State of Affairs:

Confidential Computing on OpenStack

fkr@osb-alliance.com

Sovereign Cloud Stack

Only Open Source guarantees digital sovereignty by interoperability, transparency and independence from unlawful claims of third parties and thus from any unauthorised interference.

Sovereign
Cloud Stack

Why do ~~I~~ you need a *Trusted Execution Environment* in a Cloud Environment?

I am root

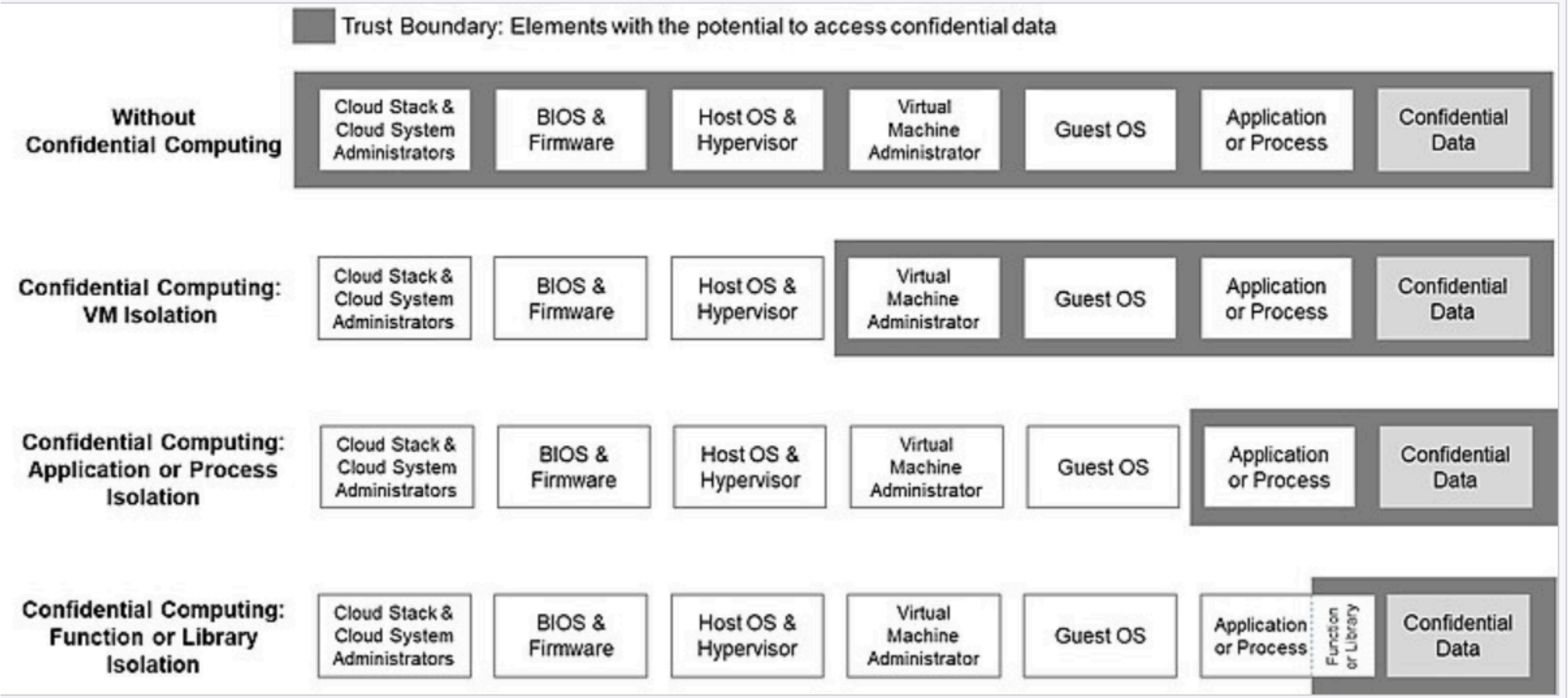
Sovereign Cloud Stack

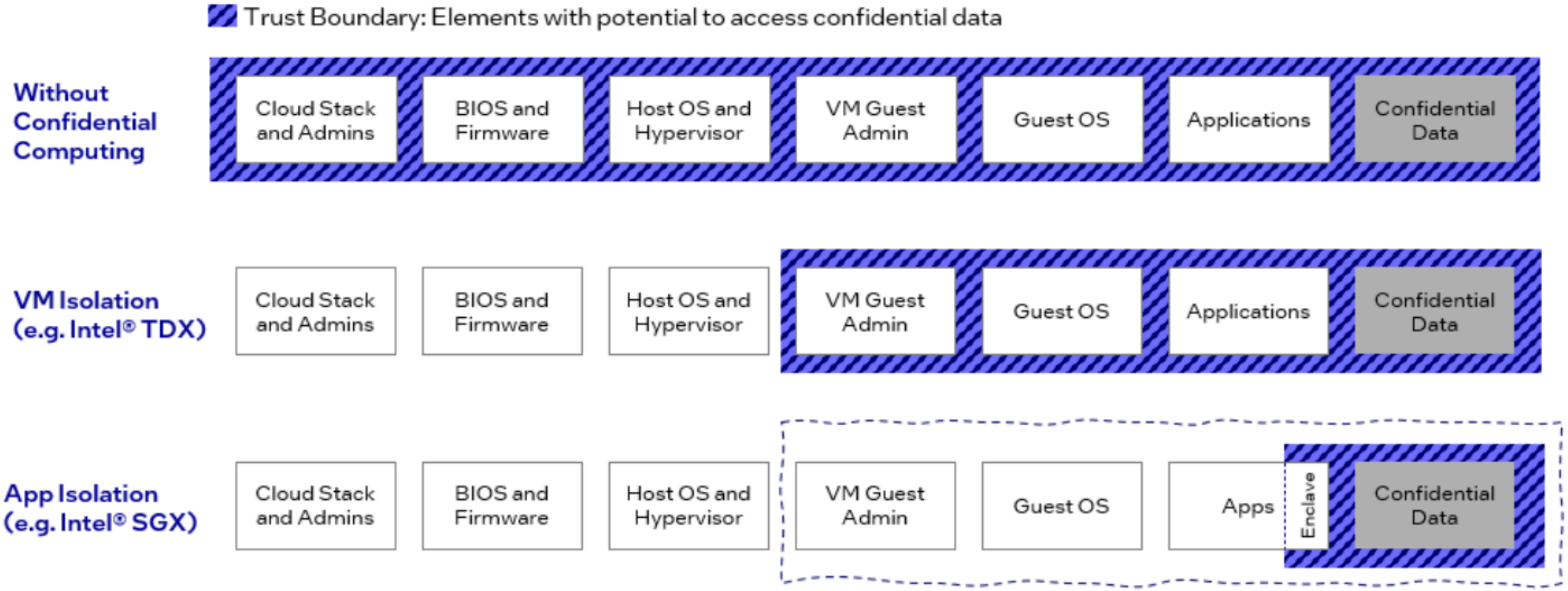
Why do I *want* Confidential Computing?

Sovereign
Cloud Stack

Technology available

- Intel SGX
- Intel TDX
- AMD SEV/SEV-SNP
- ARM TrustZone
- IBM Secure Execution
- RISC-V TSM


Trust Boundary: Elements with the potential to access confidential data
Without Confidential Computing
Confidential Computing: VM Isolation
Confidential Computing: Application or Process Isolation
Confidential Computing: Function or Library Isolation
Cloud Stack & Cloud System Administrators
BIOS & Firmware
Host OS & Hypervisor
Virtual Machine Administrator
Guest OS
Application or Process
Function or Library
Confidential Data



▨ Trust Boundary: Elements with potential to access confidential data

Without Confidential Computing

Cloud Stack and Admins | BIOS and Firmware | Host OS and Hypervisor | VM Guest Admin | Guest OS | Applications | Confidential Data

VM Isolation (e.g. Intel® TDX)

