
KubeCon
CloudNativeCon
North America 2023

From Threats to Trust: Safeguarding Sensitive Data in K8s

Moritz Eckert

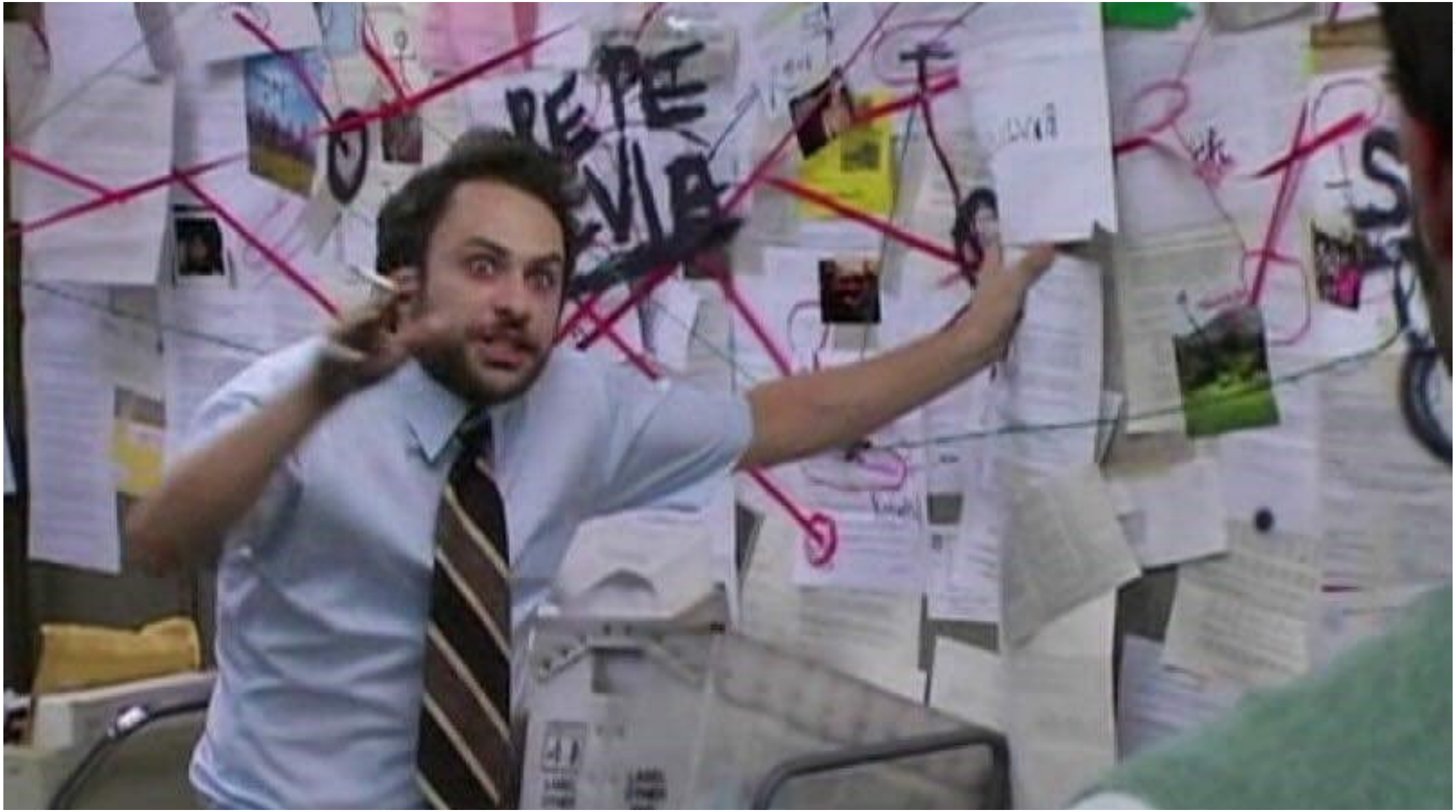
whois

Moritz Eckert
Chief architect @ Edgeless Systems

[Edgeless]
Startup from Bochum Germany
Open Source Confidential Computing
Organizers of OC3

[Moritz]
Background in software security research
Retired member of CTF team Shellphish
Cycling fanatic p/b coffee

