
KubeCon
CloudNativeCon
Europe 2023
TiKV

The Next Episode in Workload Isolation: Confidential Containers

Jeremi Piotrowski (Microsoft)

About Me

KubeCon CloudNativeCon Europe 2023

- Hardware Security Modules
- Flatcar Container Linux
- Microsoft Azure
- Confidential Containers
- Email: jpiotrowski@microsoft.com

Confidential Containers (CoCo)

CONFIDENTIAL CONTAINERS

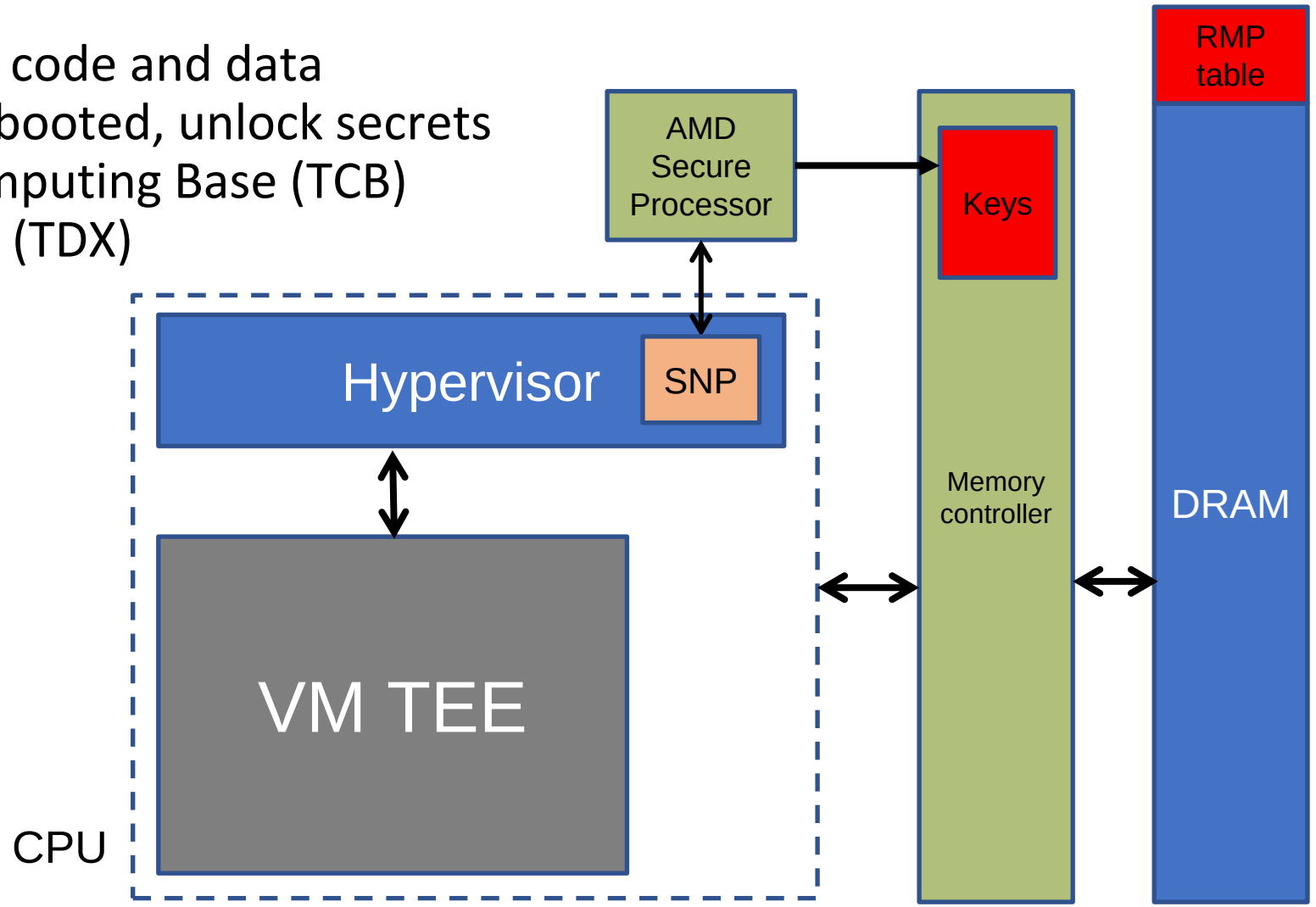
- CNCF sandbox project
- Built on top of Kata Containers
- Just released v0.5.0
- *Enable cloud native confidential computing by leveraging Trusted Execution Environments to protect containers and data.*
- https://github.com/confidential-containers/community

