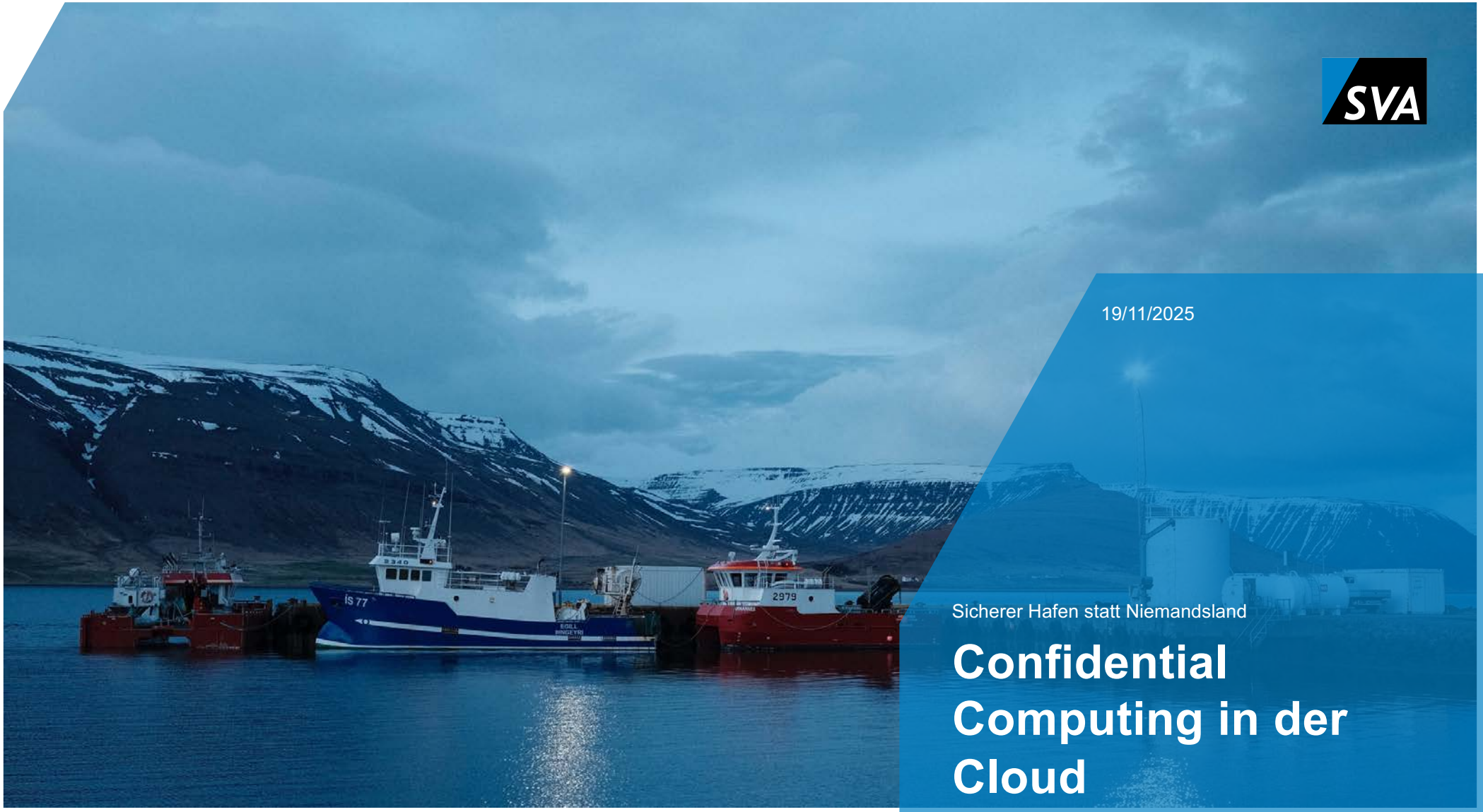


SVA

19/11/2025

Sicherer Hafen statt Niemandsland

Confidential Computing in der Cloud

Agenda

1. Introduction & Motivation
2. Confidential Computing Basics
3. Confidential Containers with Red Hat OpenShift
4. Use cases & Lessons learned

Whoami

Moritz Meid

Solution Architect

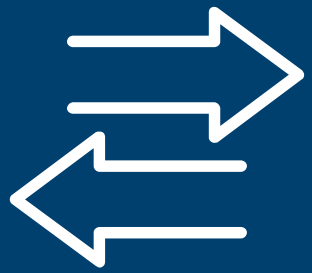
Niklas Werker

Technical Lead


/ Mit Confidential Computing
Kein Auflaufen, trotz schwieriger Gewässer
„Financial entities shall design, procure and implement ICT security strategies, policies, procedures, protocols and tools that aim at, in particular, ensuring the resilience, continuity and availability of ICT systems, and maintaining high standards of security, confidentiality and integrity of data, whether at rest, in use or in transit.“
- DORA Chapter II Section II Article 8 Paragraph 2