Cloud Stack and Admins | BIOS and Firmware | Host OS and Hypervisor | VM Guest Admin | Guest OS | Applications | Confidential Data

App Isolation (e.g. Intel® SGX)

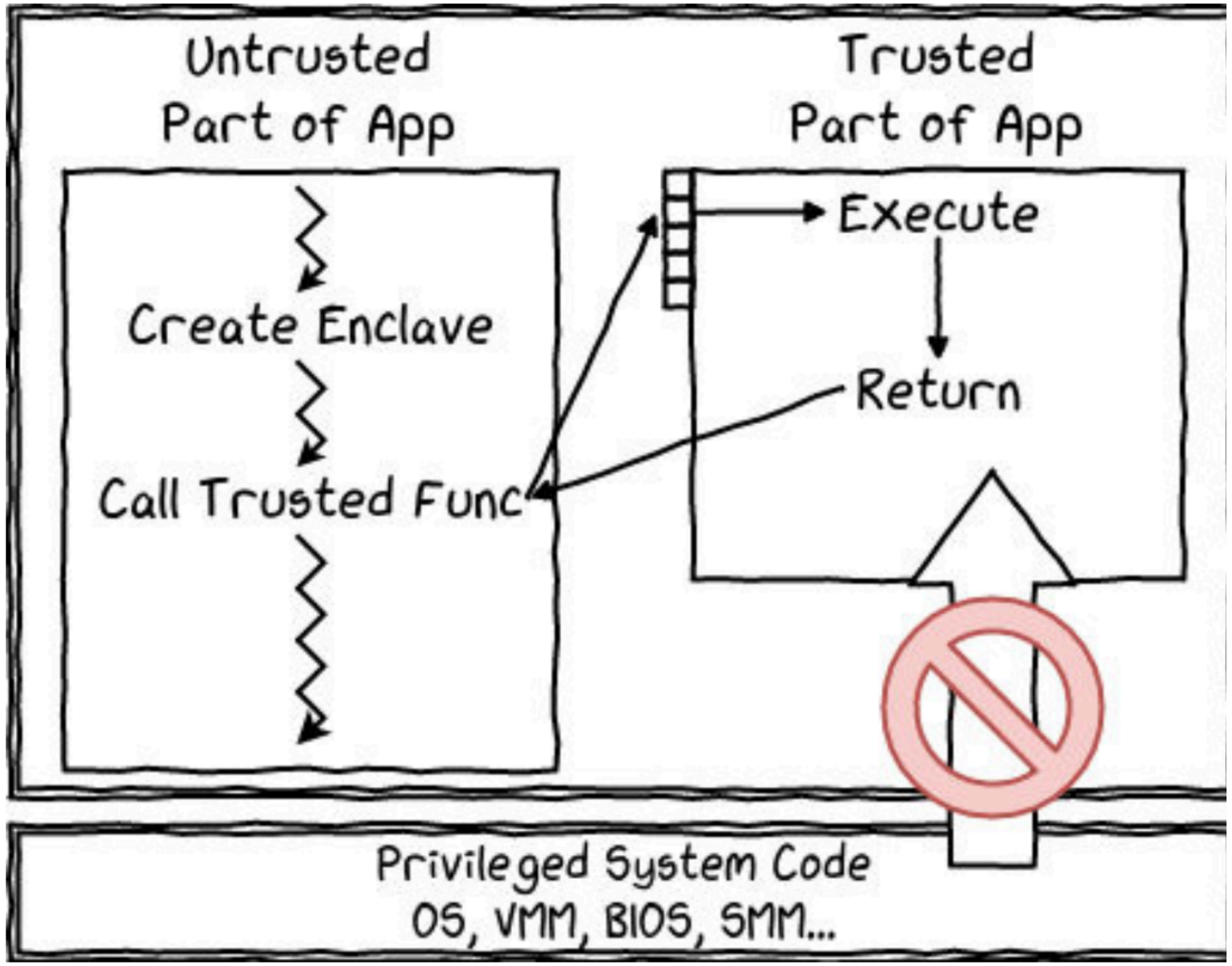
Cloud Stack and Admins | BIOS and Firmware | Host OS and Hypervisor | VM Guest Admin | Guest OS | Apps | Enclave | Confidential Data