Related talks

- Confidential Containers Made Easy - Fabiano Fidencio, Intel && \
  Jens Freimann, Red Hat
  https://sched.co/1HyVQ
- Experience with “Hard Multi-Tenancy” in Kubernetes Using Kata Containers - Shuo Chen, Databricks
  https://sched.co/1Hydz

Properties of AMD SEV-SNP

- Secure Encrypted Virtualization – Secure Nested Paging
- VM based TEE
- Confidentiality and integrity – code and data
- Attestation - prove what was booted, unlock secrets
- Hypervisor out of Trusted Computing Base (TCB)
- Intel Trust Domain Extensions (TDX)
  – different solutions
  equivalent semantics



Secrets unlocked through attestation

Remote ATtestation procedureS
https://datatracker.ietf.org/doc/rfc9334/

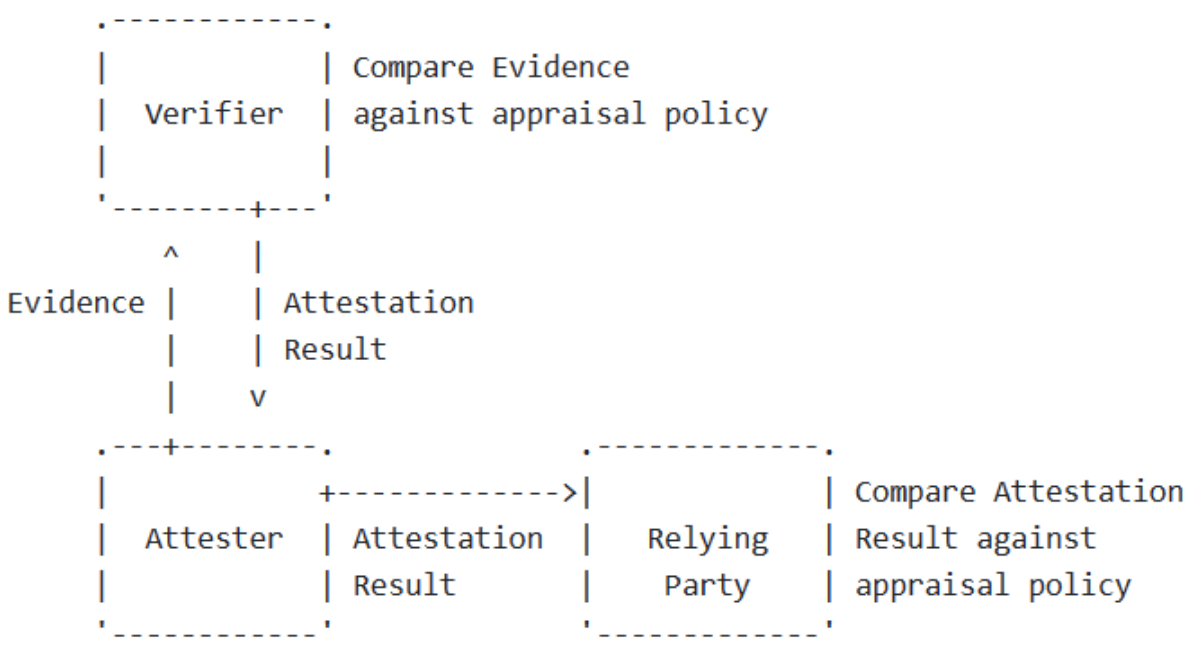


Figure 5: Passport Model

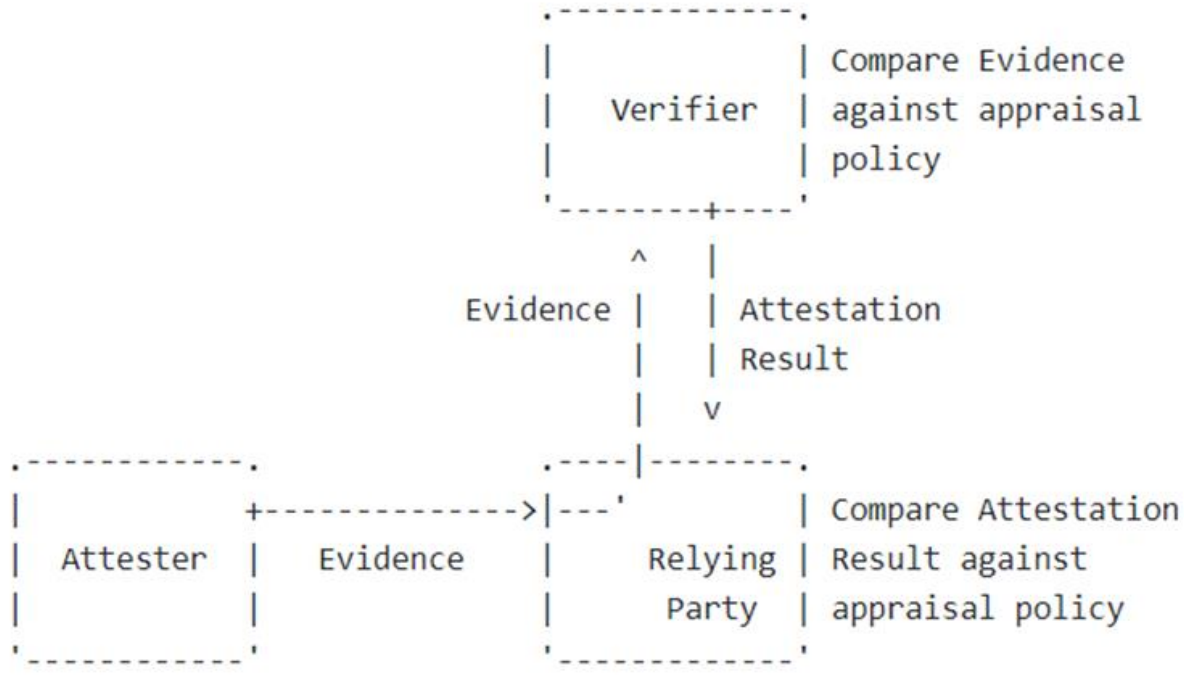
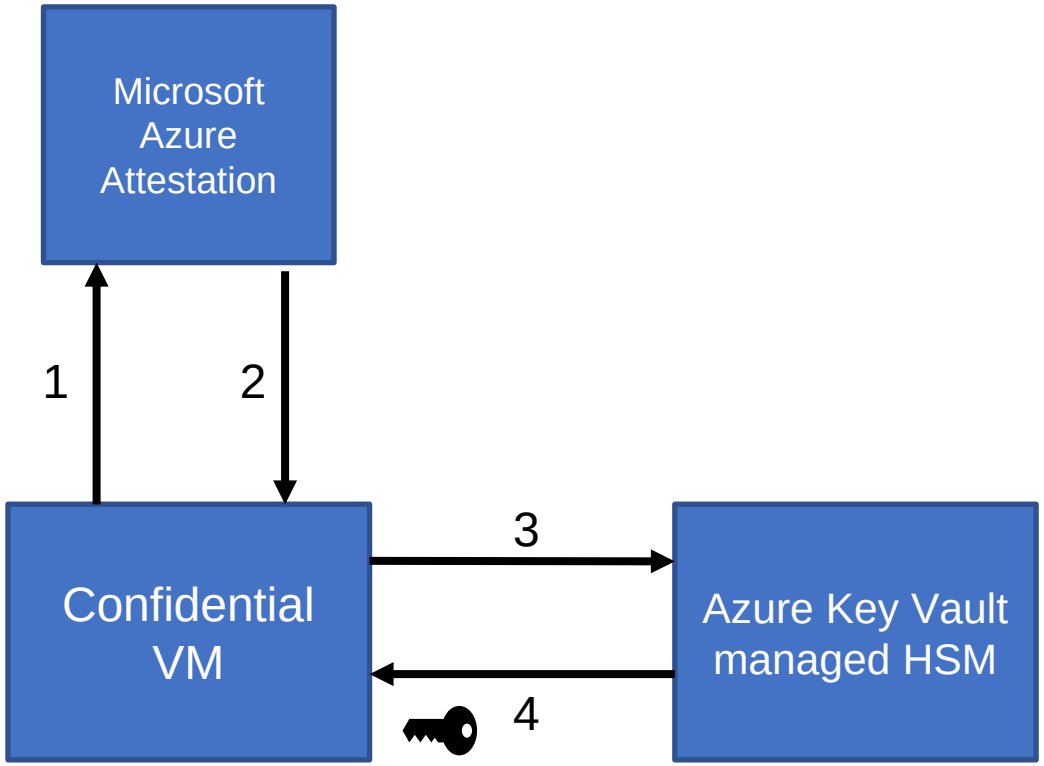
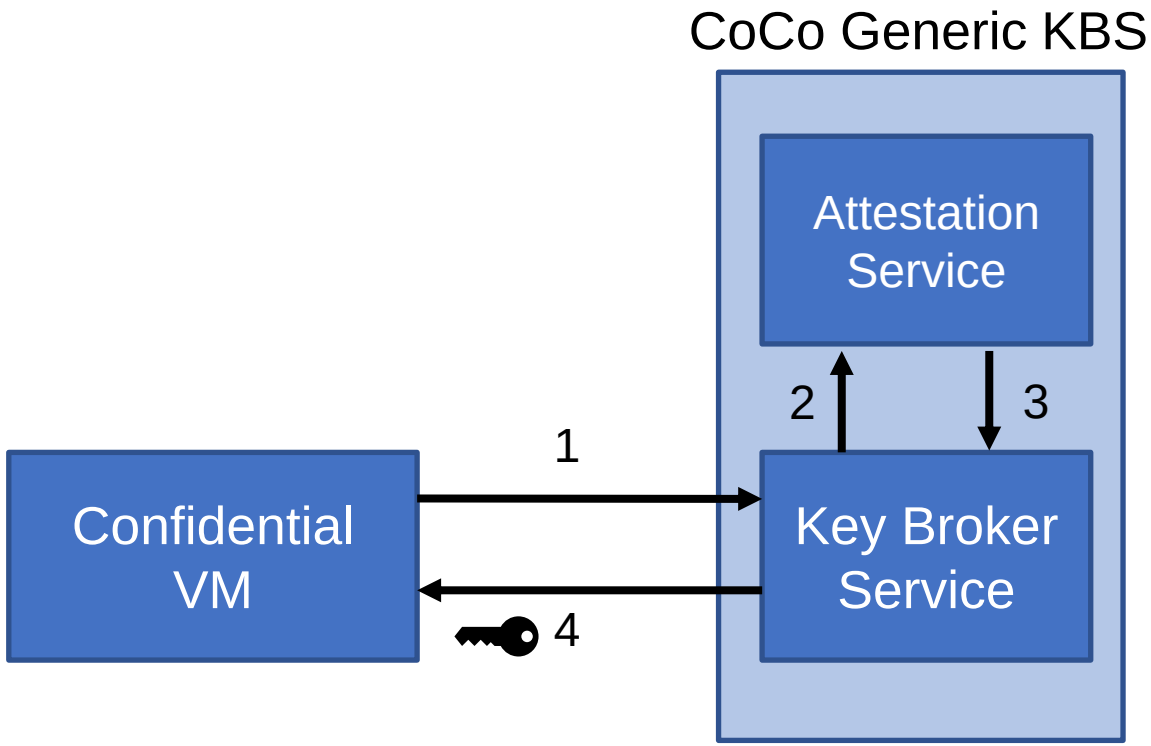