Grundlagen Confidential Computing

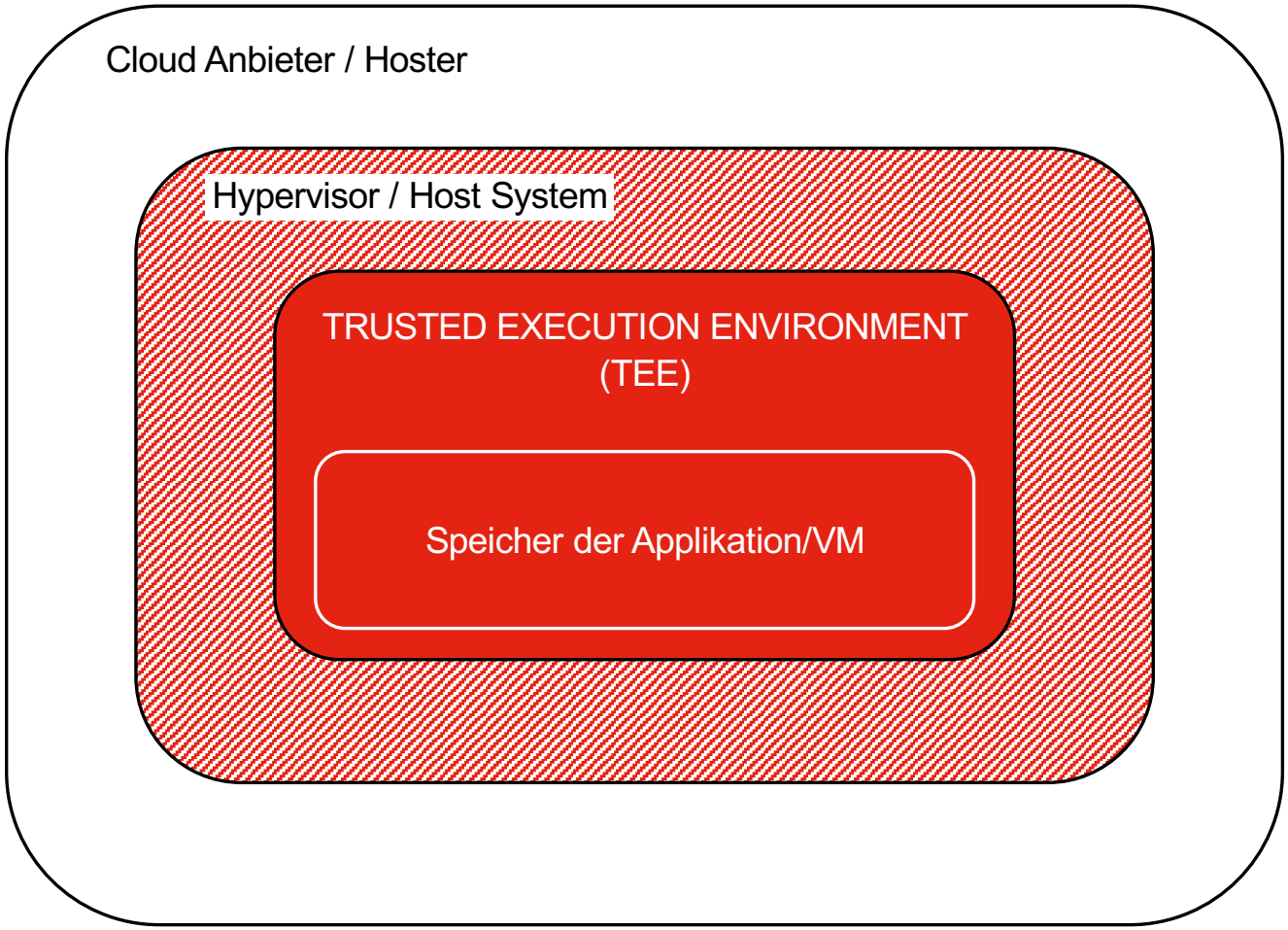
Data at rest



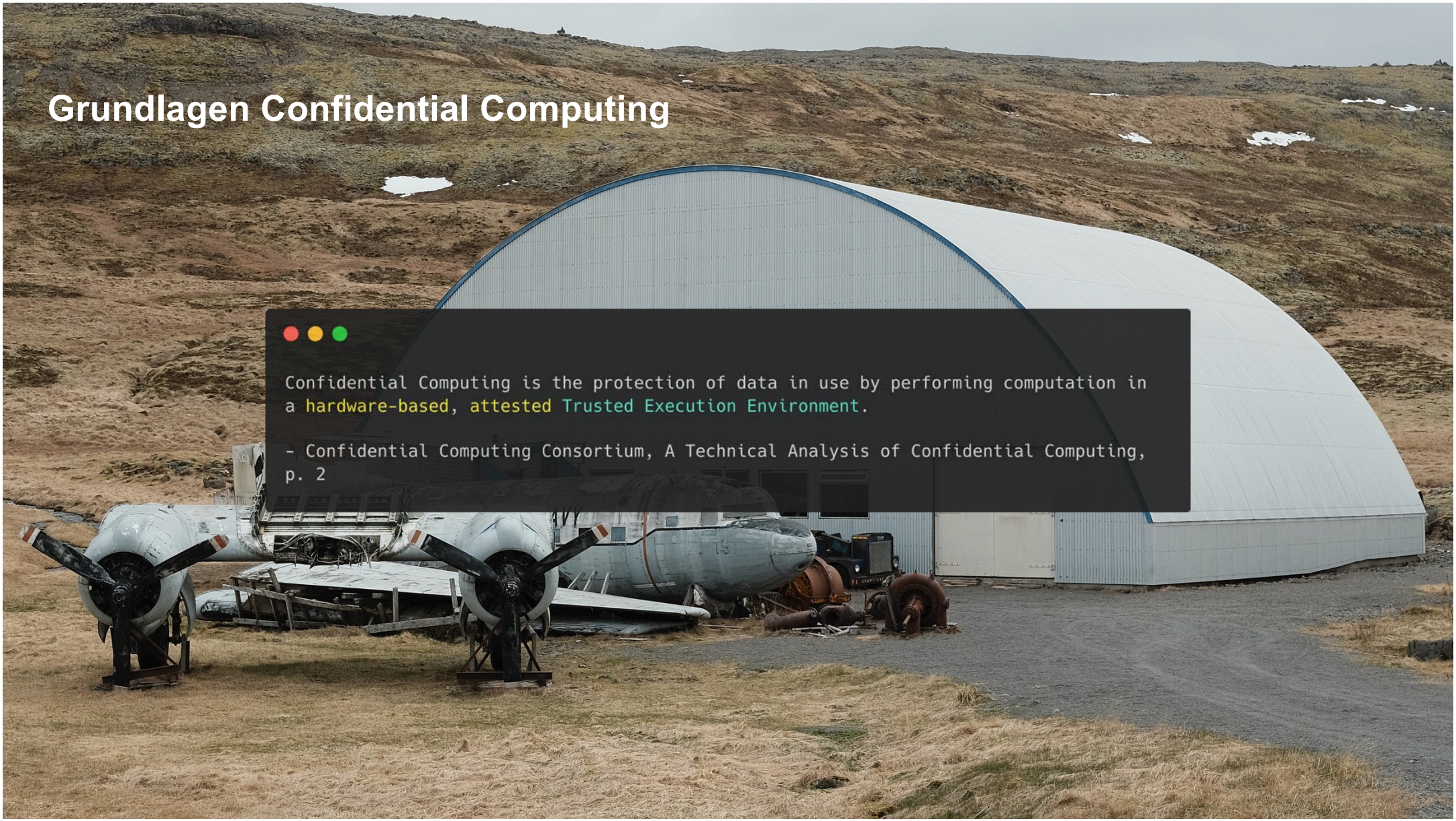
Data in transit

Data in use

Data in Use


Cloud Anbieter / Hoster
Hypervisor / Host System
TRUSTED EXECUTION ENVIRONMENT
(TEE)
Speicher der Applikation/VM

Grundlagen Confidential Computing



Kernkonzepte Confidential Computing

Integrität

Trust

Remote Attestation

Warum ist Integrität wichtig?

- Läuft mein Code in der intendierten Konfiguration?
- Ist meine Applikation oder Umgebung ggfs. kompromittiert?

= Nur wenn wir wissen, *was wo* ausgeführt wird, können wir es schützen

- **Measurements**: Vermessung von Systemkomponenten mit kryptografischen Hash-Funktionen

```
$ curl -LO "https://dl.k8s.io/release/$(curl -L -s
https://dl.k8s.io/release/stable.txt)/bin/linux/amd64/kubectl"
$ curl -LO "https://dl.k8s.io/release/$(curl -L -s