Intel SGX

Software Guard Extensions

Protected private regions of memory: enclaves

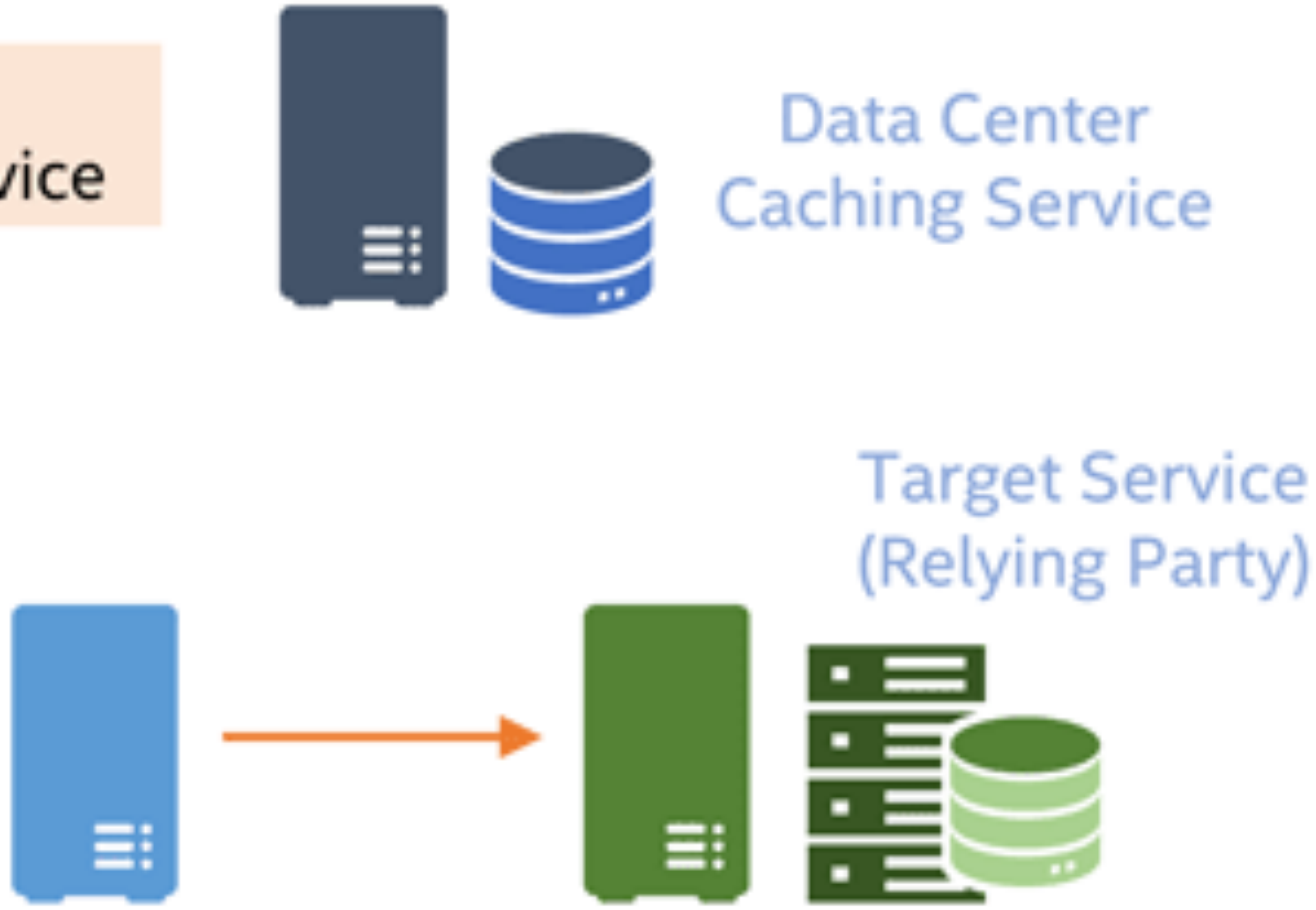
Process-based TEE



Sovereign Cloud Stack

Intel® SGX ECDSA Attestation

Step 1:
Workload contacts service



Data Center Caching Service

Target Service (Relying Party)