Figure 6: Background-Check Model

Secrets unlocked through attestation

Remote ATtestation procedureS
https://datatracker.ietf.org/doc/rfc9334/





SNP Attestation Report

1. Launch measurement – evidence of initial contents of TEE memory

```
Measurement:
5a 71 e4 ba 7e 0b 83 e4 4c 8e 85 31 30 a6 55 57
db 0a 77 82 cd b2 d9 06 c5 4b 0b f5 87 82 02 80
5a b1 59 bf e0 cf 7d 57 49 aa 6f 62 b7 09 45 08
```

SNP Attestation Report

2. Host data – used to tie data to attestation before launch

```
Host Data:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Friday 11:00
Microsoft booth

SNP Attestation Report

KubeCon CloudNativeCon Europe 2023

3. Report data – used to tie data to attestation at runtime

```
Report Data:
30 3d 9c 72 9a ef 00 9c cb d7 09 91 fd a6 15 67
47 27 06 b1 b3 cc 45 b9 67 13 09 fe dc 74 cf d5
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

SNP Attestation Report

KubeCon CloudNativeCon Europe 2023

4. Signed by AMD Secure Processor, certificate chains to AMD

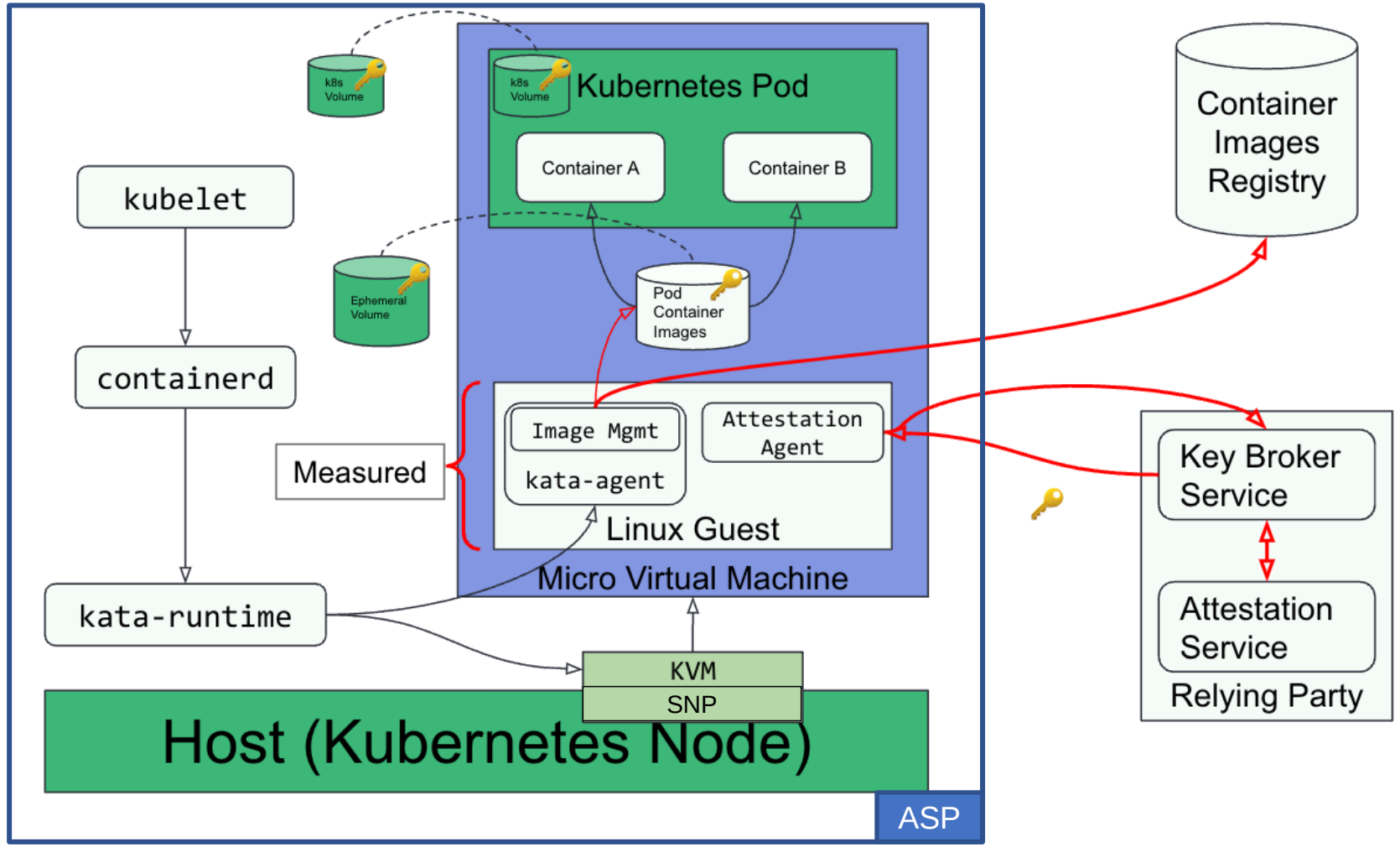
```