https://dl.k8s.io/release/stable.txt)/bin/linux/amd64/kubectl.sha256"
$ echo "$(cat kubectl.sha256)  kubectl" | sha256sum --check
$ kubectl: OK
```


src: Magnus Kulke

Measurement Chain: Der Nachweis der Integrität

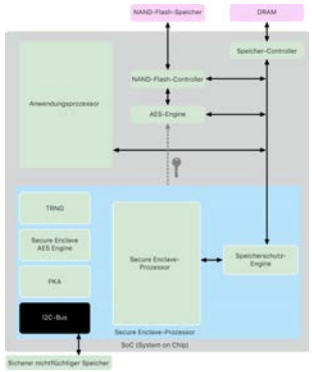
- Jede Komponente des Runtime Environments wird beim Initialisieren kryptografisch gehasht.

- Die resultierenden Hashes werden in TEE/TPM-geschützten Registern gespeichert (z.b. Platform Configuration Registers – **PCRs**)

Wie entsteht Trust?

- Grundlegende Prämisse: Ein System ist zunächst nicht als vertrauenswürdig zu betrachten
- Vertrauen kann nur durch eine **unabhängige, externe Instanz** hergestellt werden

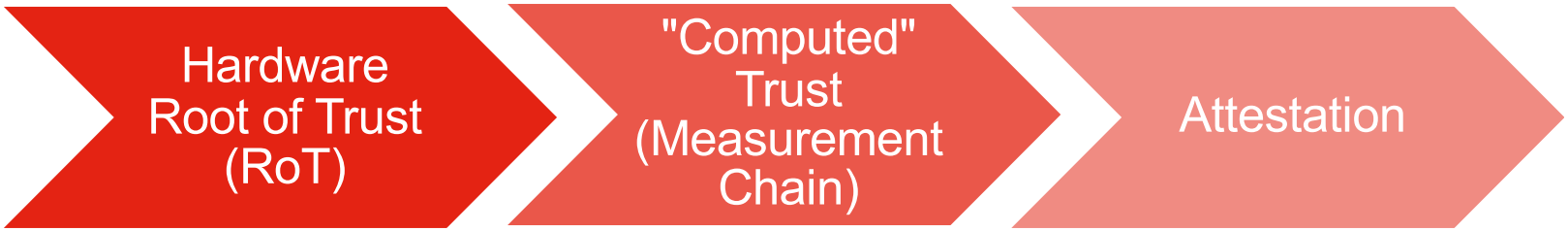
Thales PCIe HSM



Apple Silicon Secure Enclave Processor

GIGABYTE TPM

Wie entsteht Trust?



Ablauf der Remote Attestation

a) Verschlüsselte Inhalte werden dem TEE bereitgestellt.

