Edgeless Systems

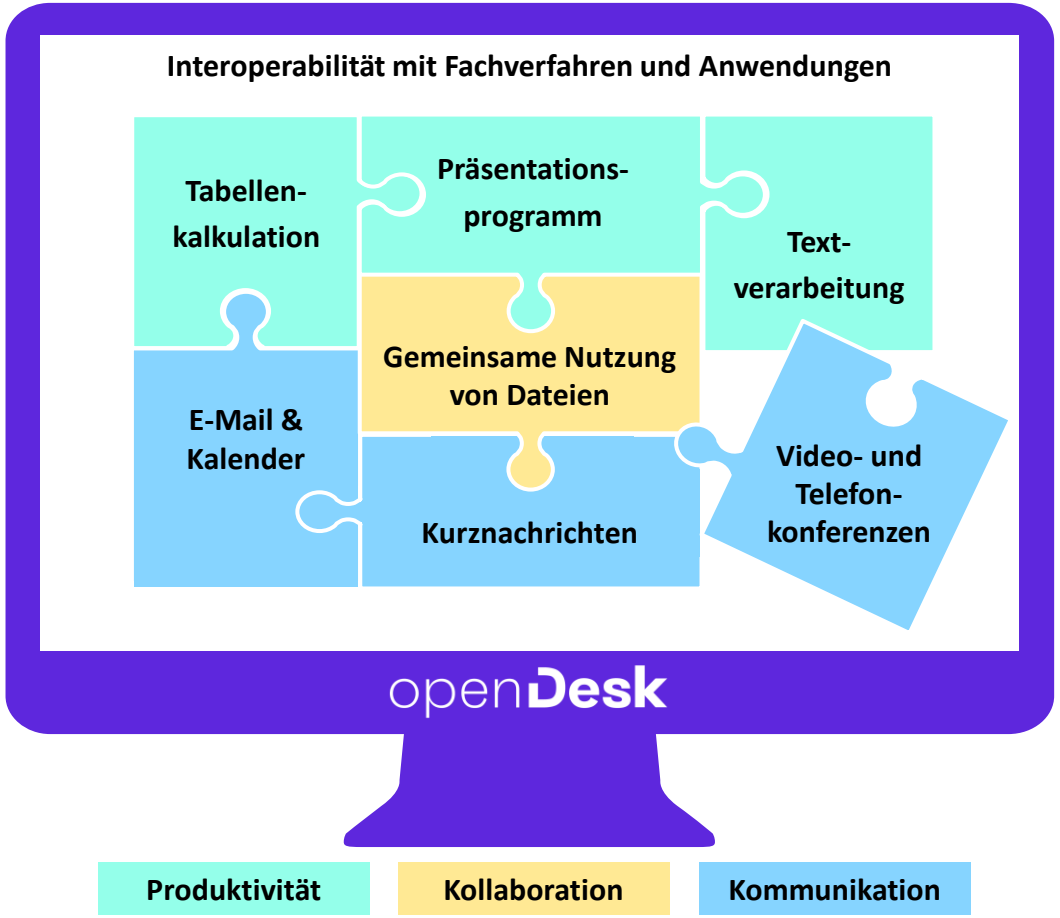
Sicher in die Cloud mit Confidential Computing

Andreas Reckert-Lodde
Dr. Felix Schuster
Dr. Dietmar Wippig

openDesk

Ein souveräner digitaler Arbeitsplatz für die ÖV

- Einsatz von Open Source
- Offene Standards und Schnittstellen
- Modularität, Austauschbarkeit und Interoperabilität
- Betreiberunabhängigkeit
- IT-Grundschutz
- Integration der Komponenten



- Nutzung auf mobilen Endgeräten
- Barrierefreiheit
- Einheitliches Look & Feel
- Single Sign-on
- Webanwendung
- Individualisierbares Design