Trust




KubeCon | CloudNativeCon

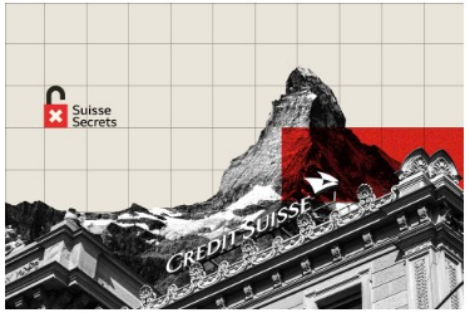
North America 2023

Where trust matters

Investigative Journalism

https://www.icij.org/investigations/panama-papers/

Getty Images



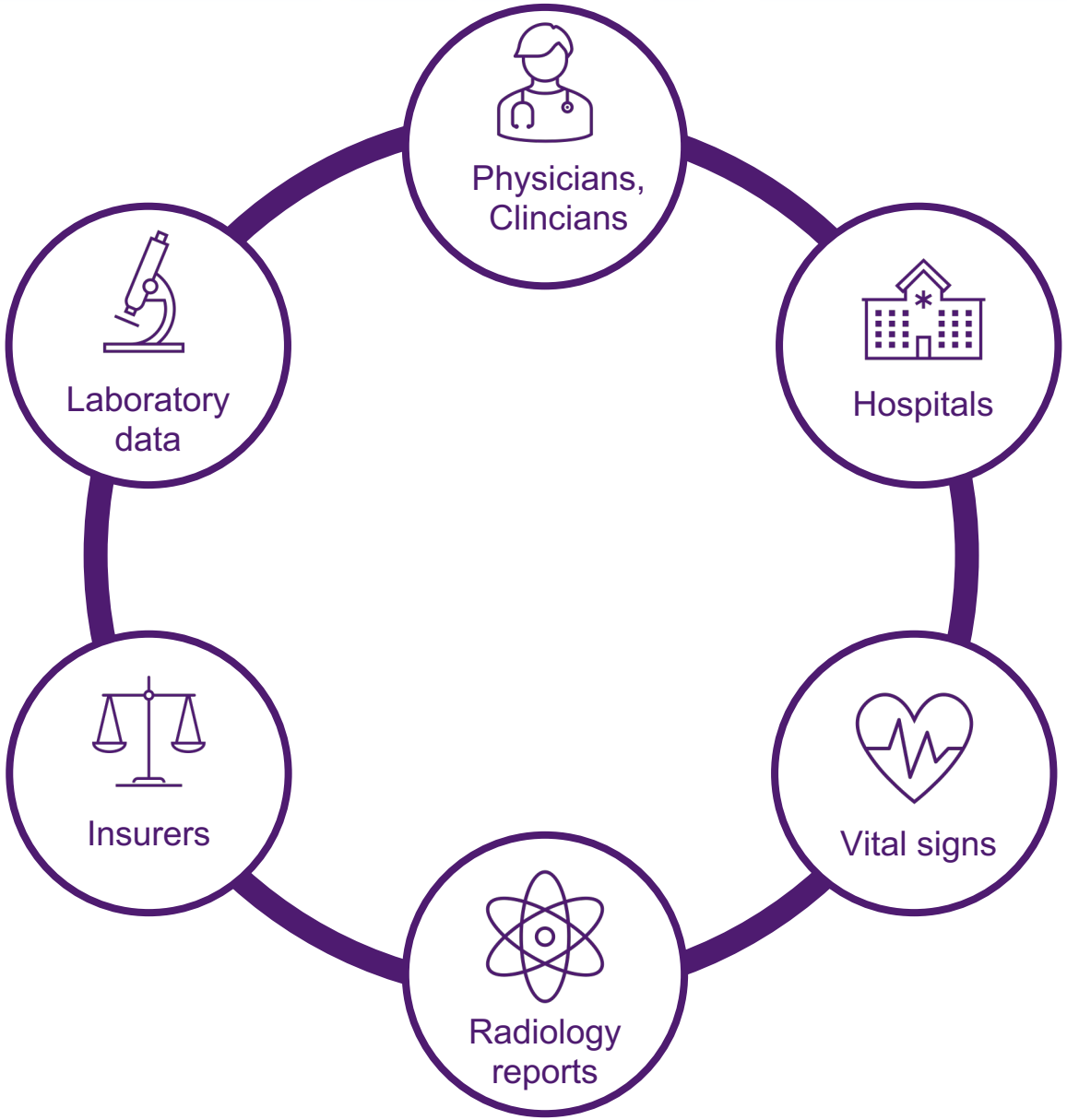
Suisse Secrets

The Pandora Papers

The Pegasus Project

https://www.occrp.org/en

Electronic Health Records

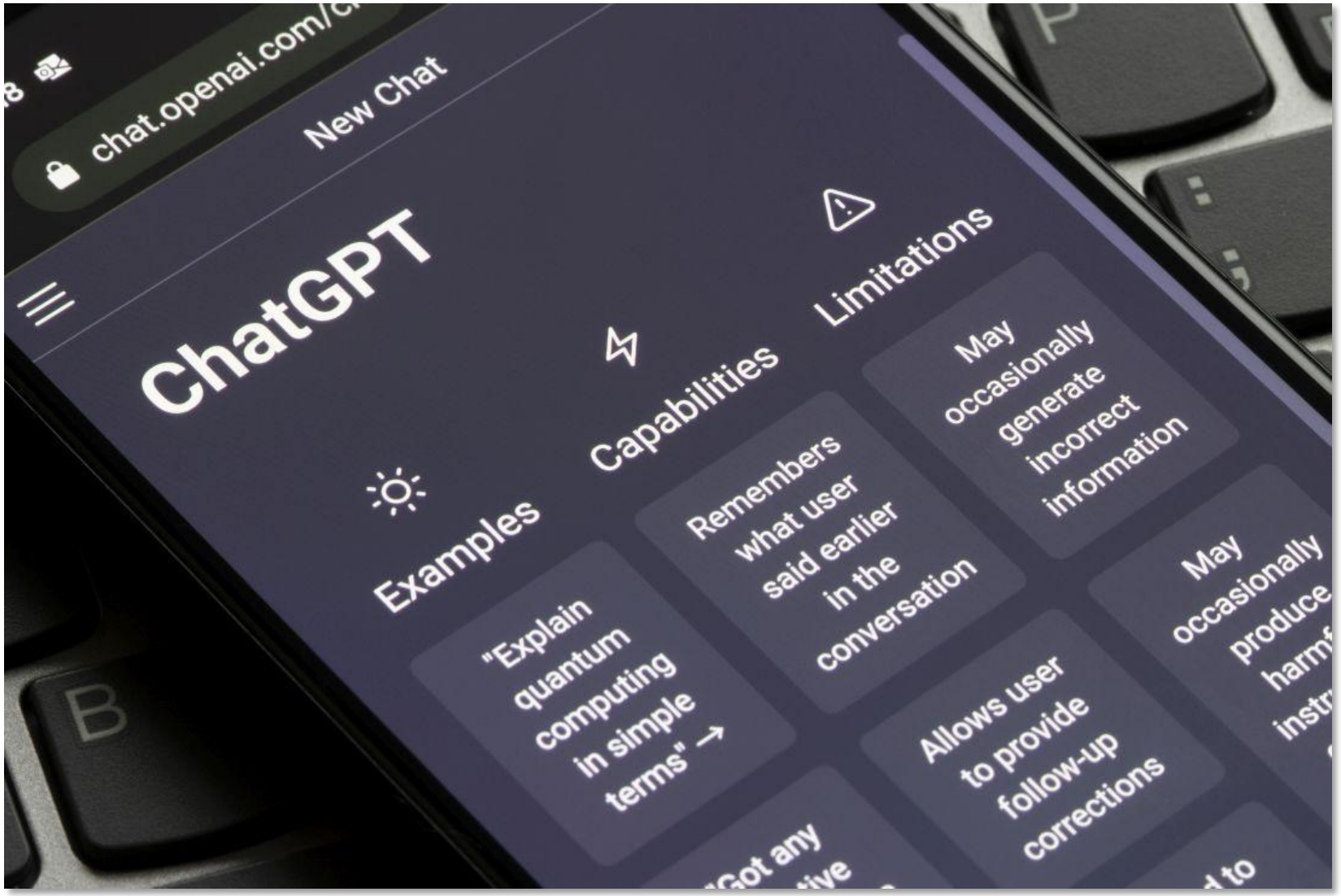


EU: Digital Operational Resilience Act

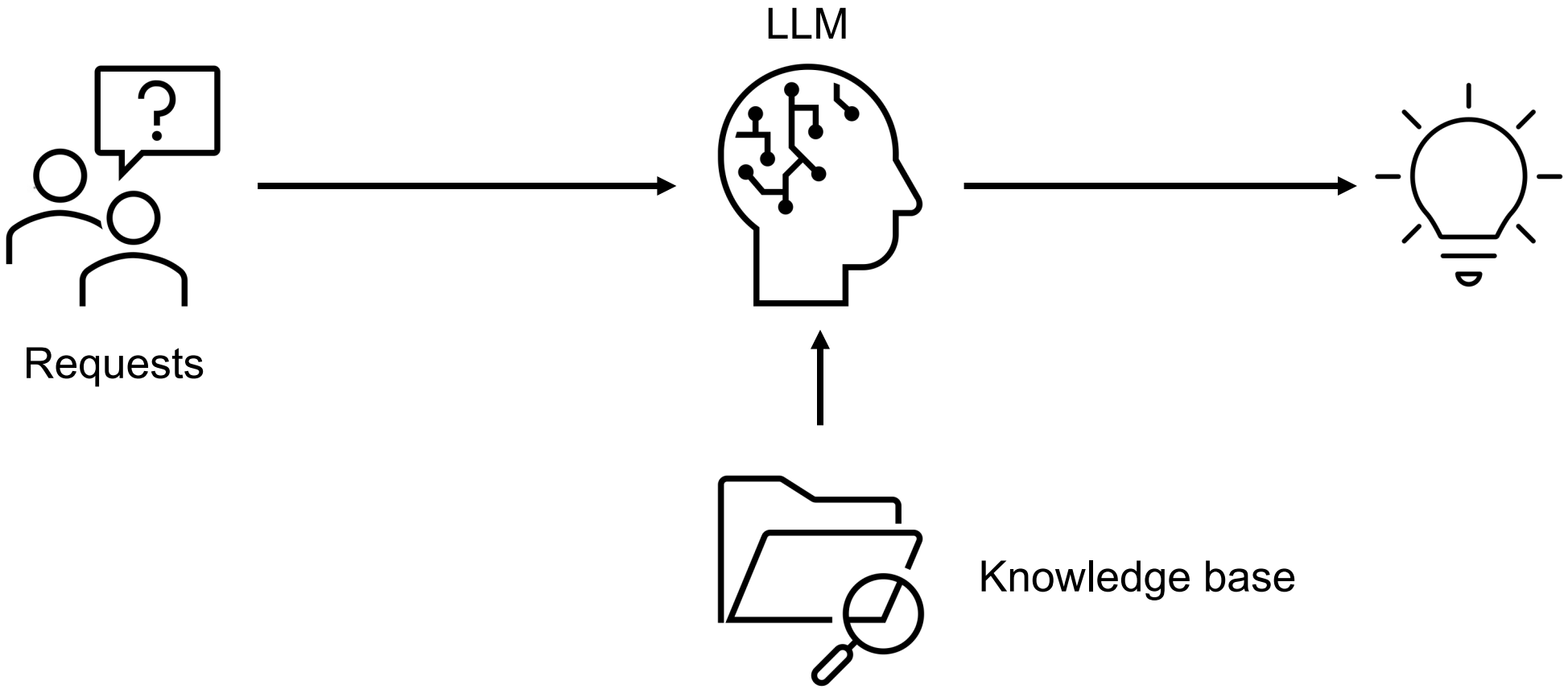
RTS Article 6 Encryption and cryptographic controls

2. (a) […] rules for the **encryption of data at rest, in transit and, where relevant, in use**, taking into account the results of the approved data classification […]
If encryption of data in use is not possible, financial entities shall process data in use in a **separated and protected environment** […]

AI & LLMs

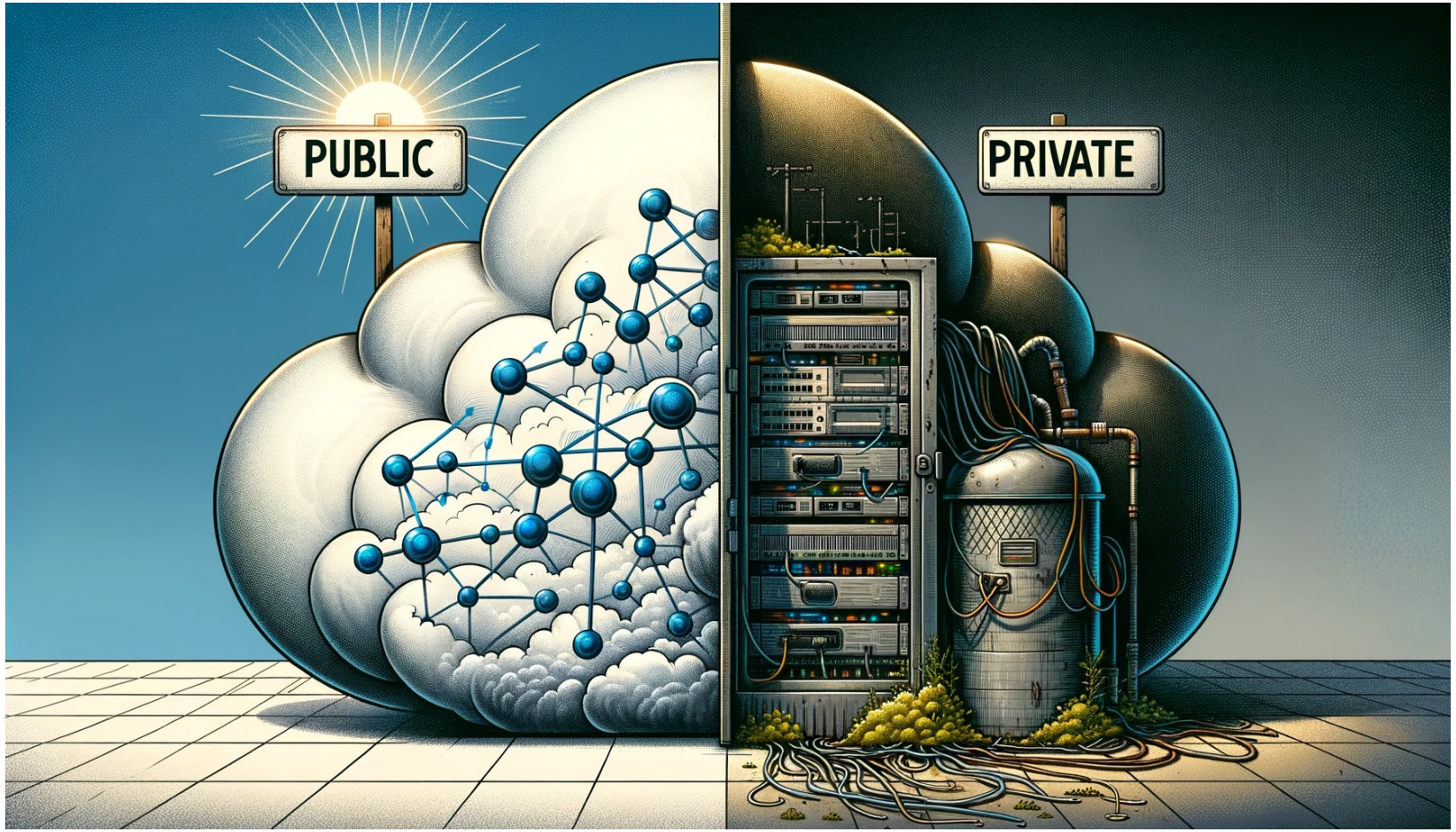

chat.openai.com/
New Chat
ChatGPT
Examples
Capabilities
Limitations
"Explain quantum computing in simple terms" →
Remembers what user said earlier in the conversation
May occasionally generate incorrect information
Allows user to provide follow-up corrections
May occasionally produce
B