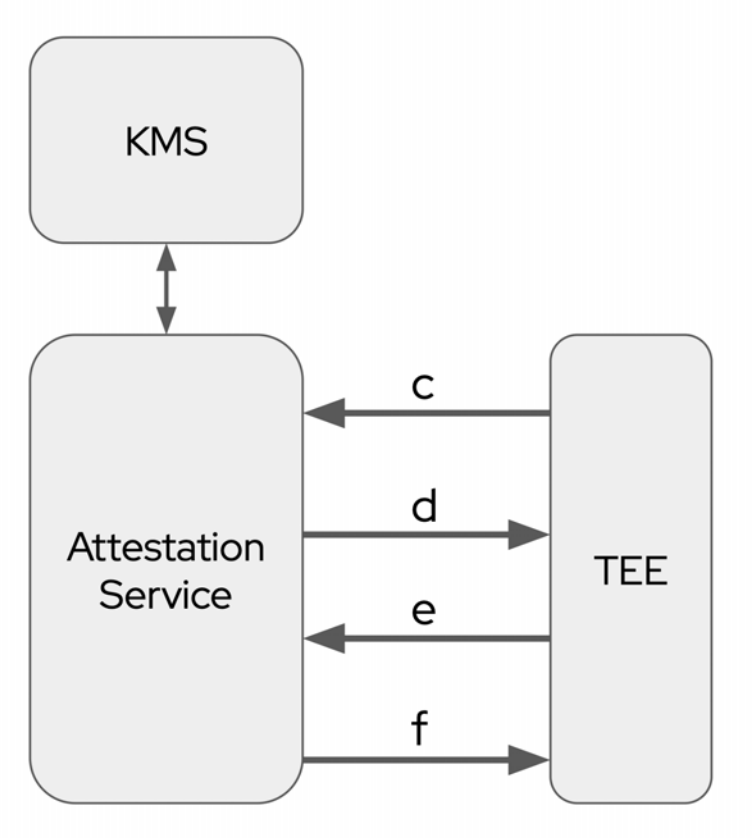
b) Eine Anwendung braucht Zugriff auf diese Inhalte

c) Das TEE fordert ein Schlüssel an, um die Inhalte zu entschlüsseln

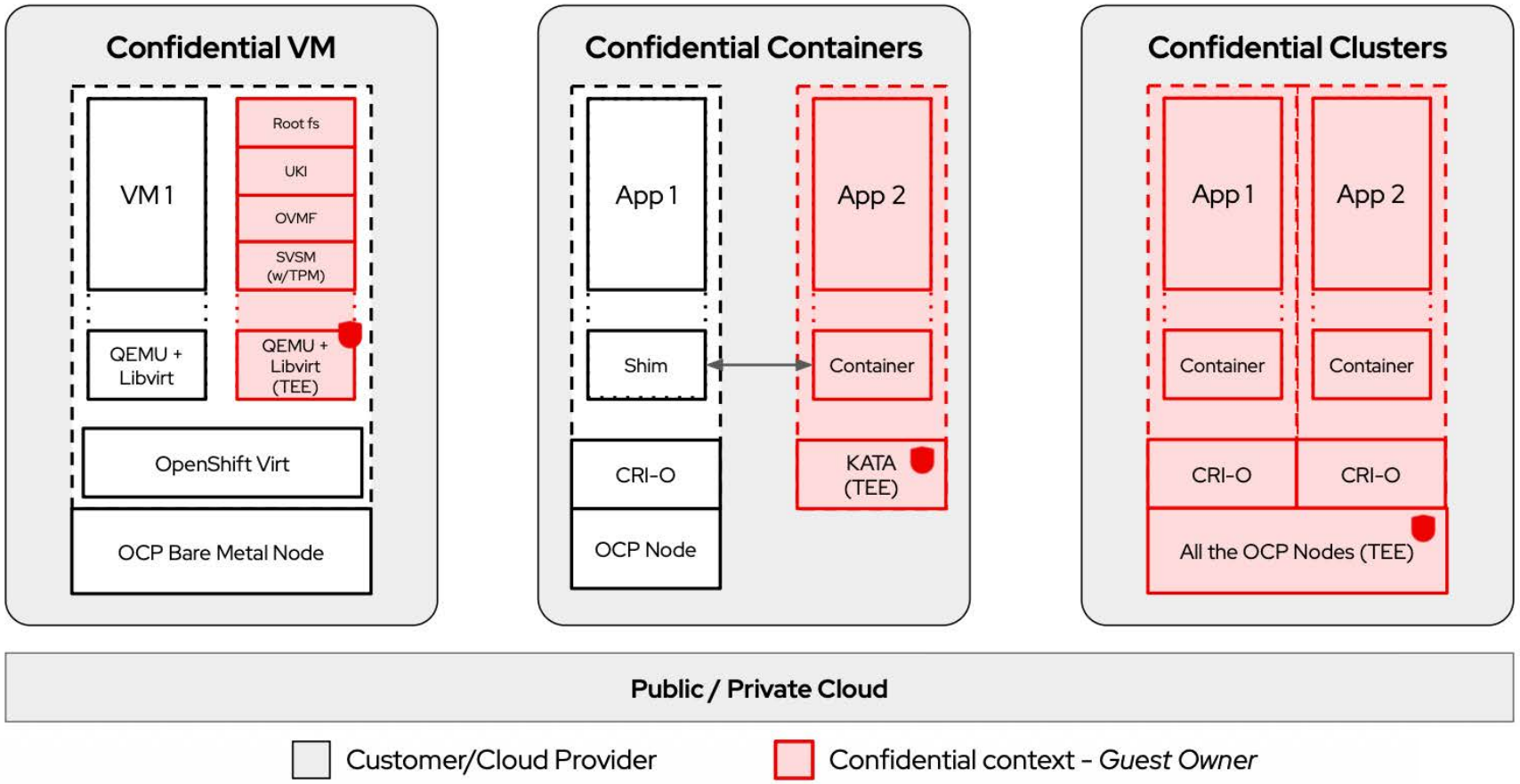
d) Der Attestation-Service fordert Nachweise an, dass die Umgebung tatsächlich „confidential“ ist.

e) Das TEE liefert eine signierte Measurement-Chain, welche auf Hardware-Ebene verifiziert werden kann.

