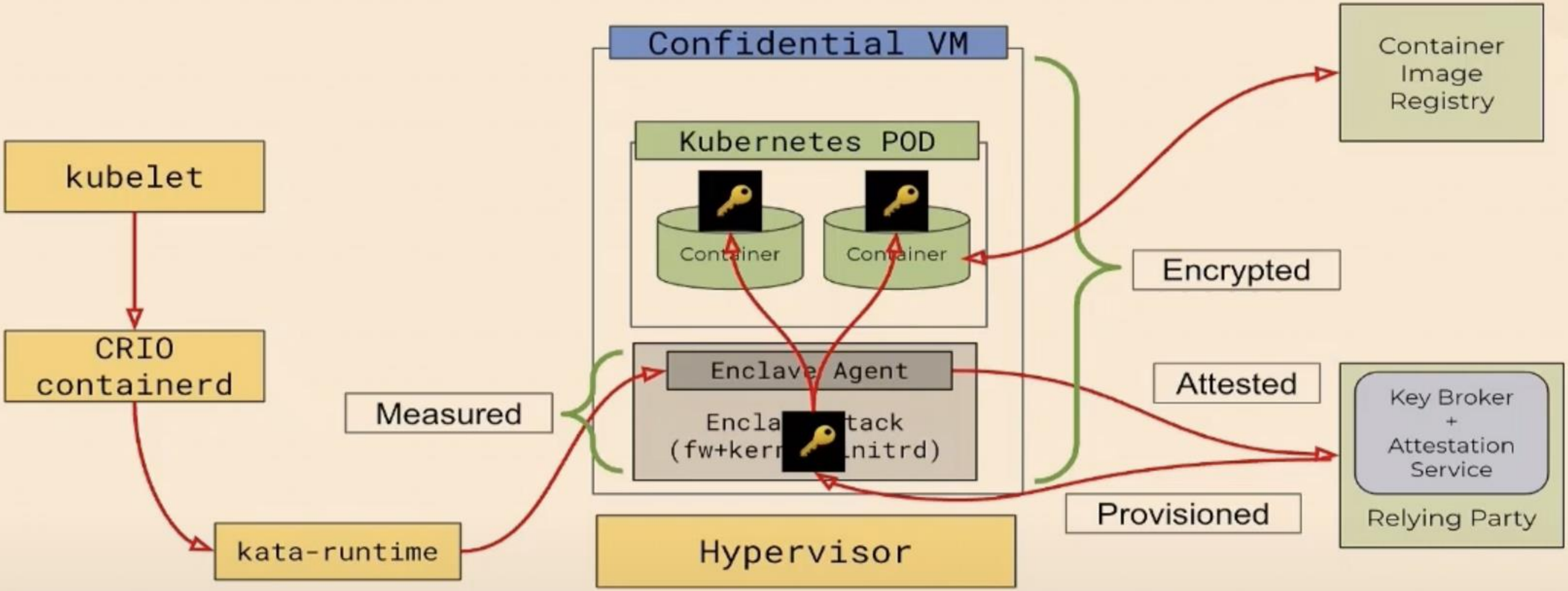
Attestation

- The enclave stack is measured by the processor and the measurements are sent to attestation server.
- Attestation server verifies if everything in the measurement is alright.
- The external server is controlled by the workload owner.
- The external server makes a decision according to the policies configured by the workload owner.



Post-Successful Attestation

- An encryption key is retrieved to decrypt the encrypted container image.



Kubernetes Node with Confidential Computing HW

Upstream developments

- Attestation Service
  - Source Code
  - Design
- Key Broker Service
  - Protocol
  - Source

Resources

- https://github.com/magowan/documentation/blob/TrustModel/TrustModel.md#personas
- https://confidentialcomputing.io/
- https://github.com/confidential-containers
- https://youtu.be/rdC2ETvzun0
- https://youtu.be/zTn9Xt1k1OA
- https://github.com/confidential-containers/documentation/blob/main/Overview.md
- https://docs.microsoft.com/en-us/azure/attestation/
- https://github.com/confidential-containers/community/issues/54
- https://docs.microsoft.com/en-in/azure/attestation/overview
- https://youtu.be/aGKn2OmrB1s
- https://youtu.be/BrSLOMYiJco
- RATS: https://www.ietf.org/archive/id/draft-ietf-rats-architecture-15.txt

Thank you 😊