Signature:
  R:
02 73 25 bd 0a f9 1a 81 9a 86 ee 95 9d 23 6b c4
0d 4e 94 3c 7b e7 ca ae 5d b8 60 fe 70 da 0f a2
f0 22 f6 7a 51 44 de 31 fc 93 39 f6 5e 4e 78 59
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

  S:
c9 07 6c 31 61 7e 50 0d 5e 6a 11 00 e9 86 50 94
f3 7c b5 33 db 35 22 dd 0b a2 72 5a 2a 15 d6 06
8f 1b 5a 7c 0a cb fa 8b 42 3b 2c 68 18 b1 1f 0c
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
```

Launch measurement

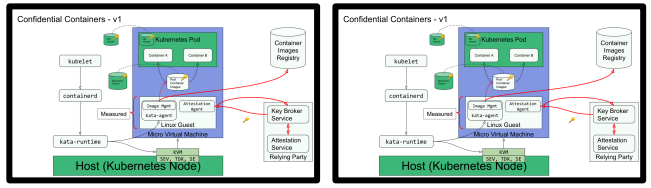
- Every page loaded into TEE address space is encrypted by the AMD Secure Processor and measured into the launch measurement
- LM = HASH(old LM || #ADDR || HASH(DATA))
- Special pages: VM Save Area (registers)

CoCo Bare metal

Confidential Containers - v1



CoCo Nested



Confidential Containers - v1

kubelet

containerd

kata-runtime

Measured

k8s Volume

Ephemeral Volume

Kubernetes Pod

Container A

Container B

Pod Container Images

Image Mgmt

kata-agent

Attestation Agent

Linux Guest

Micro Virtual Machine

KVM/Hyper-V

SNP

VM (Kubernetes Node)