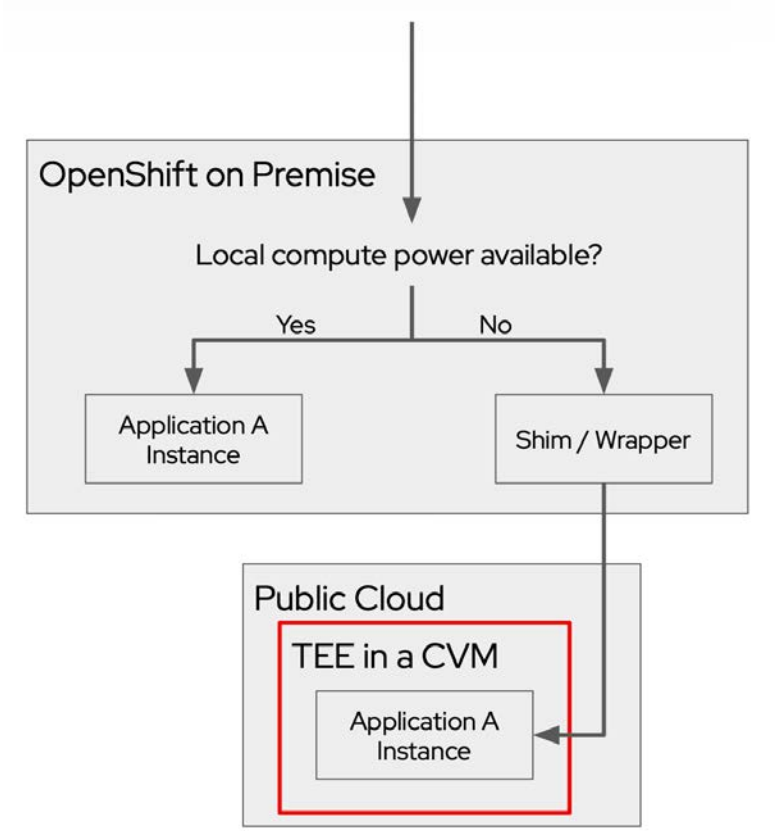
f) Der Attestation-Service prüft die Measurements und gibt bei erfolgreicher Prüfung den Key aus dem KMS an das TEE weiter.