Roadmap
Planung 2024

April - Juni | Juli -September | Oktober – Dezember

Übernahme openDesk

- Beauftragung durch das BMI
- Aufbau Erprobungs- & Betriebsumgebung
- Aufstellen der Roadmap für 2024
- Ausschreibung Rahmenvertrag

Entwicklung v1

- Erarbeitung notwendiger Komponenten
- Aufsetzen von Dokumentationen
- Zuschlag RV & Ausschreibung SaaS
- Aufsetzen neuer Board-Strukturen

Bereitstellung v1

- Inbetriebnahme einer Support-Infrastruktur
- Onboarding erster openDesk-Kunden
- Weiterentwicklung von Features (ff.)

openDesk v1
Fokusthemen

	2024	**2025**
Usability	UX-Upgrade, neue Startseite, PoC openDesk-App, KI-Integration	neues ZenDiS-Portal (Intranet), Offline-Fähigkeit, Mobile App
Sicherheit	Eigenständige LuP-Infrastruktur, Kooperation mit BSI	VS-NfD-Version, Post Quantensicherheit
Skalierbarkeit	Vollständige Containerisierung, Ersatz erster Komponenten	Vereinfachung der Upgradeability, Aufbau einer Interoperabilitätssicht zur Modularität von Komponenten
Support & Dokumentation	Aufbau Support-Infrastruktur, Betriebsdokumentation, Anwender-Doku	Trainings für Anwender

openDesk
Confidential Cloud

Warum ist es notwendig?

- Public Cloud ermöglicht hohe Skalierbarkeit
- Garantiert Erreichbarkeit von diversen (inter-)nationalen Standorten aus
- Daten dürfen jedoch zu keinem Zeitpunkt entschlüsselt werden

Der Lösungsweg:

- Confidential Cloud bei einem (inter-)nationalen Hyperscaler
- Gemeinsames Pilotprojekt mit Edgeless Systems & dem BSI

Weitere openDesk Versionen:

Community Edition

Enterprise

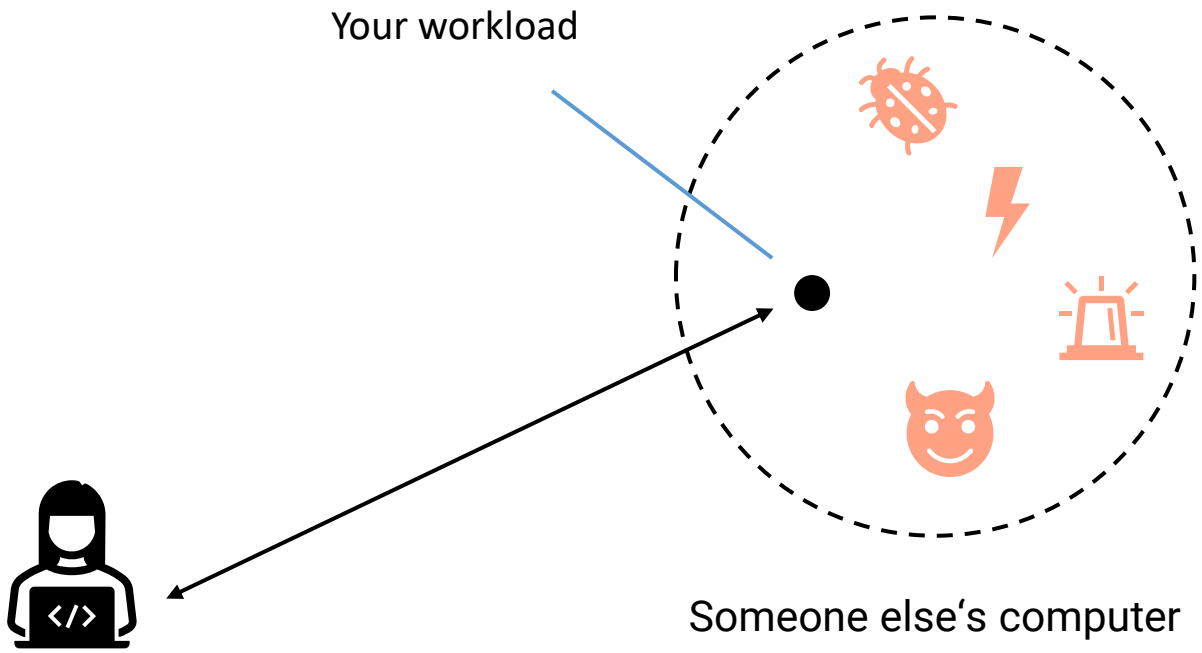
Secure

Edgeless Systems

Confidential Computing

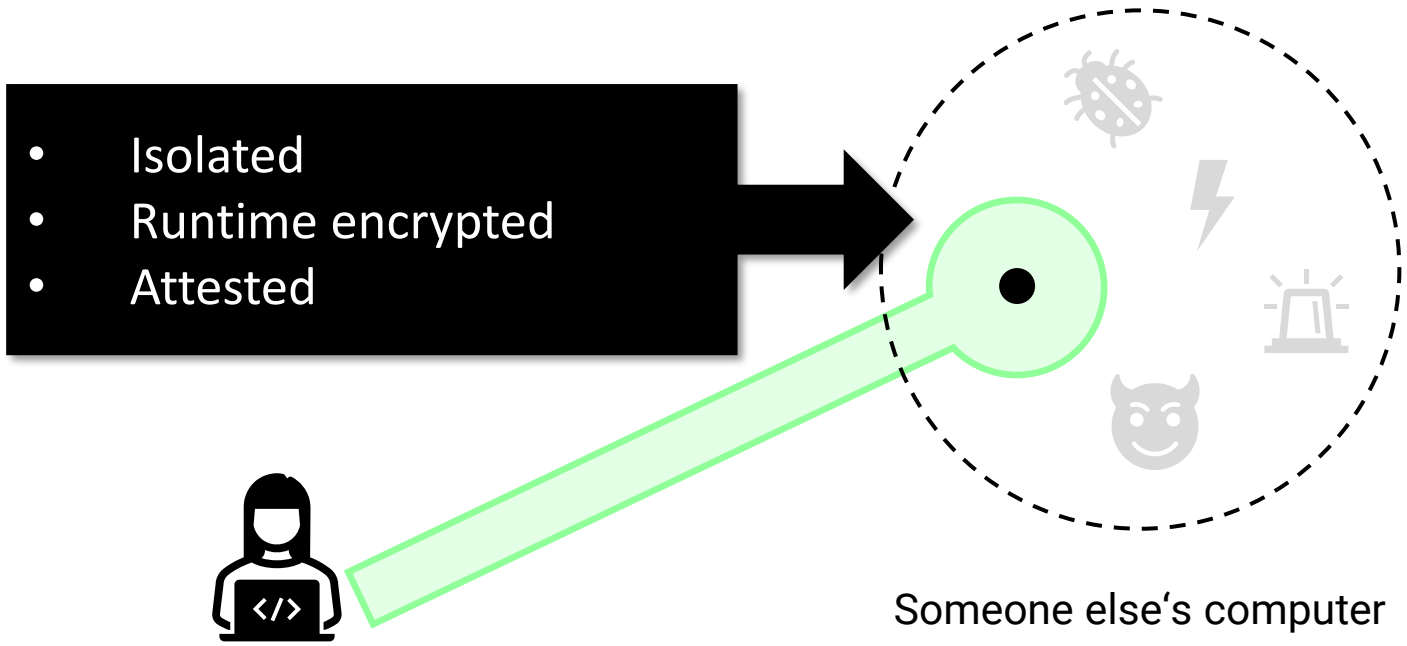
Edgeless Systems

Wie können Daten auf Infrastruktur dritter verarbeitet werden?