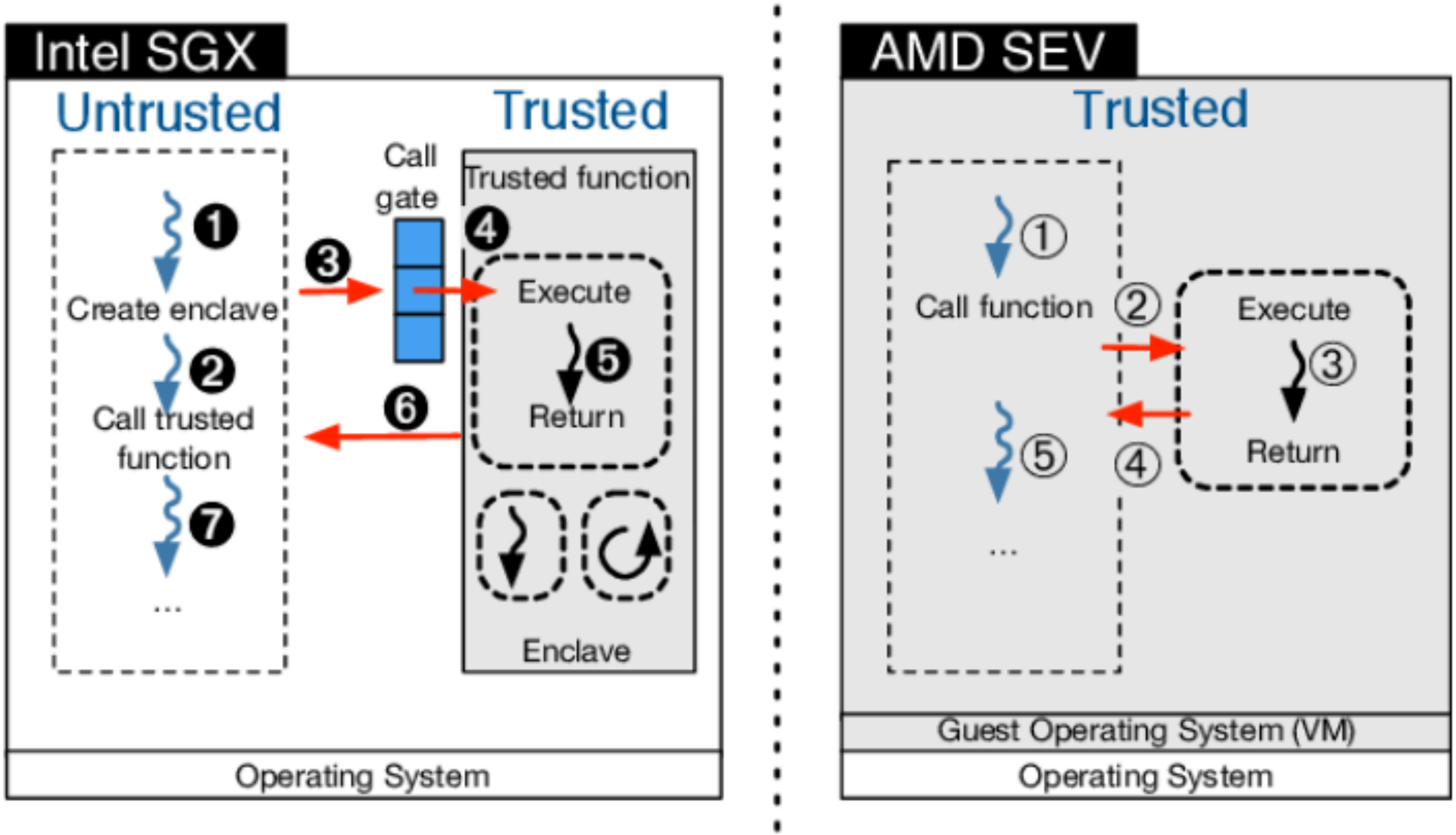
Intel SGX-Enabled Platform

AMD SEV-SNP

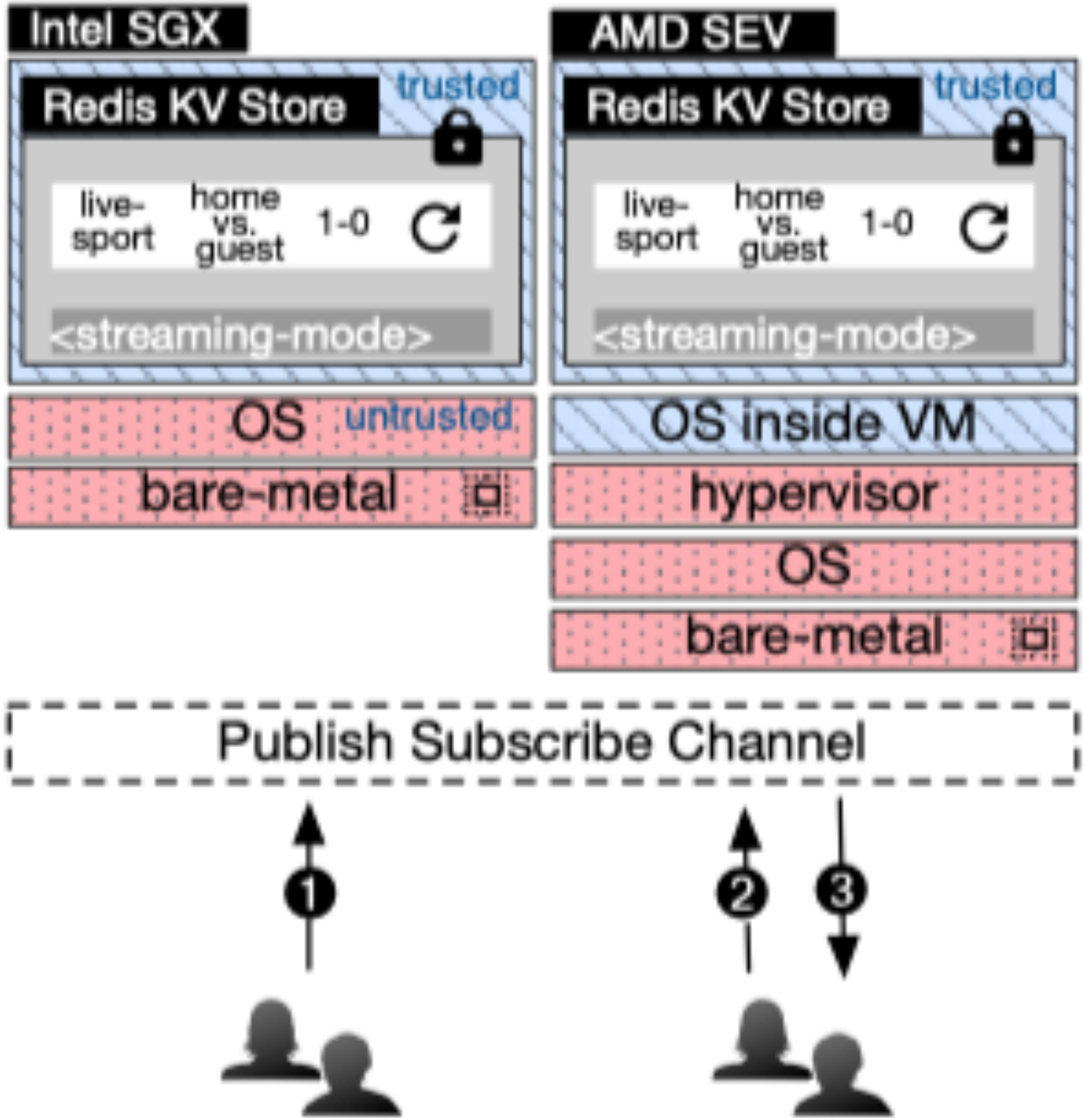
Secure Encrypted Virtualization

Secure Nested Paging