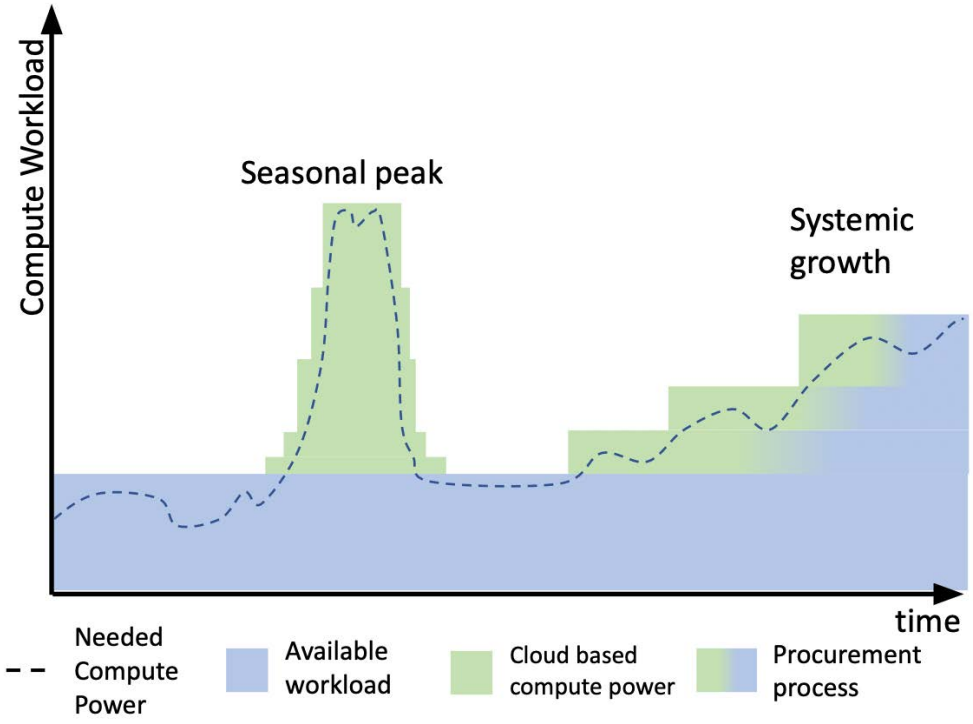


Red Hat Lösungsansätze

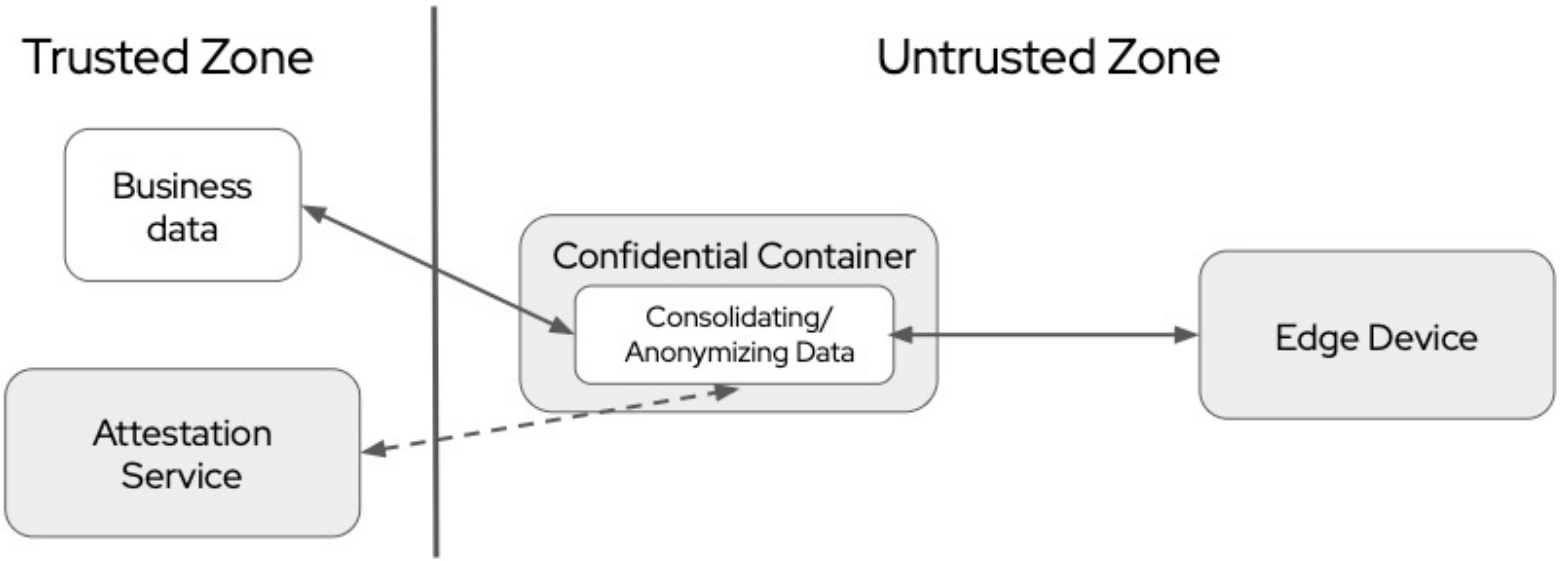


Usecase: Cloud Burst