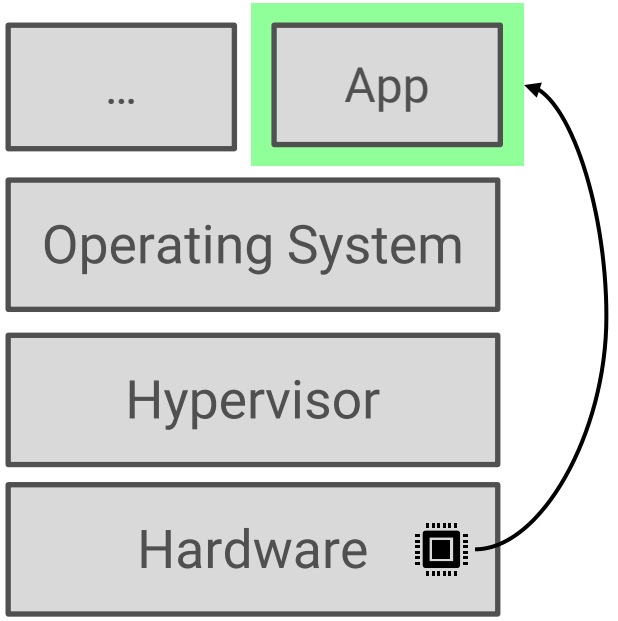
Edgeless Systems

Wie können Daten auf Infrastruktur dritter verarbeitet werden?