Virtual-Machine-based TEE



Sovereign Cloud Stack

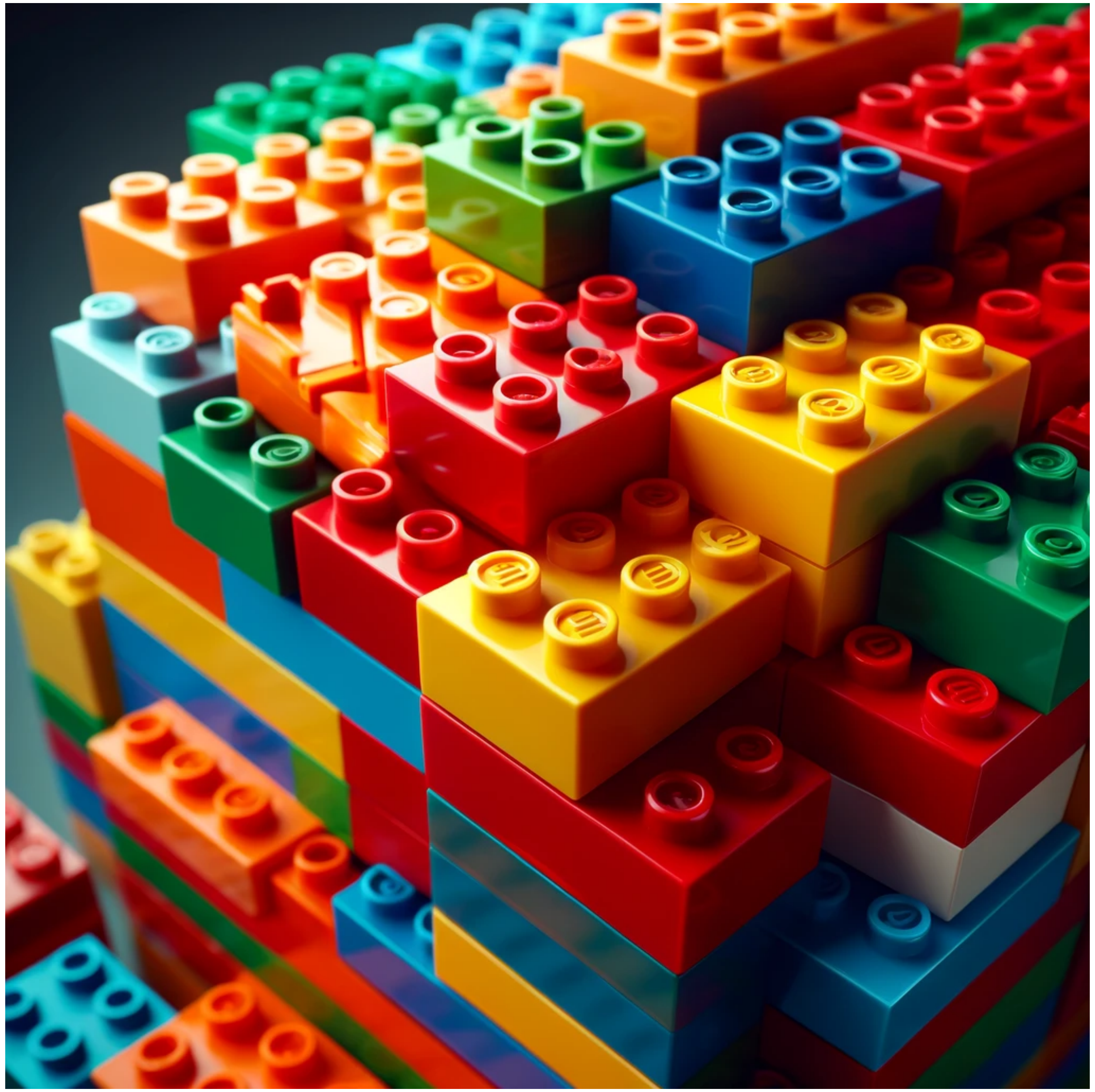

Intel SGX
AMD SEV
Redis KV Store
trusted
live-sport
home vs. guest
1-0
<streaming-mode>
Redis KV Store
trusted
live-sport
home vs. guest
1-0
<streaming-mode>
OS
untrusted
bare-metal
OS inside VM
hypervisor
OS
bare-metal
Publish Subscribe Channel
①
②
③