AI & LLMs



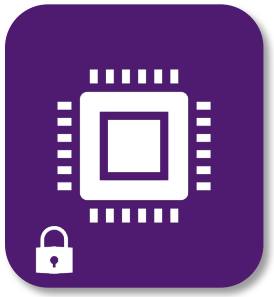
How to trust

Private Cloud



Encryption and isolation

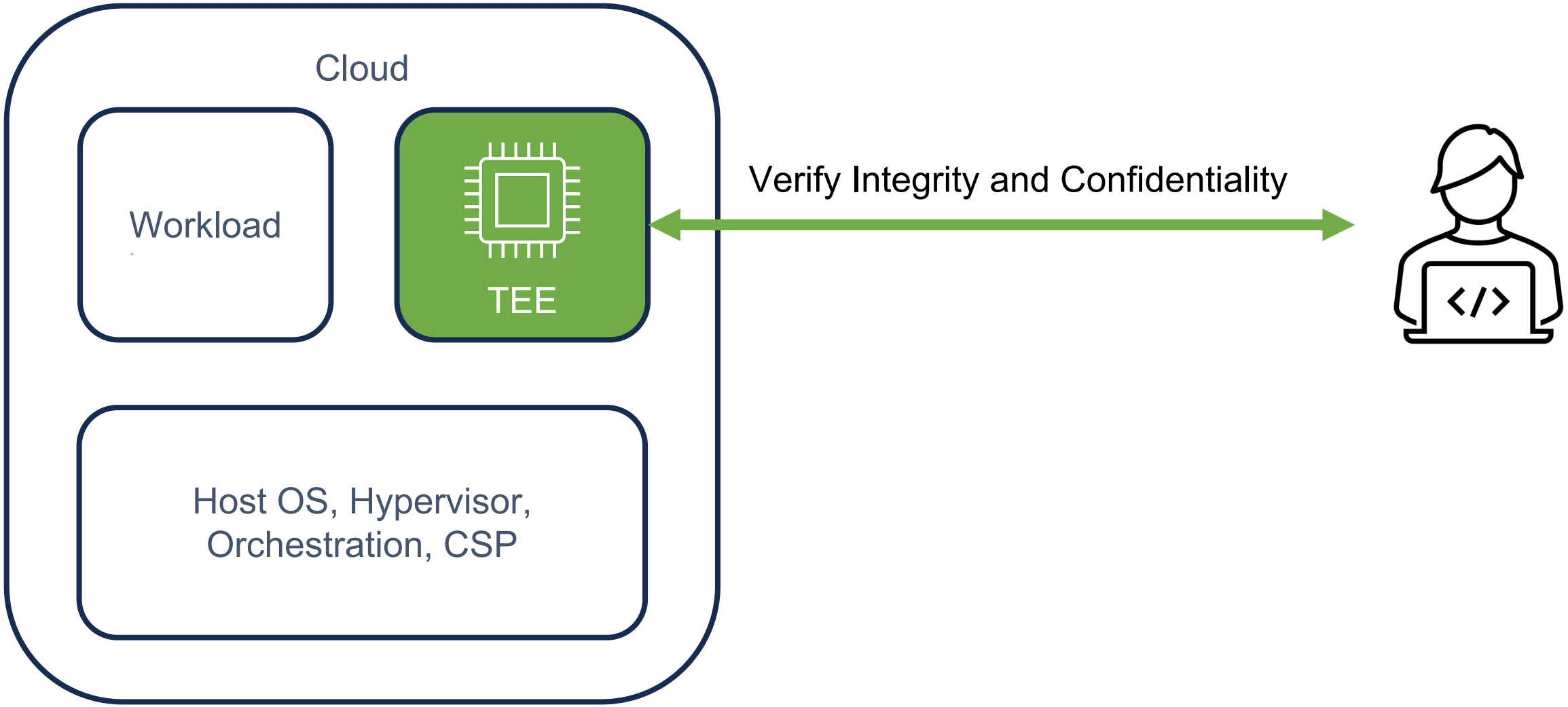
Protection at rest



Protection in use

Protection in transit

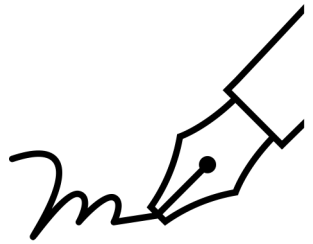
Confidential Computing



Trusted Execution Environments

Encryption of Data In-Use

Measurements of Identity

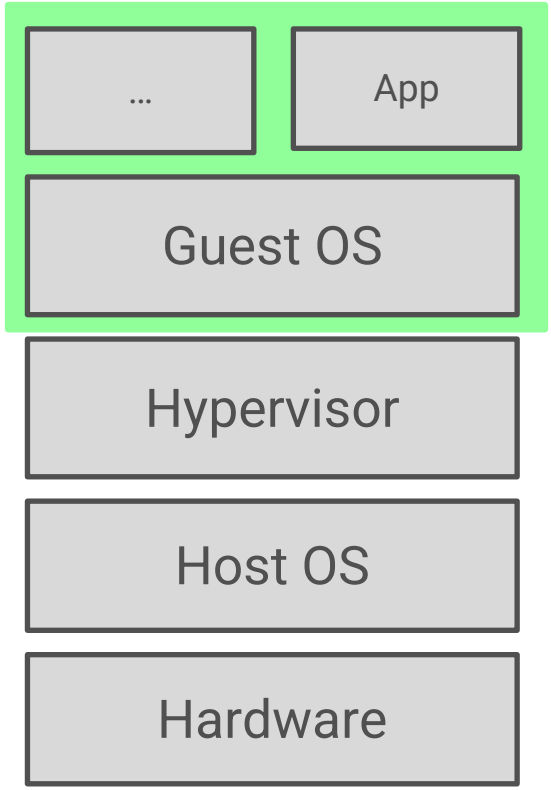


Remote Attestation

Trusted Execution Environments

- 🏝️ Isolation of VMs
- 🏃 Runtime memory-encryption
- 📃 Remote attestation

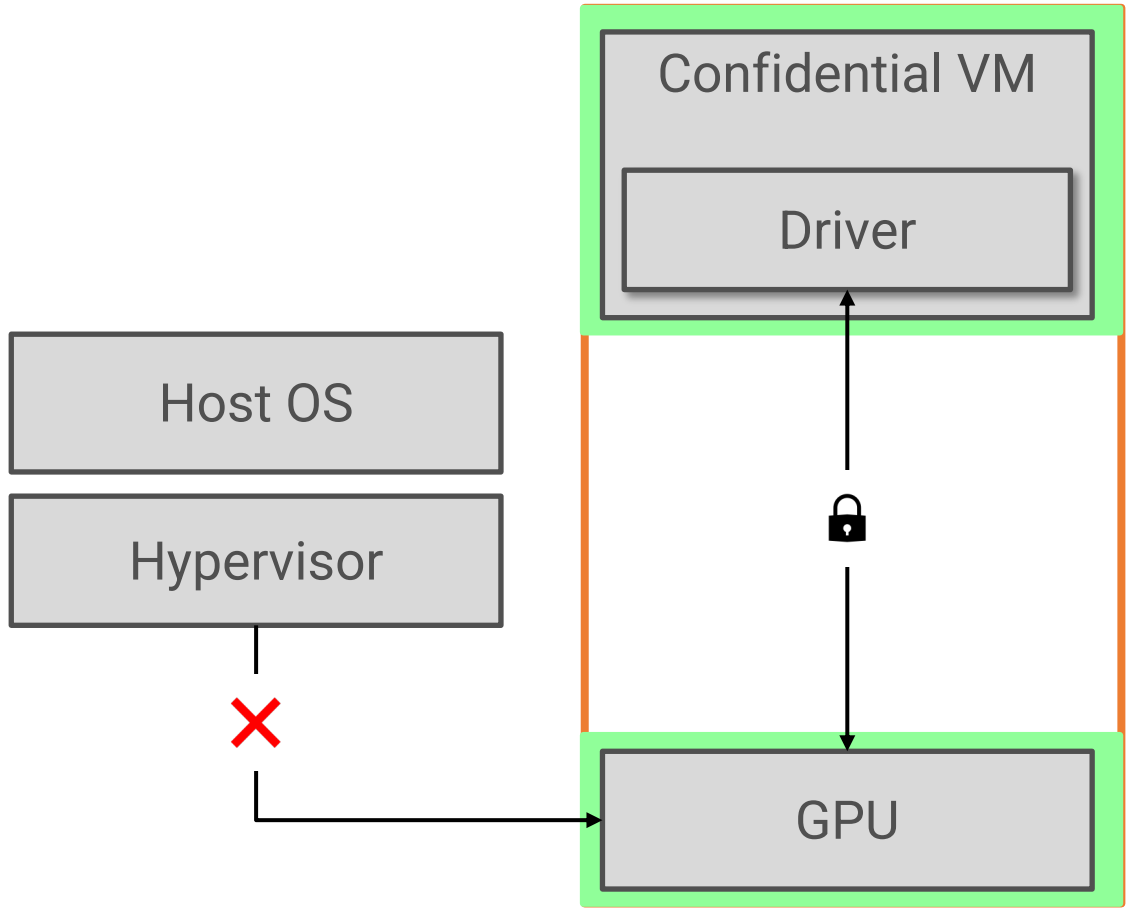
AMD SEV, Intel TDX, ARM CCA,
IBM SE, RISC-V AP-TEE