ASP

Container Images Registry

Key Broker Service

Attestation Service

Relying Party

Hyper-V

SNP

ASP

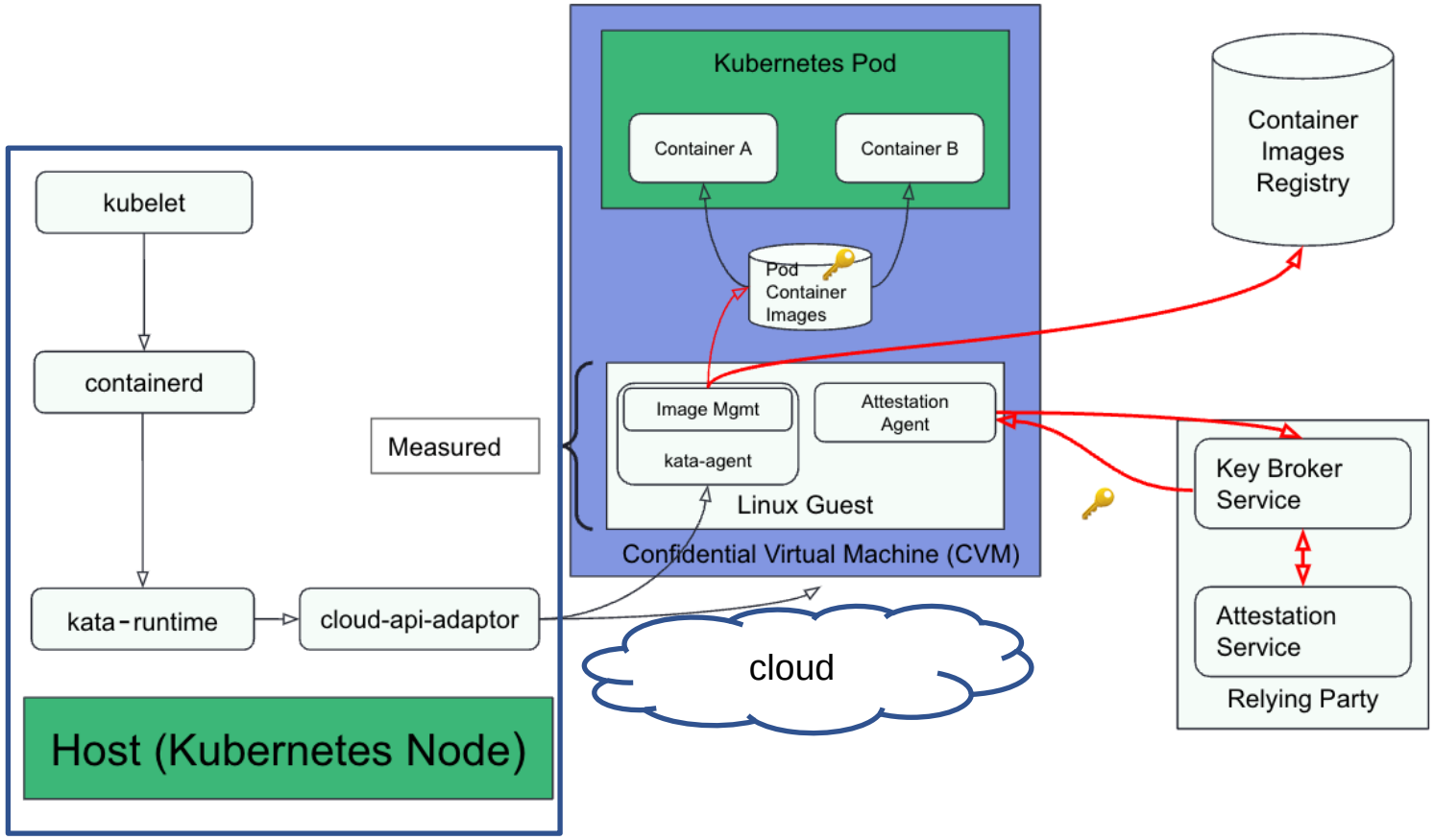
aka.ms/cocoaks

CoCo Peer Pods

KubeCon CloudNativeCon Europe 2023

Thursday 14:00
Red Hat booth

Confidential Containers - v1



https://www.redhat.com/en/blog/deploying-confidential-containers-public-cloud

Imagine a world…

where you…

- build your software…
- generate a signed Software Bill of Materials (SBOM) that includes the expected measurement…
- run your workload in a TEE…
- request secrets, providing an attestation report…
- the verifier matches your measurement to your SBOM
- and releases secrets based on SBOM contents