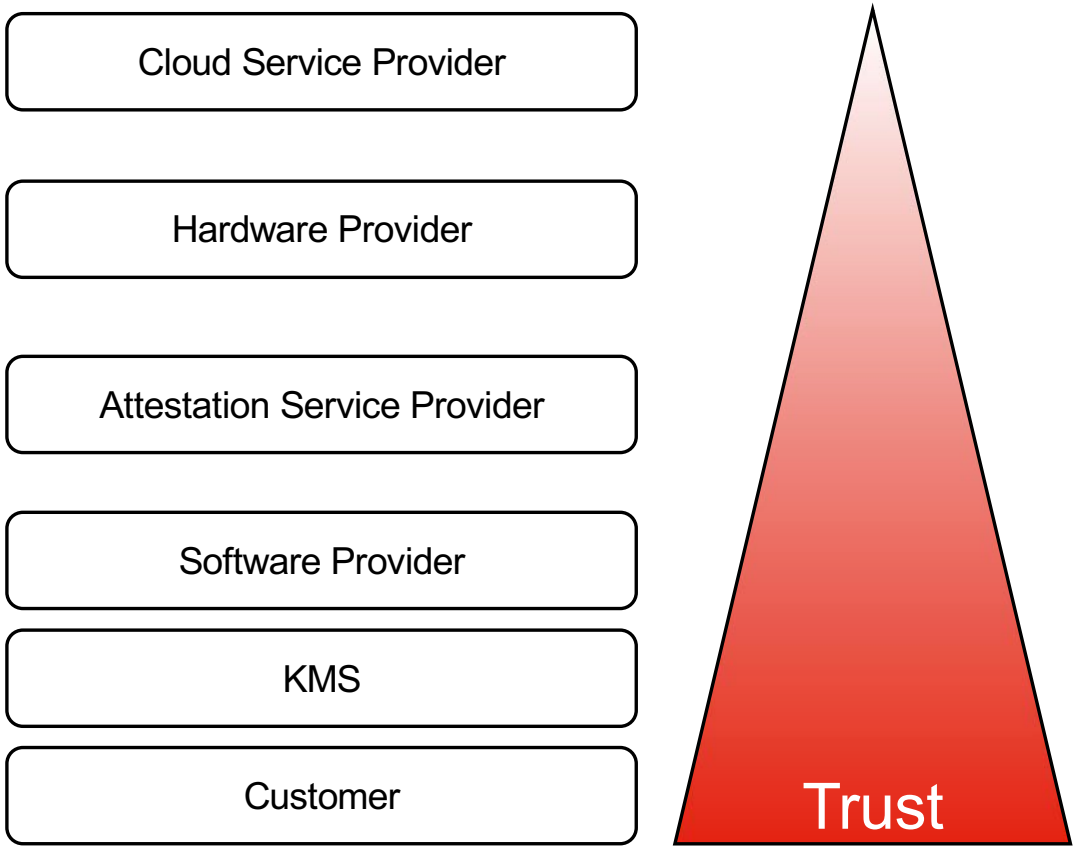




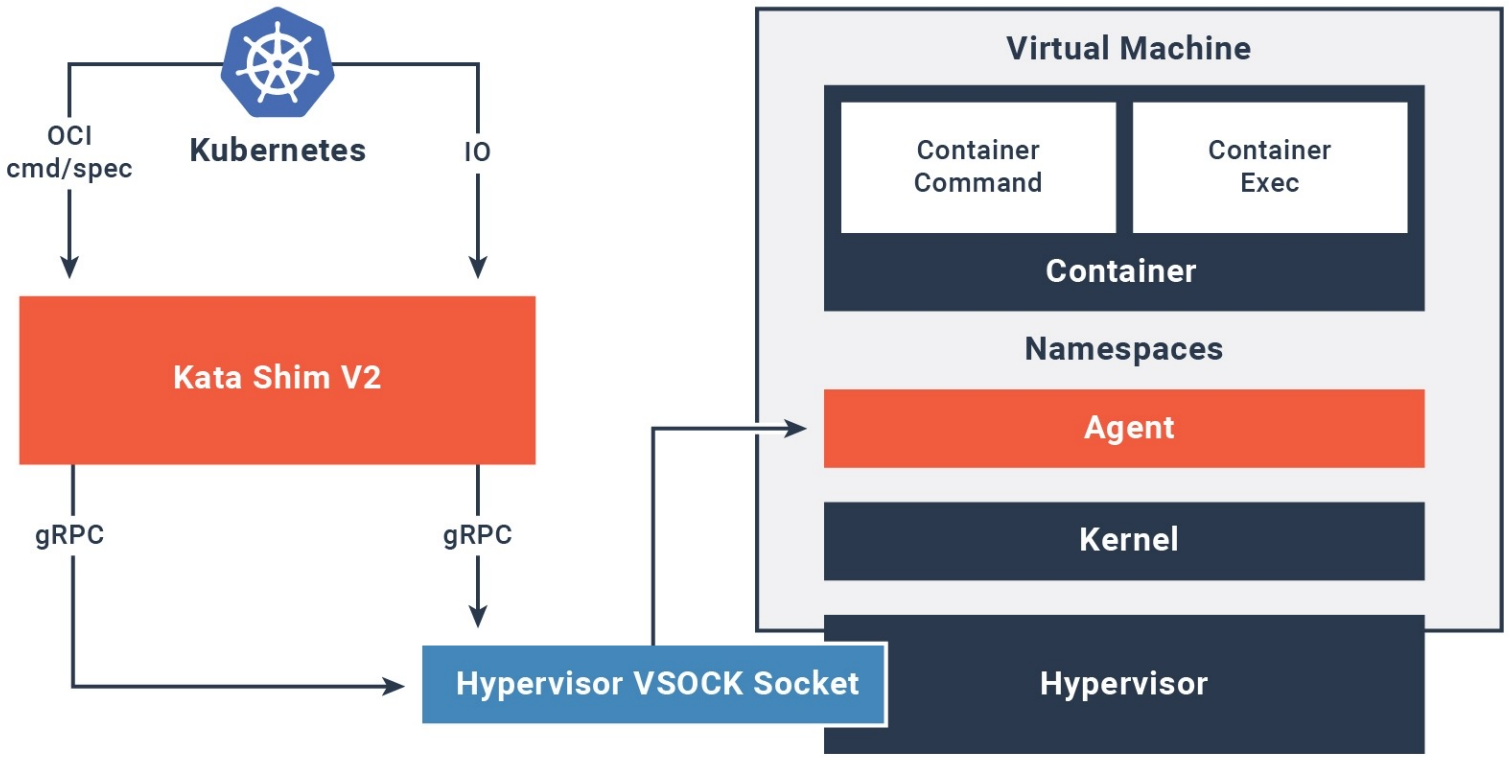
Usecase: Edge Integration



Trust: Wem vertraue ich in der Cloud?