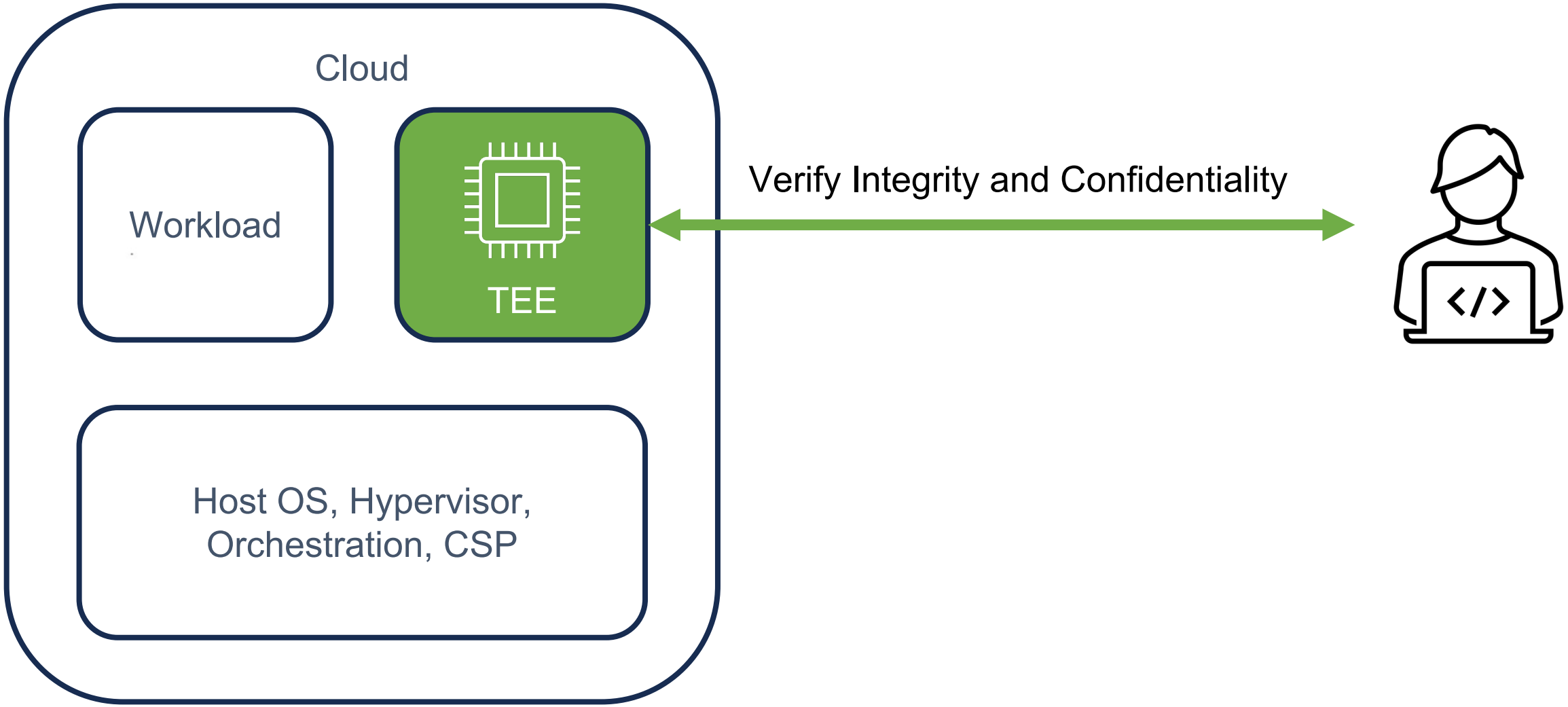
Trusted Execution Environments

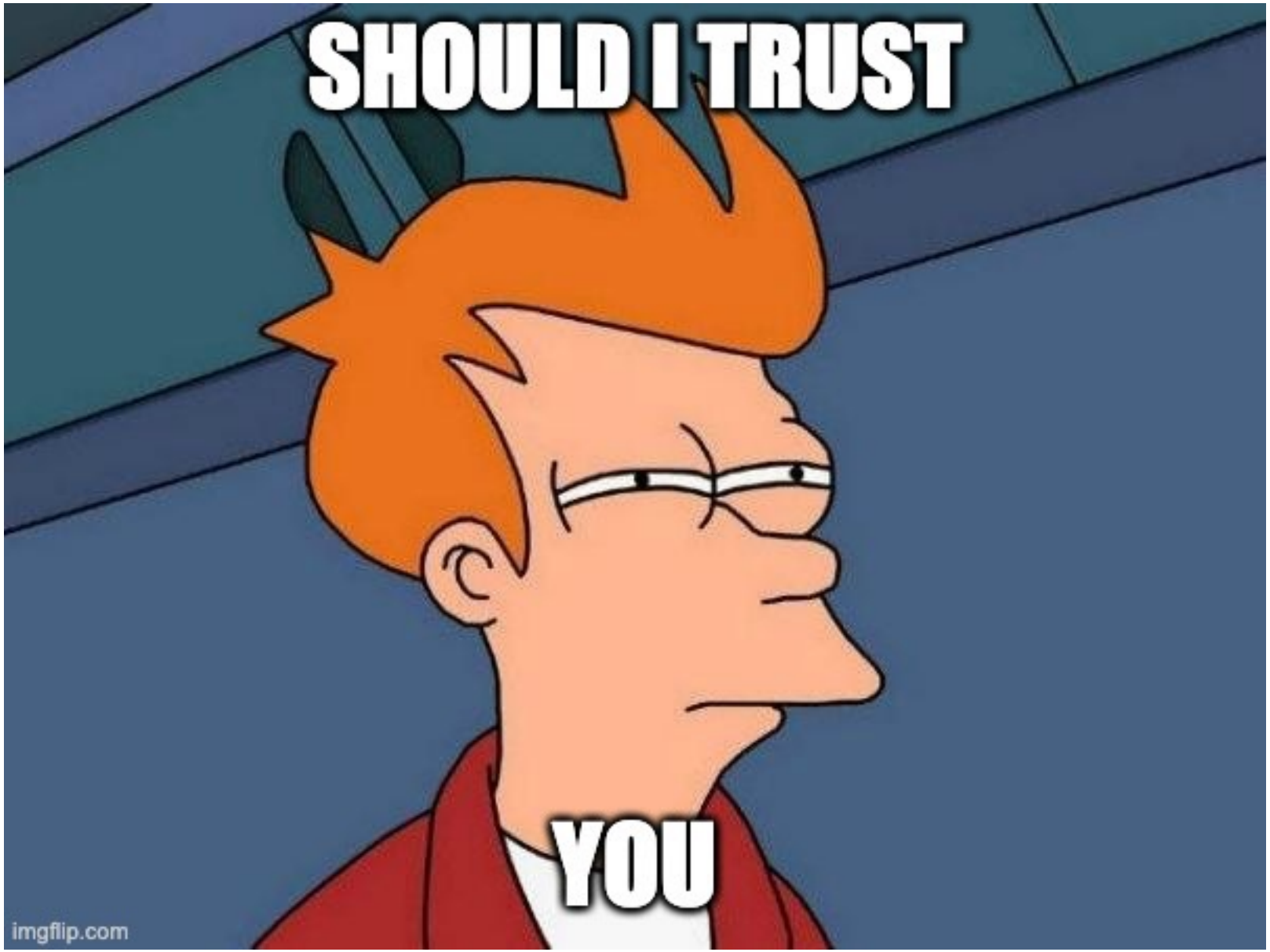
- 🏝️ TEE isolation inside GPU
- 🏃‍♀️ Encrypted CPU to GPU transfer
- 📃 Remote attestation