Summary

- **Foundation of multi-tenant/zero trust architectures**
- CoCo integrates confidential computing features with containers and Kubernetes
- Supports multiple TEE: Intel SGX/TDX, AMD SEV/SNP, IBM SE
- Spectrum of deployment options: bare metal, nested VM, CVM/peer-pod

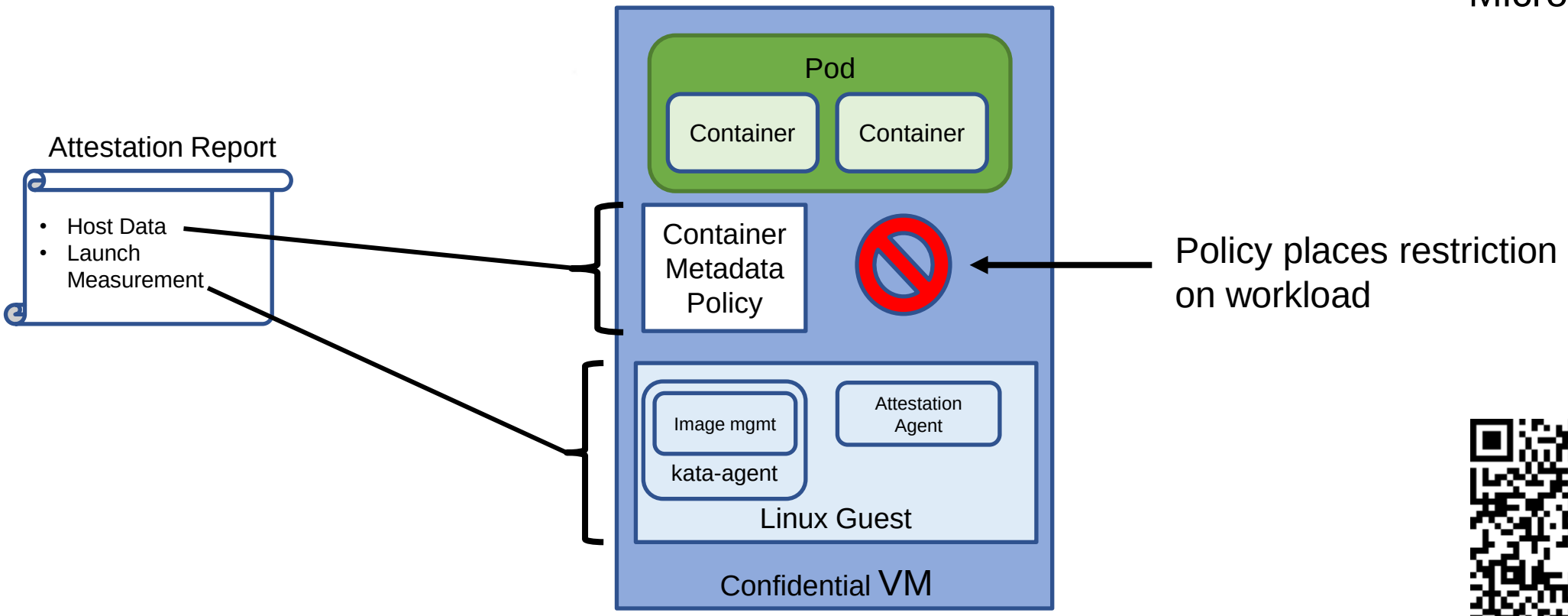
https://www.redhat.com/en/blog/understanding-confidential-containers-attestation-flow

KubeCon | CloudNativeCon
Europe 2023

Please scan the QR Code above
to leave feedback on this session

Container Metadata Validation

Friday 11:00
Microsoft booth



https://docs.google.com/document/d/1E3GLCzNgrcigUlgWAZYlgqNTdVwiMwCRTJ0QnJhLZGA/edit#heading=h.bf7ezhzz5b