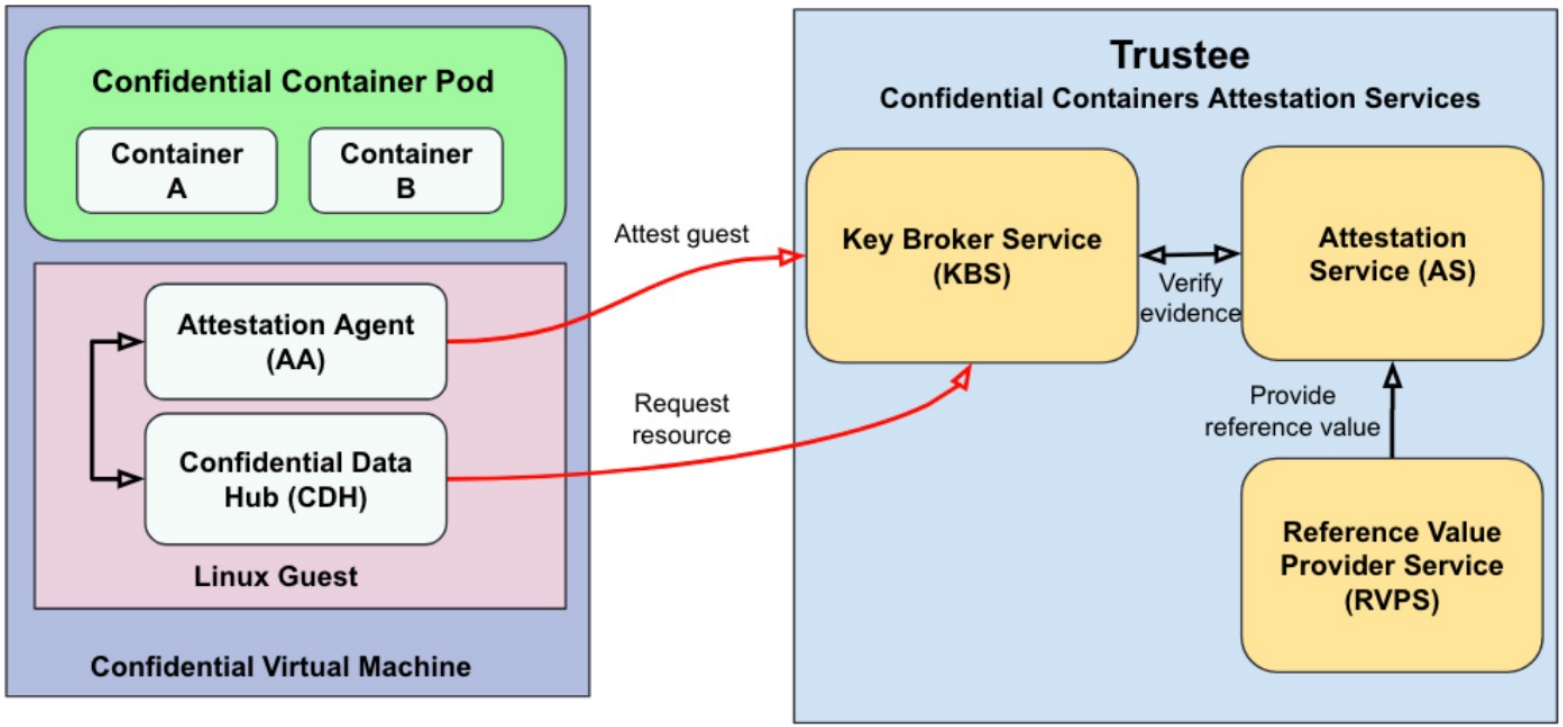


Kata Container

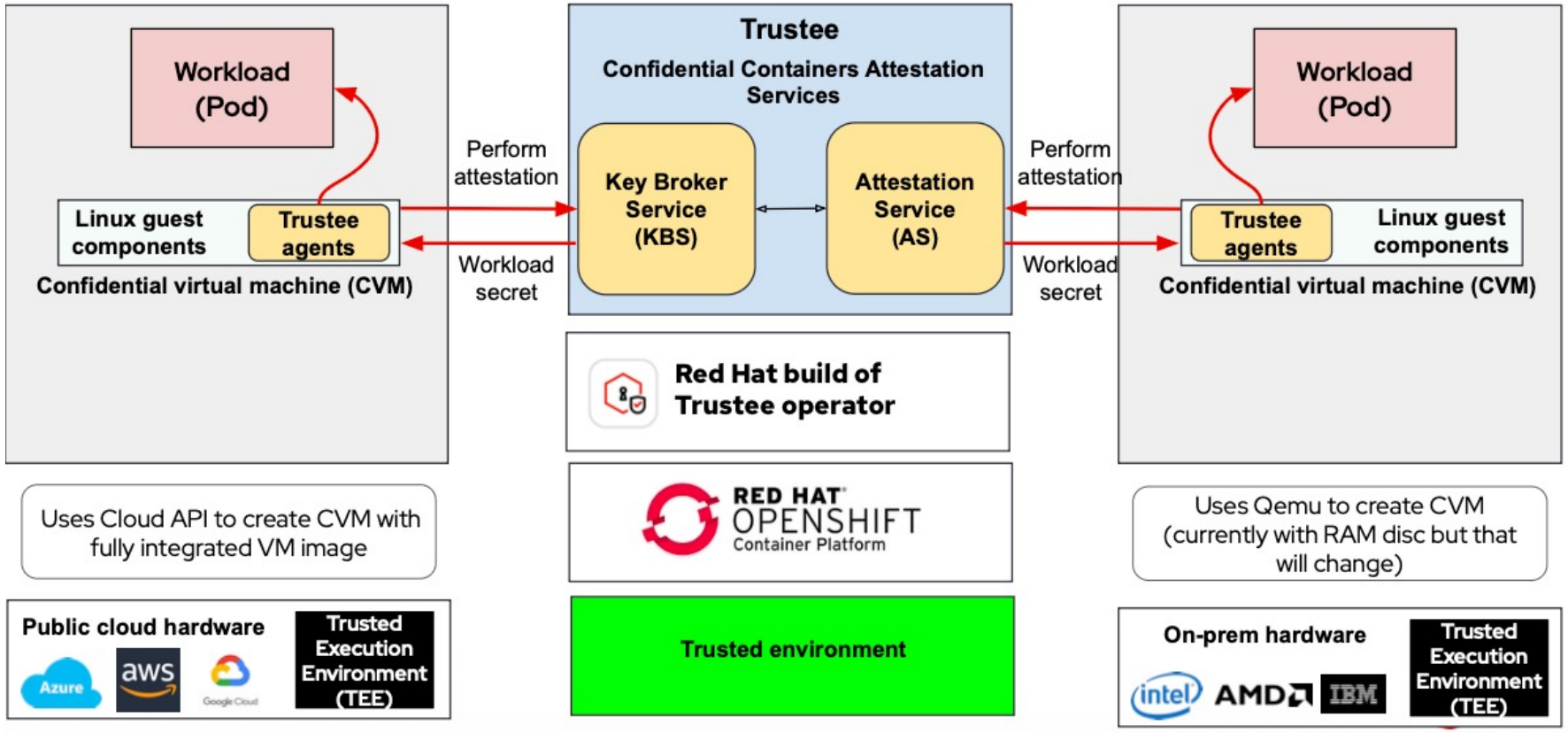


Quelle: https://katacontainers.io/

Trustee


Confidential Container Pod
Container A
Container B
Attestation Agent (AA)
Confidential Data Hub (CDH)
Linux Guest
Confidential Virtual Machine
Attest guest
Request resource
Trustee
Confidential Containers Attestation Services
Key Broker Service (KBS)
Verify evidence
Attestation Service (AS)
Provide reference value
Reference Value Provider Service (RVPS)

Red Hat OpenShift Confidential Container



Lessons Learned

/ Confidential Computing: Vertraulichkeit endet nicht beim Speicher

/ Trust muss messbar sein: Remote Attestation als Grundbaustein

/ Confidential Container Workloads lassen sich in bestehende Cloud und Kubernetes Workloads integrieren

/ Confidential Container ermöglichen Public Cloud Nutzung im stark regulierten Bereich & Pattern wie Cloud Bursting

Kontakt

Moritz Meid
Solution Architect

moritz.meid@sva.de
www.sva.de

Lokation Köln
Maarweg 165
50825 Cologne

Niklas Werker
Technical Lead Ansible

niklas.werker@sva.de
www.sva.de

Lokation Köln
Maarweg 165
50825 Cologne


SVA
ALWAYS ON:
ALWAYS BETTER.
↳ SVA @ Red Hat Summit Connect 2025
Besucht uns bei
BOOTH G08