NVIDIA H100

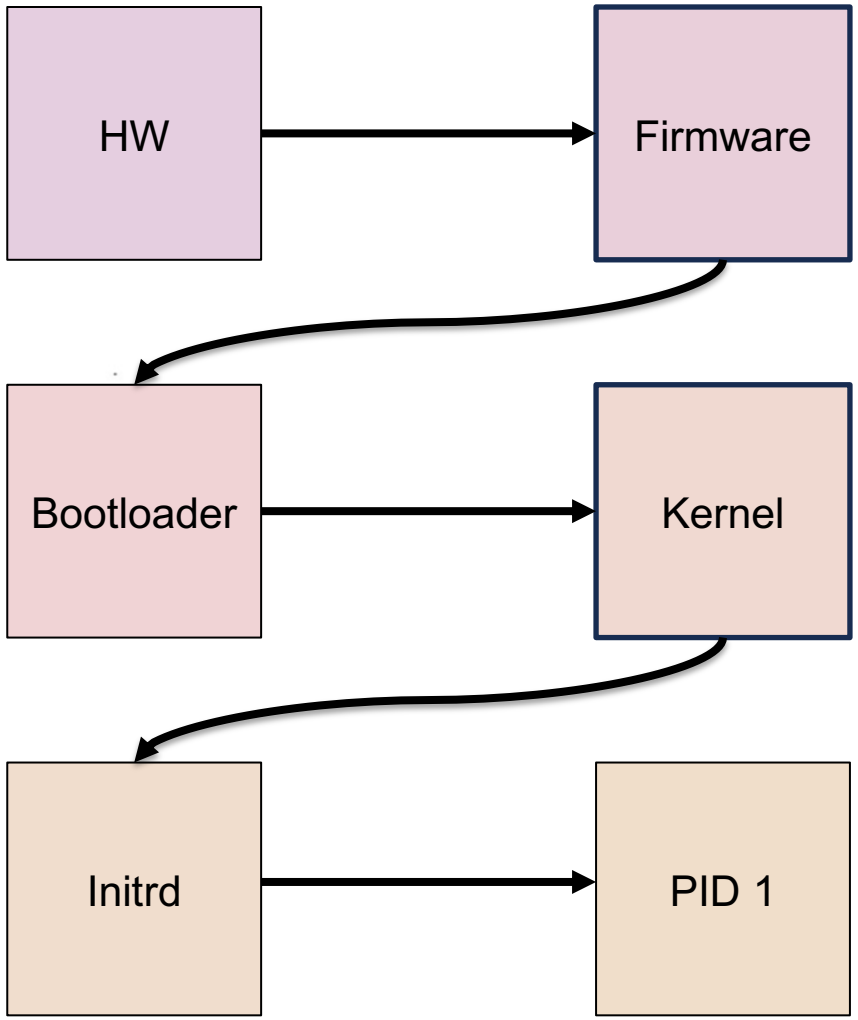


Confidential Computing



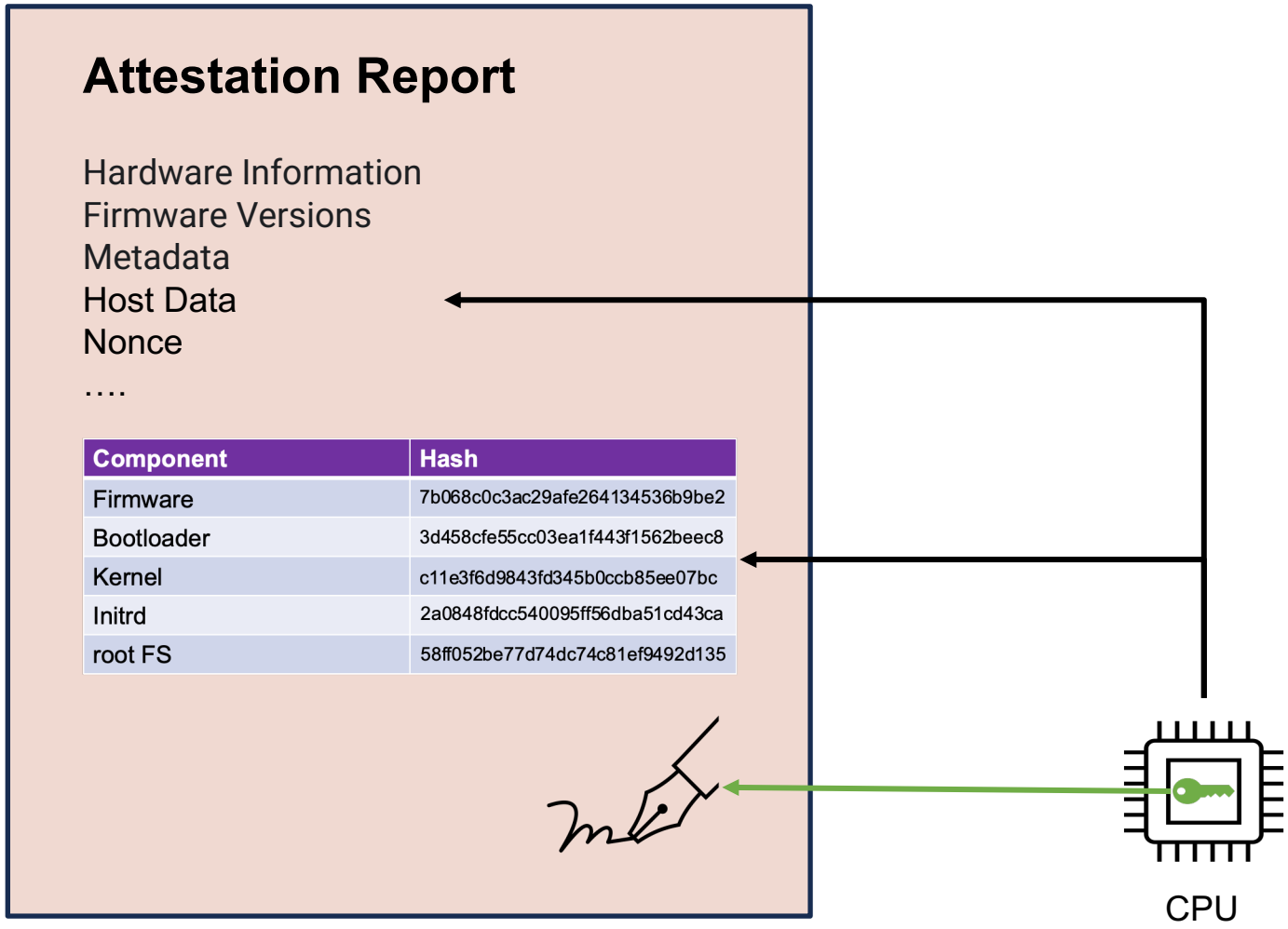

SHOULD I TRUST
YOU
imgflip.com

Measurements of Identity



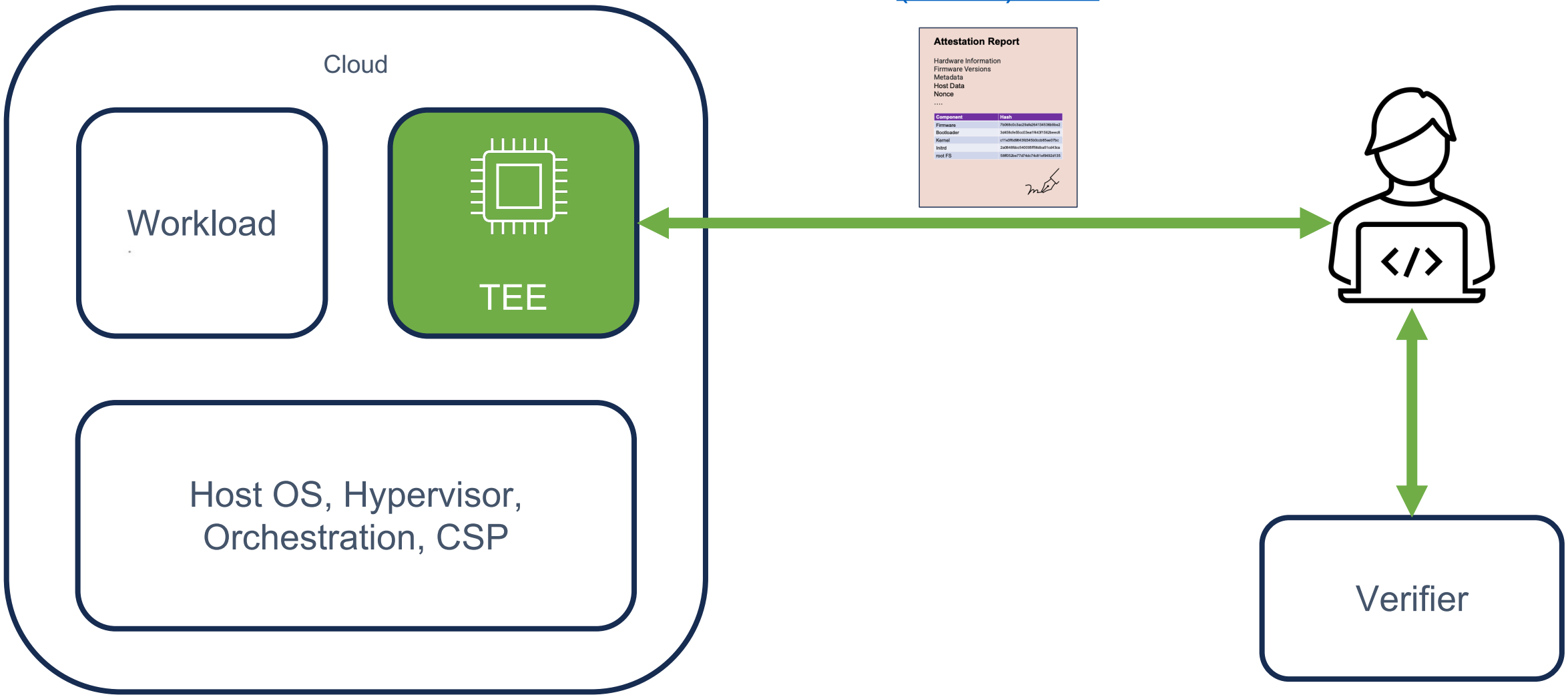
Component	Hash
Firmware	7b068c0c3ac29afe264134536b9be2
Bootloader	3d458cfe55cc03ea1f443f1562beec8
Kernel	c11e3f6d9843fd345b0ccb85ee07bc
Initrd	2a0848fdcc540095ff56dba51cd43ca
root FS	58ff052be77d74dc74c81ef9492d135

Attestation Report

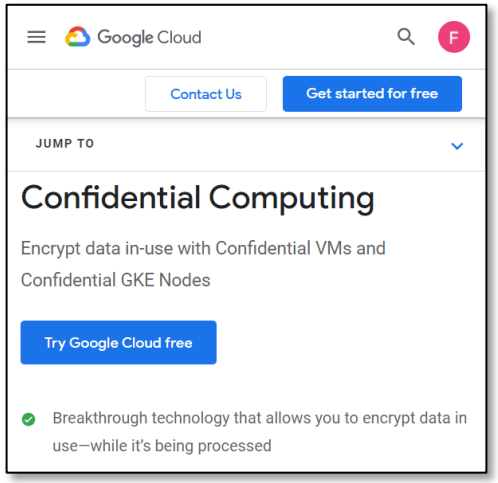


Attestation

[Remote ATtestation procedureS (RATS) RFC]