Edgeless Systems

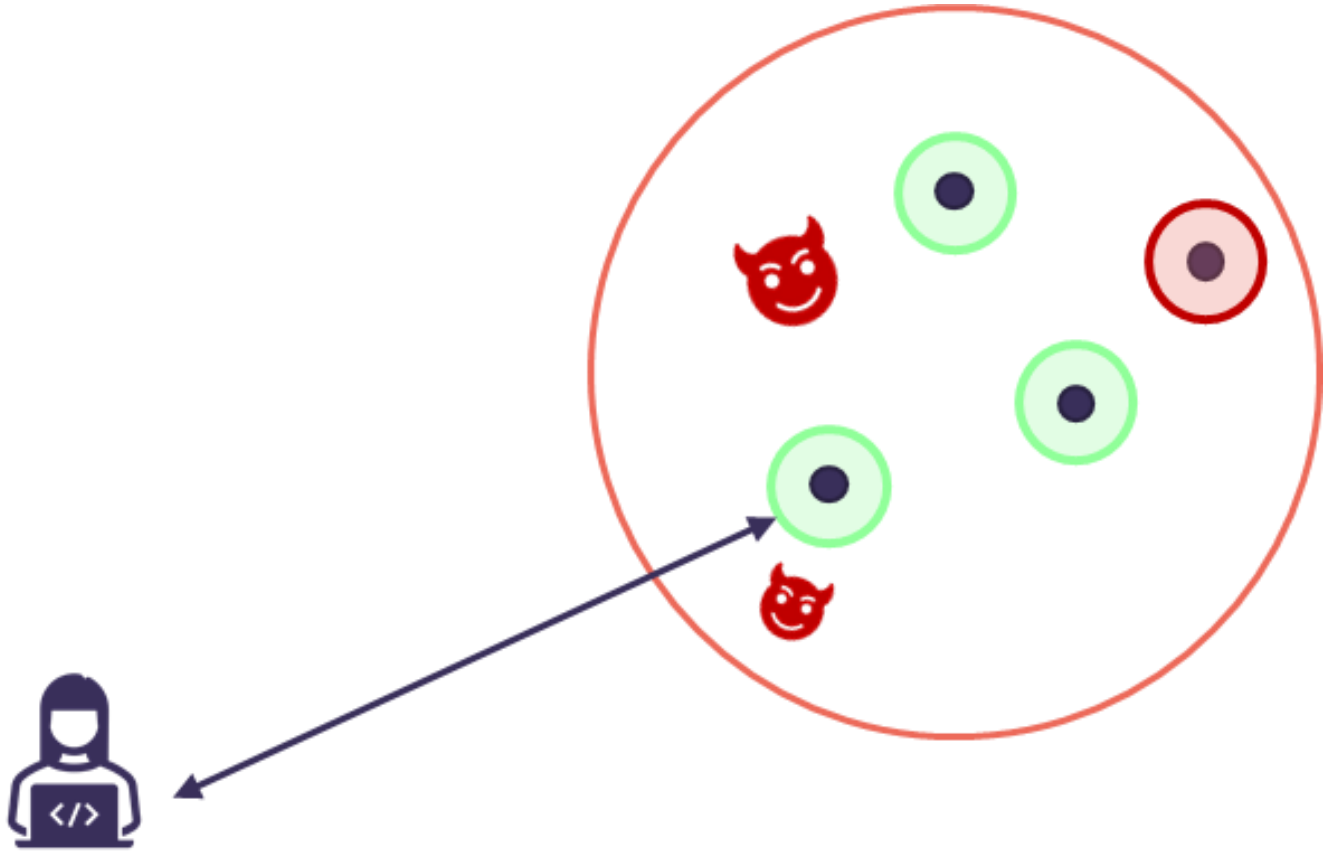
Grundbaustein: Sichere Enklaven



CPU creates and enforces enclave

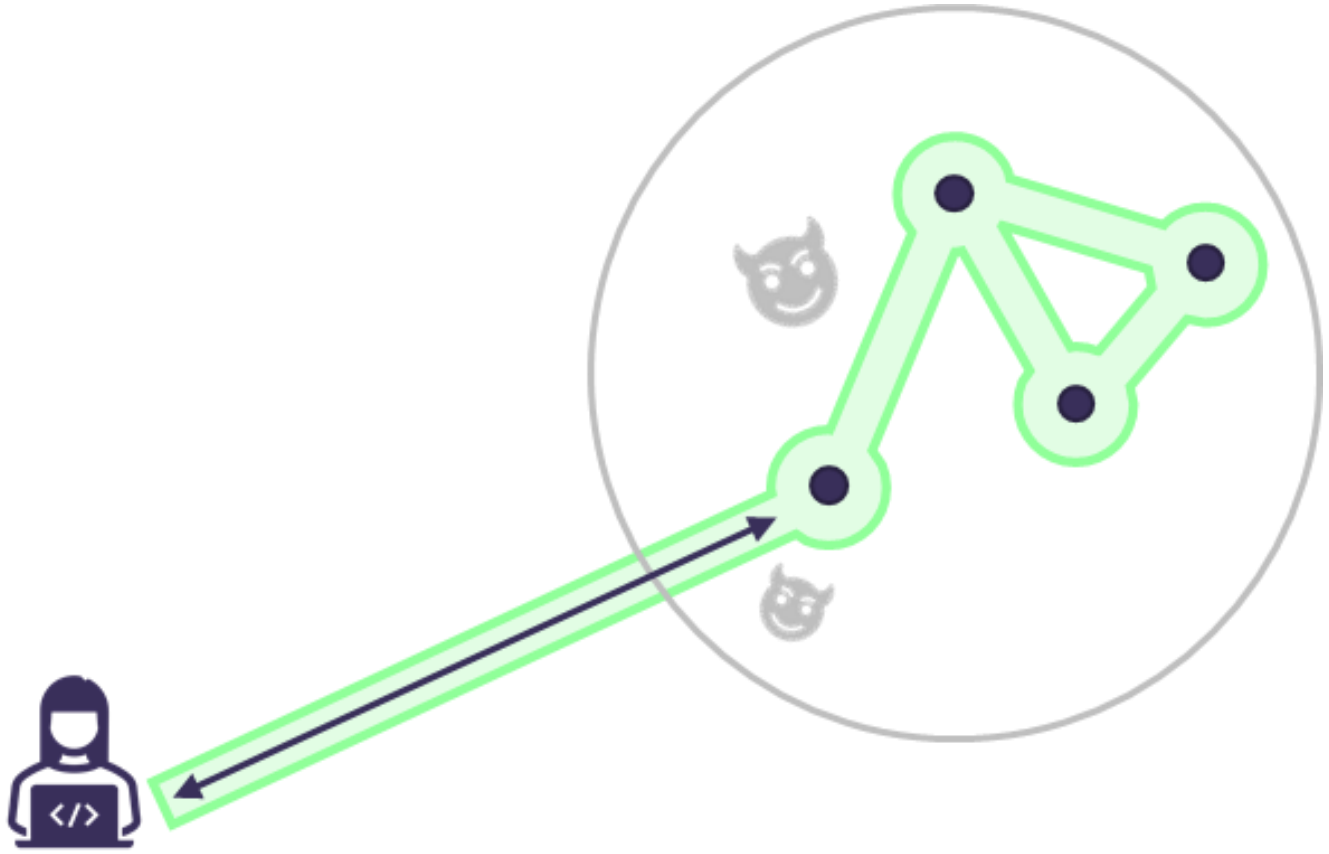
Edgeless Systems

Confidential Computing muss Ende-zu-Ende eingesetzt werden



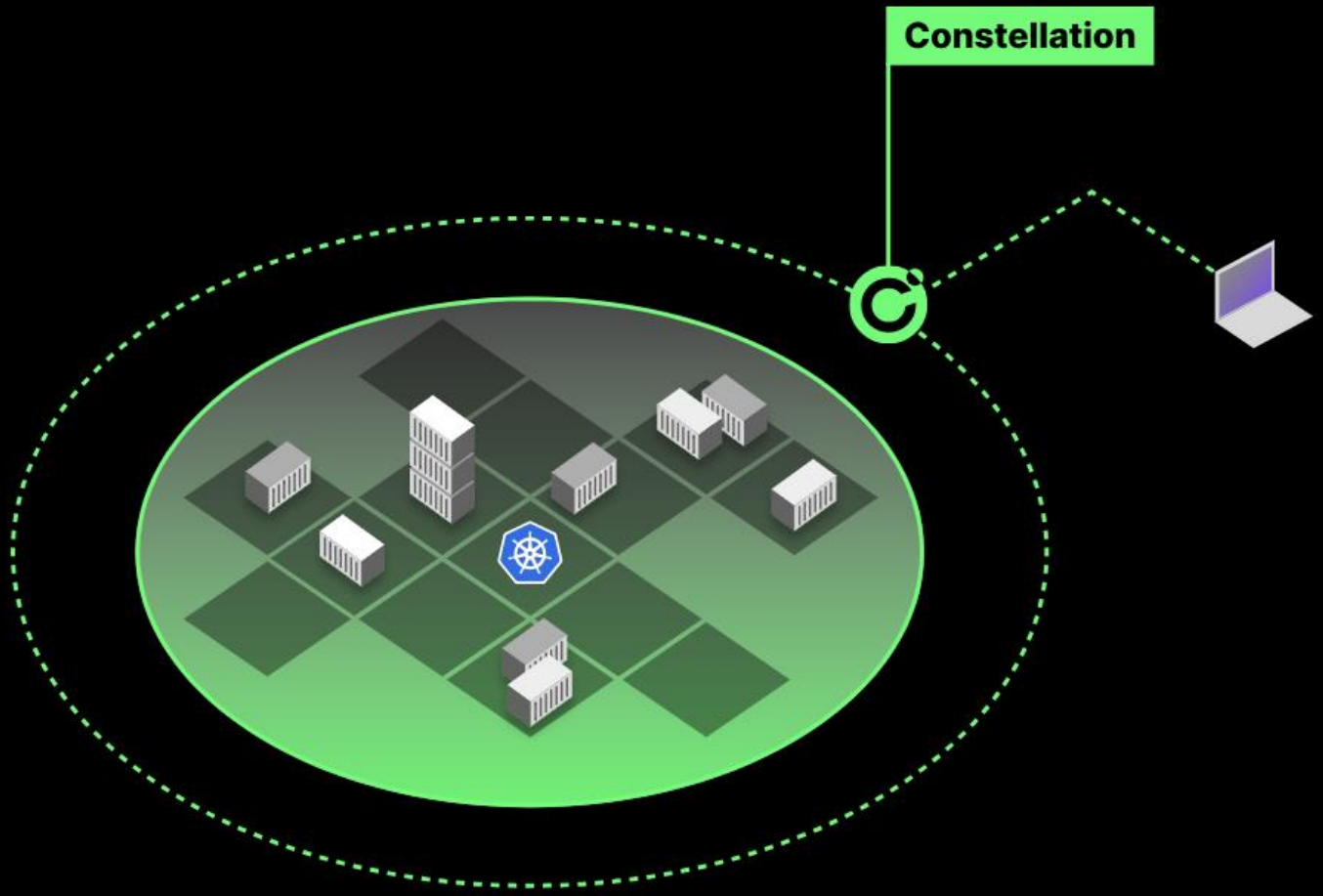
Edgeless Systems

Confidential Computing muss Ende-zu-Ende eingesetzt werden



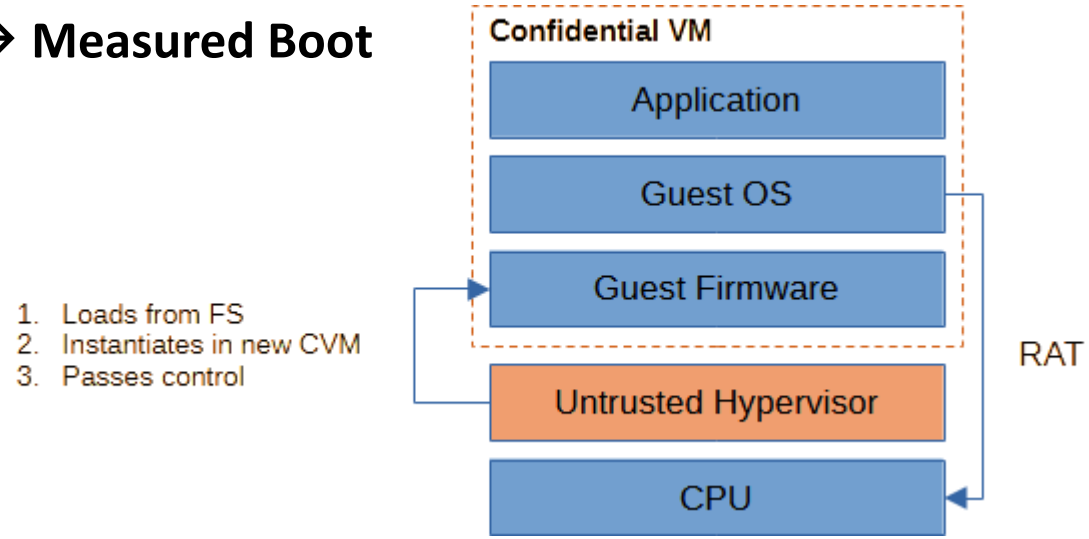
Edgeless Systems

Confidential Computing muss Ende-zu-Ende eingesetzt werden



Transparency of the whole stack

- A trusted **processor** is **not sufficient**. You also need:
  - Secure and verifiable **Firmware** inside your Confidential VM
  - Confidence that the correct firmware is running → **Measured Boot**



Transparency Features of Clouds

Feature	Azure	GCP	AWS	STACKIT	OpenStack
Access to raw attestation statements					
Verifiable firmware inside CVMs					
Measured Boot (HV not in TCB)					

Source: https://docs.edgeless.systems/constellation/overview/clouds

 = available

 = not available / not sufficient

 = depends on configuration

Current State of Cooperation

- Edgeless will provide a test environment running Constellation to BSI
- BSI will challenge Edgeless to provide …
  - Full transparency about what is running below Constellation
  - Non-ambiguous and complete documentation about the product itself and the guarentees (not) given in combination with different cloud stacks

18.06.2024