Availability

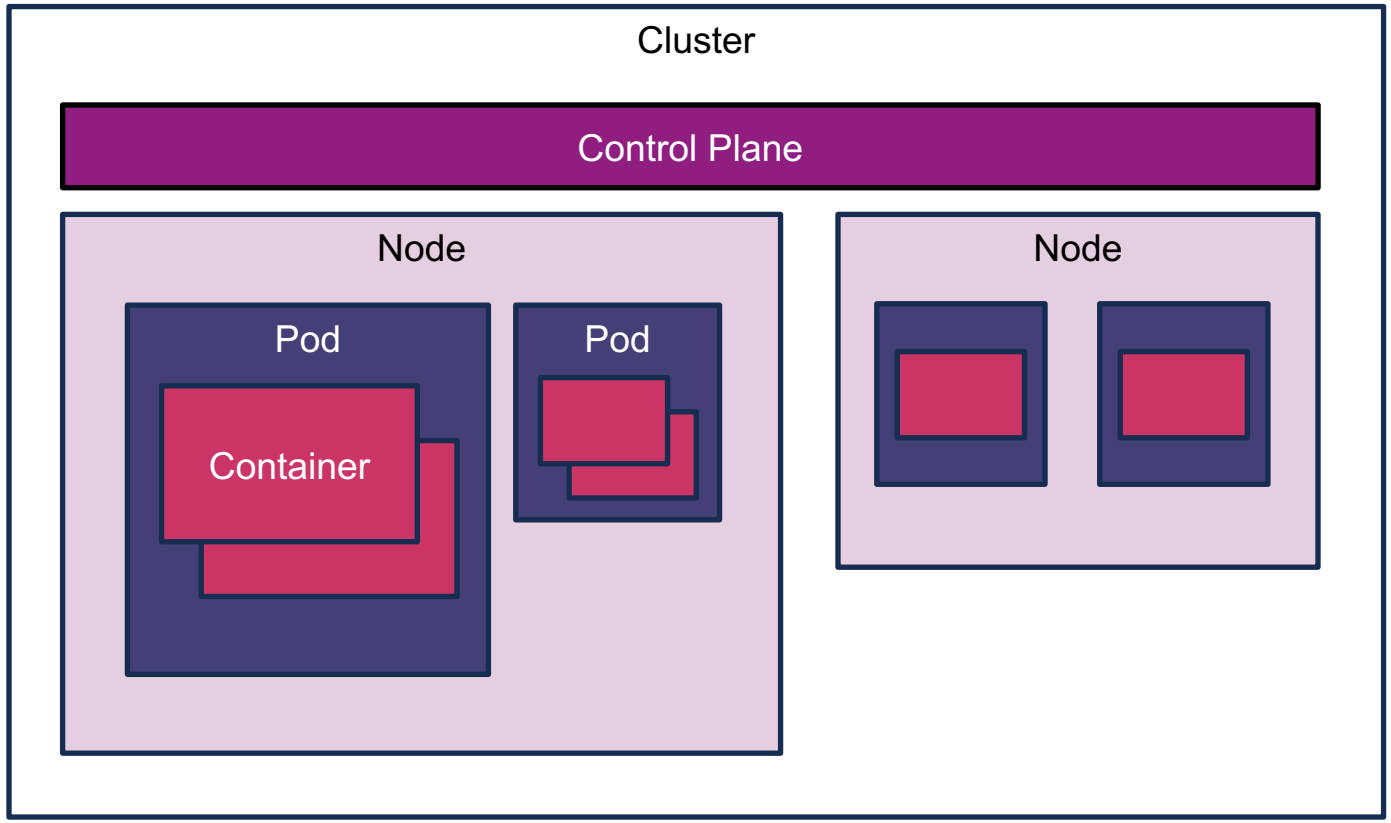



KubeCon | CloudNativeCon

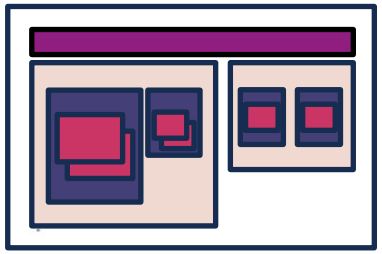
North America 2023

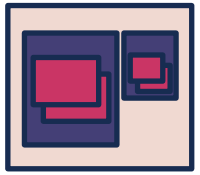
How to use

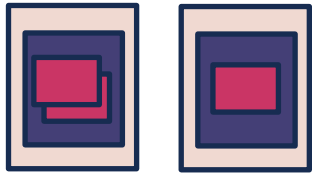
TEEs & Kubernetes



TEEs & Kubernetes







K8s Cluster as one concise Confidential Cluster

Worker Nodes on CVMs

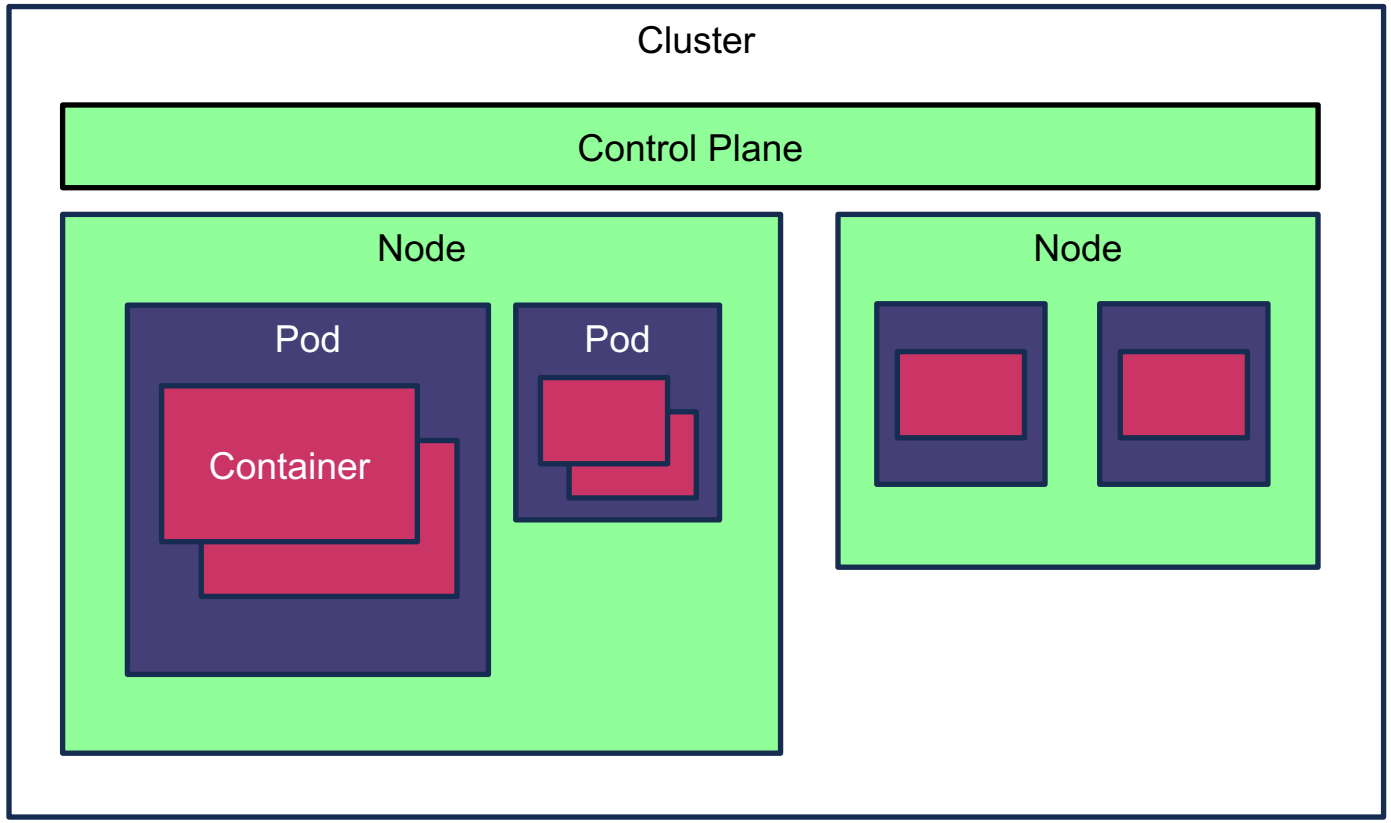
Deploy K8s Pods in CVMs

Constellation

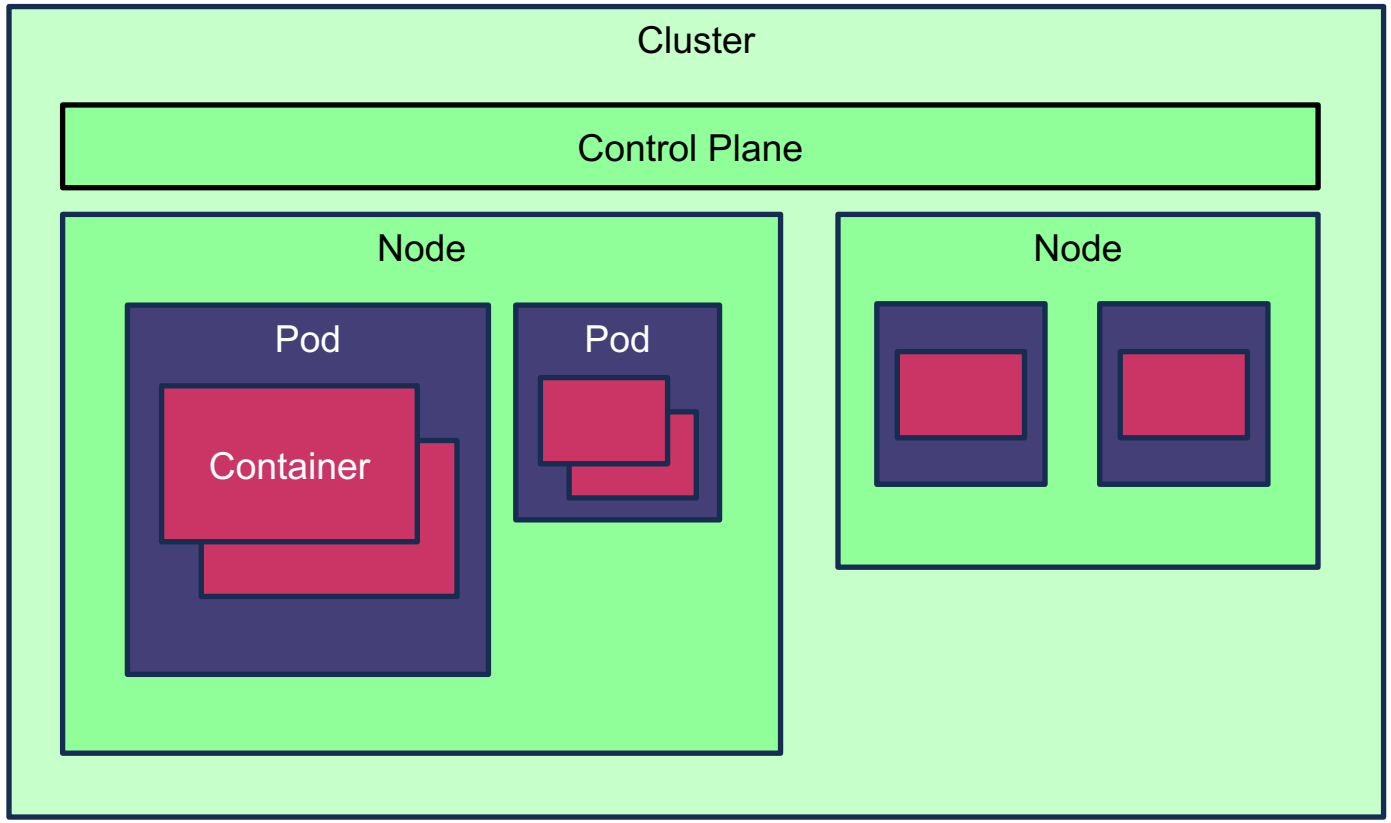
Confidential Node Pools

Confidential Containers

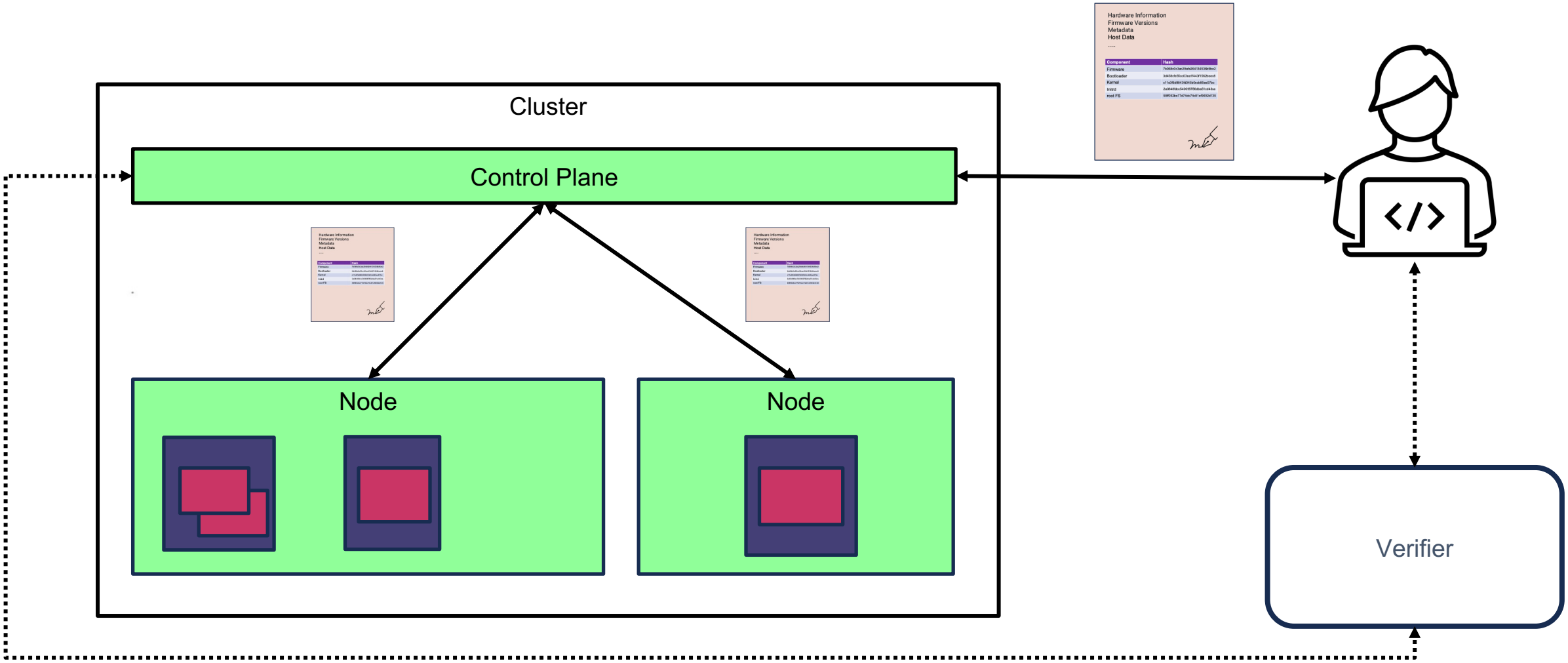
Confidential Cluster



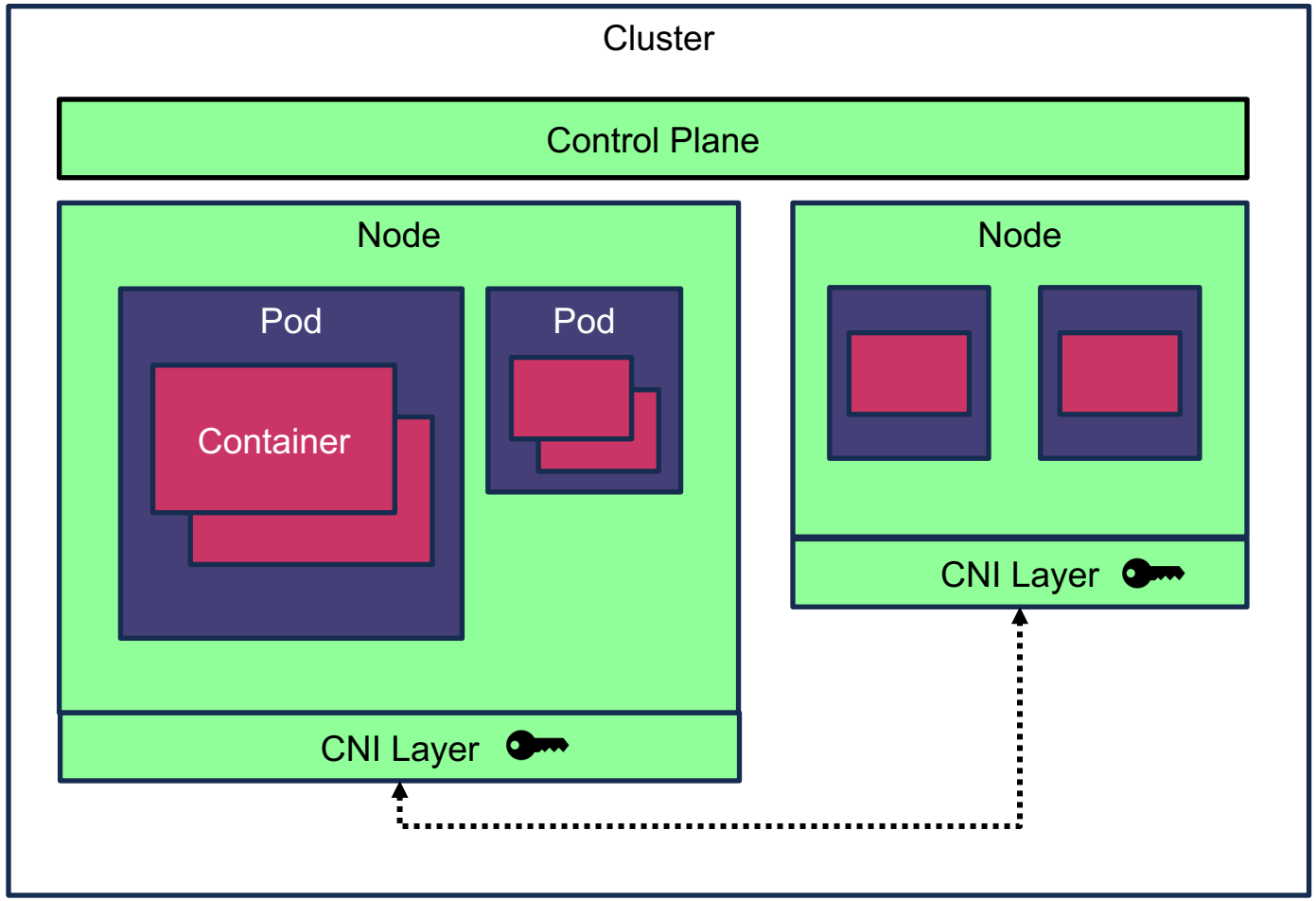
Confidential Cluster



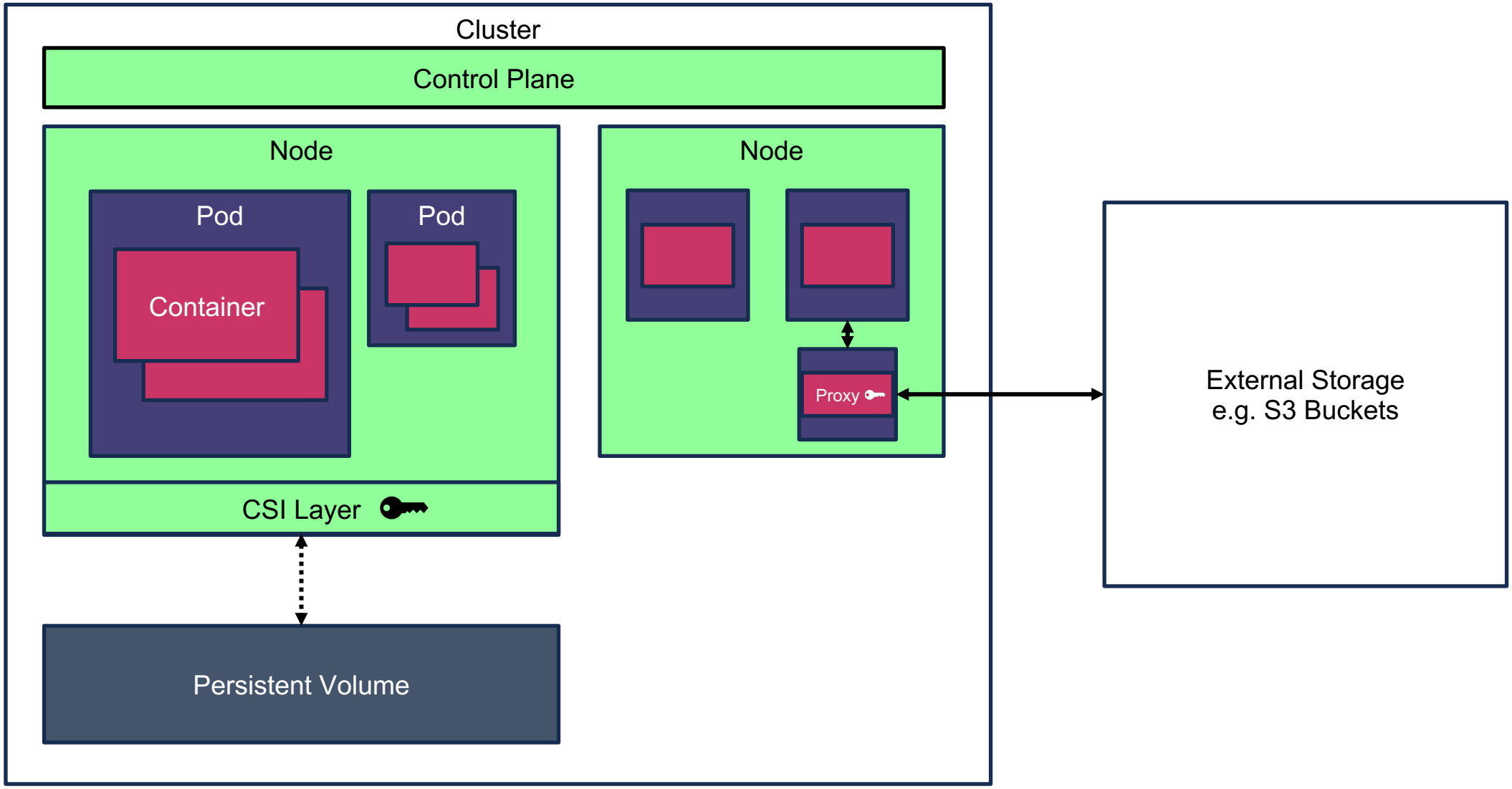
Confidential Cluster - Attestation



Confidential Cluster - Networking



Confidential Cluster - Storage

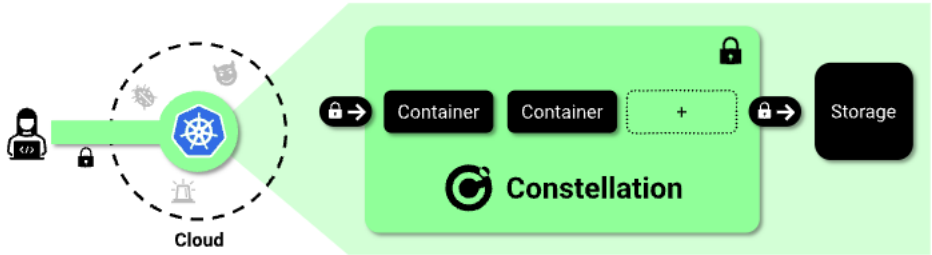


Constellation

README.md

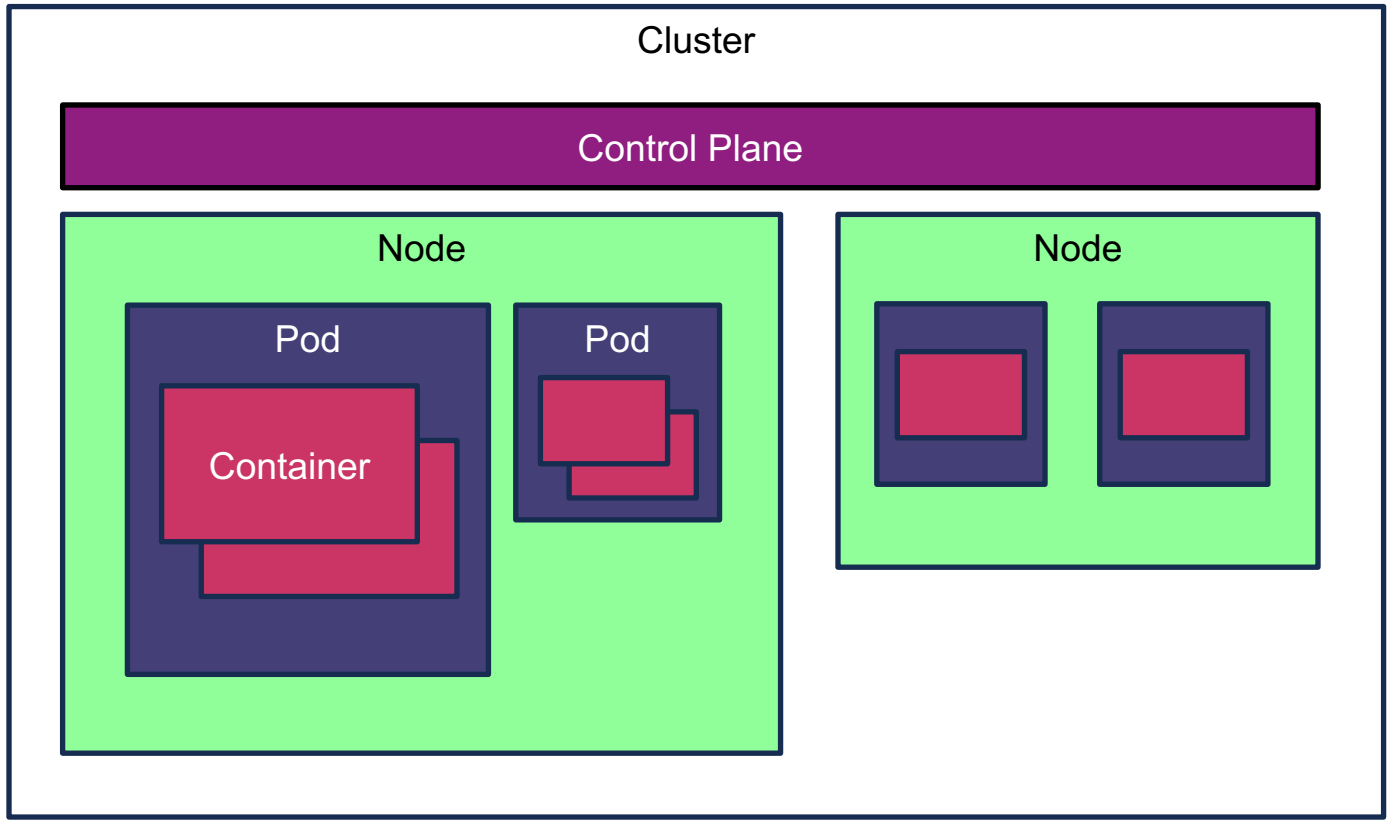
Always Encrypted Kubernetes

Constellation is a Kubernetes engine that aims to provide the best possible data security. It wraps your K8s cluster into a single *confidential context* that is shielded from the underlying cloud infrastructure. Everything inside is always encrypted, including at runtime in memory. For this, Constellation leverages confidential computing (see the whitepaper) and more specifically Confidential VMs.

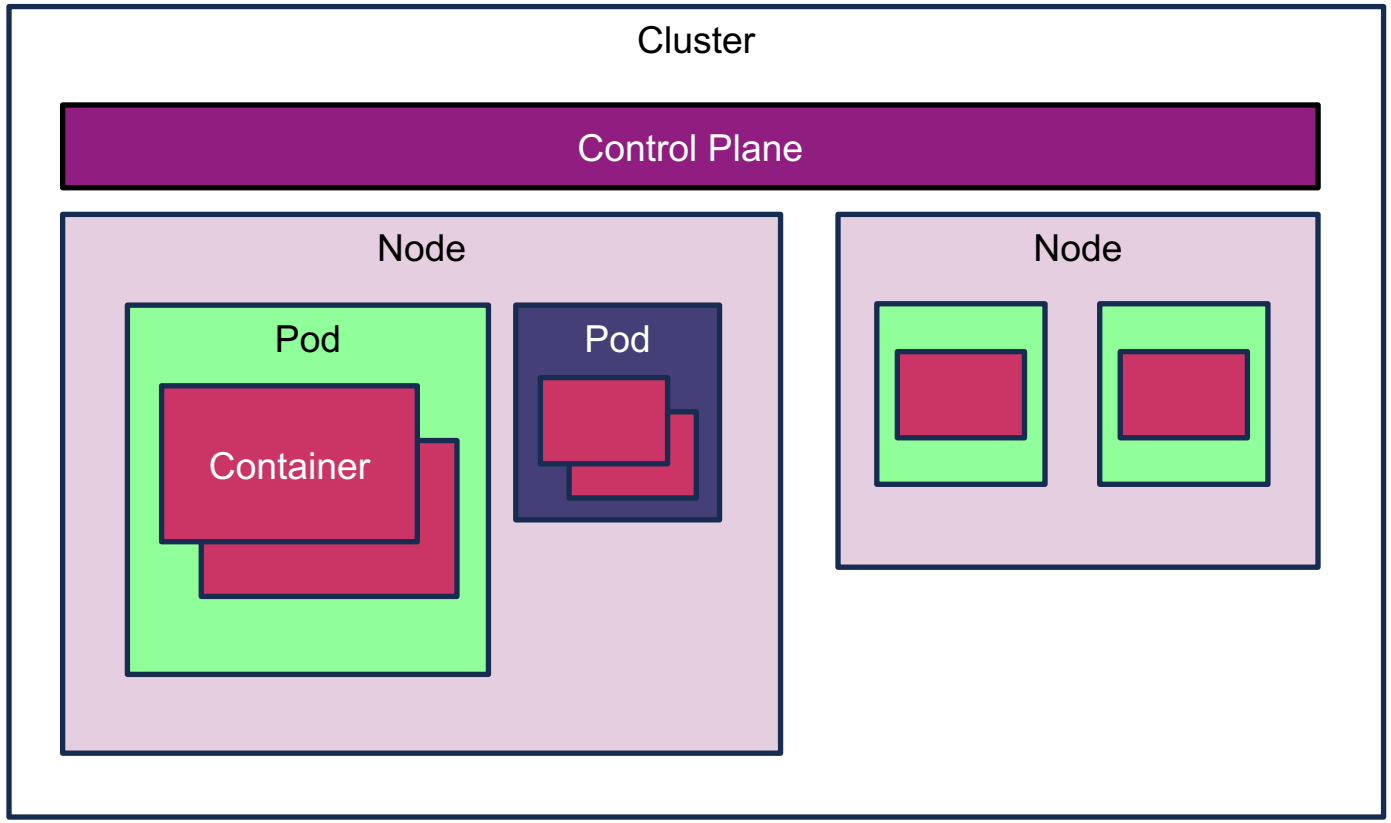


https://github.com/edgelesssys/constellation
OpenShift Confidential Cluster concept presentation (starting 40:00)

Confidential Worker Nodes

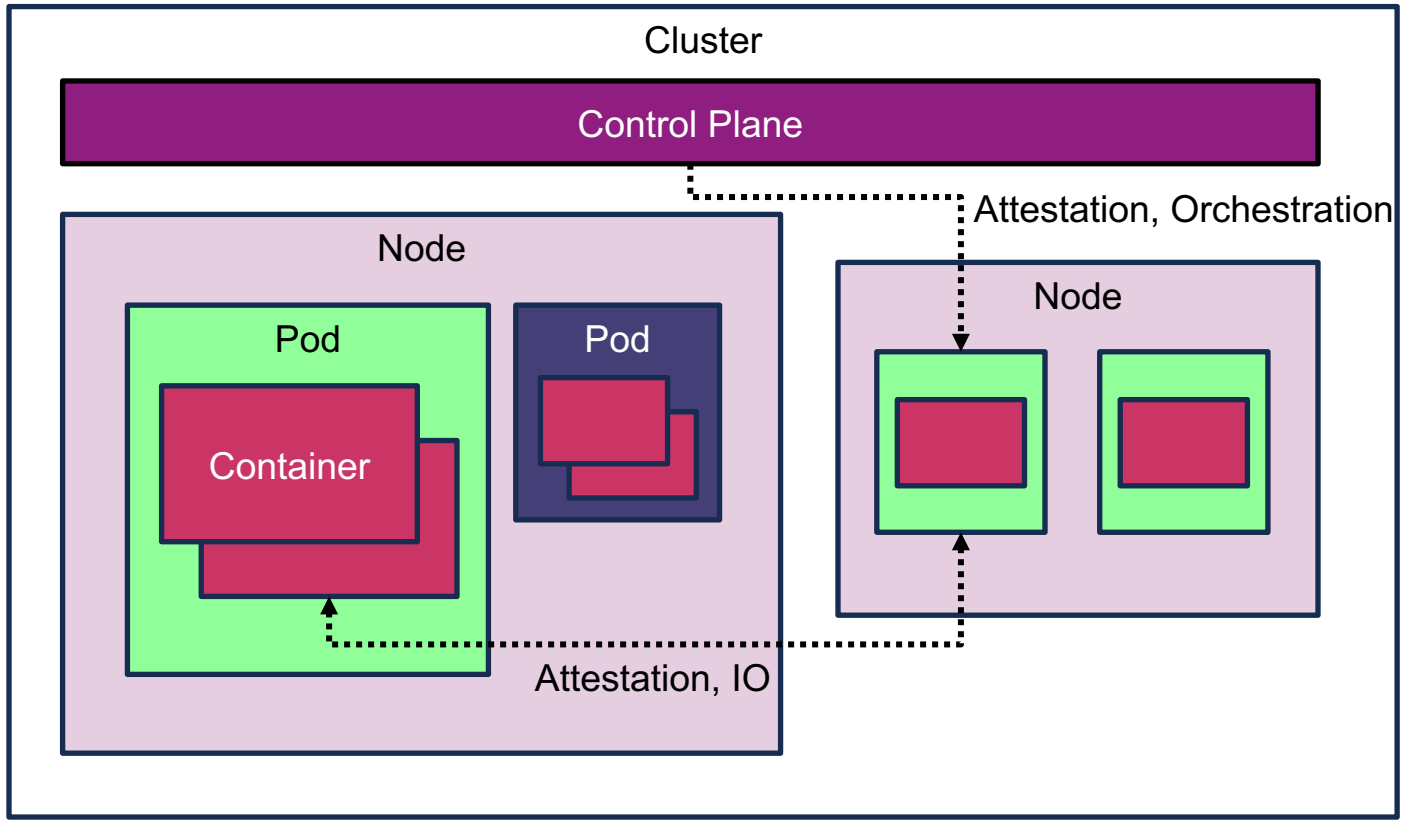


Confidential Containers



kata containers

Confidential Containers



Confidential Containers

Confidential Containers: Why, How, and Where Are We? – Magnus Kulke, Microsoft

Confidential Containers

- Abbreviation: *CoCo*
- Implements Confidential Pods
- Open Source, CNCF Sandbox Project
- Collaborative, multi-vendor effort (HW, CSPs, Linux, Security)
- Golang, Rust

github.com/confidential-containers

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT EUROPE

Confidential Containers

README.md

Confidential Containers

Welcome to confidential-containers

Confidential Containers is an open source community working to leverage Trusted Execution Environments to protect containers and data and to deliver cloud native confidential computing.

We have a new release every 6 weeks! See Release Notes or Quickstart Guide

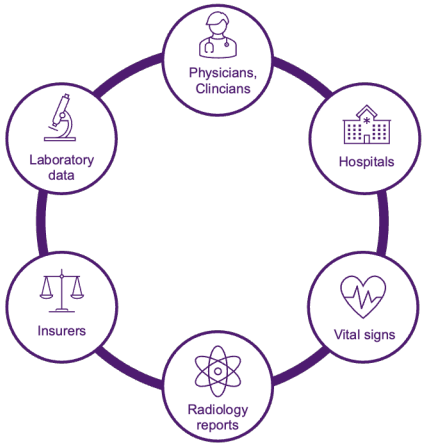
Our key considerations are:

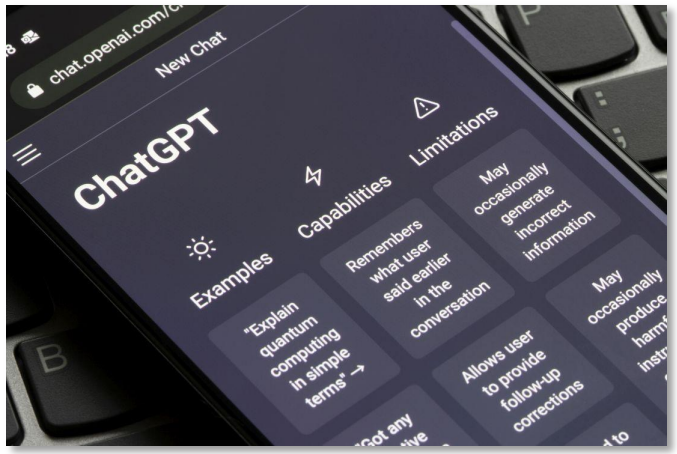
- Allow cloud native application owners to enforce application security requirements
- Transparent deployment of unmodified containers
- Support for multiple TEE and hardware platforms
- A trust model which separates Cloud Service Providers (CSPs) from guest applications
- Least privilege principles for the Kubernetes cluster administration capabilities which impact delivering Confidential Computing for guest applications or data inside the TEE

https://github.com/confidential-containers/confidential-containers
https://github.com/intel/ACON

Take aways

Why?

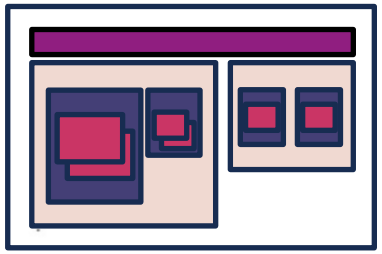


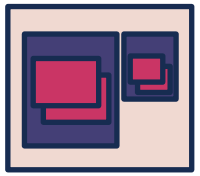


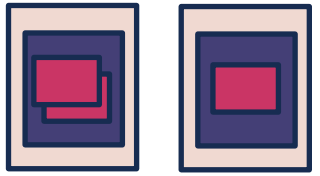
RTS Article 6 Encryption and cryptographic controls

2. (a) […] rules for the **encryption of data at rest, in transit and, where relevant, in use**, taking into account the results of the approved data classification […]
If encryption of data in use is not possible, financial entities shall process data in use in a **separated and protected environment** […]

How?







K8s Cluster as one concise Confidential Cluster

Worker Nodes on CVMs

Deploy K8s Pods in CVMs

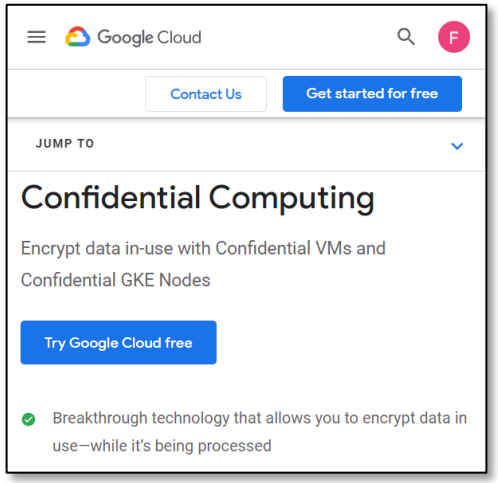
Constellation

Confidential Node Pools

Confidential Containers

Where?


Microsoft Azure
Home / Solutions / Confidential Compute
Azure confidential computing
Protect and secure your cloud data while it's in use
Start free ›


Google Cloud
F
Contact Us
Get started for free
JUMP TO
Confidential Computing
Encrypt data in-use with Confidential VMs and Confidential GKE Nodes
Try Google Cloud free
Breakthrough technology that allows you to encrypt data in use—while it's being processed


aws
AWS Nitro Enclaves
AWS Nitro Enclaves
Create additional isolation to further protect highly sensitive data within EC2 instances
Get started with AWS Nitro Enclaves


IBM Cloud
Security
Confidential computing on IBM Cloud
Protect your data at rest, in transit and in use. Get a higher level of privacy assurance.

Call to action

- For more resources: https://confidentialcomputing.io/
- Kubernetes blog article
- Explore Constellation: https://github.com/edgelesssys/constellation
- Explore Confidential Containers: https://github.com/confidential-containers
- Open Confidential Computing Conference: https://www.oc3.dev/
- Trust in Computer Systems and the Cloud – Mike Bursell

We’re heading towards a fully confidential cloud[1]

1) Mark Russinovich: Journey towards the Confidential Cloud by, OC3 2022

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