TDX

Trust Domain Extension

Virtual-Machine-based TEE

OSS Support



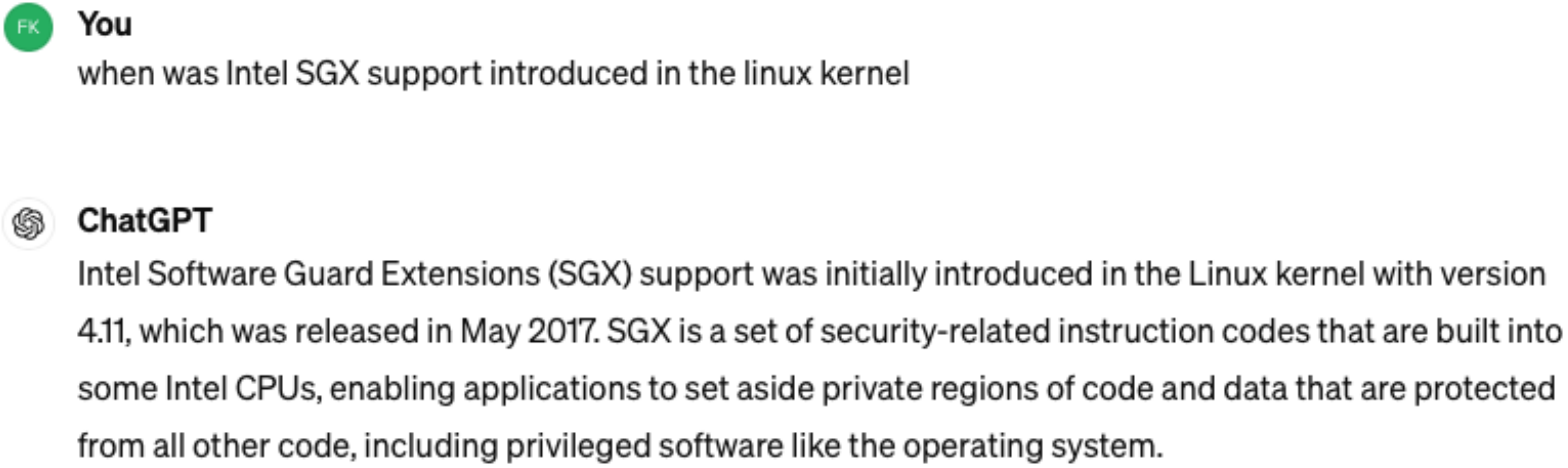
Sovereign
Cloud Stack

Linux

SGX since 5.11

SEV since 5.13

TDX since 5.19 (first patches, more in 6.x)



You

when was Intel SGX support introduced in the linux kernel

ChatGPT

Intel Software Guard Extensions (SGX) support was initially introduced in the Linux kernel with version 4.11, which was released in May 2017. SGX is a set of security-related instruction codes that are built into some Intel CPUs, enabling applications to set aside private regions of code and data that are protected from all other code, including privileged software like the operating system.

Qemu, Libvirt, KVM

Confidential Computing on OpenStack

Sovereign
Cloud Stack

AMD SEV

Hardware-based encryption: Nova features a new framework supporting hardware-based encryption of guest memory to protect users against attackers or rogue administrators snooping on their workloads when using the libvirt compute driver. This feature is useful for multi-tenant environments and environments with publicly accessible hardware.

OPENSTACK
TRAIN

Impermanent limitations

- no live-migration
- no suspension
- no PCI passthrough

Permanent Limitation

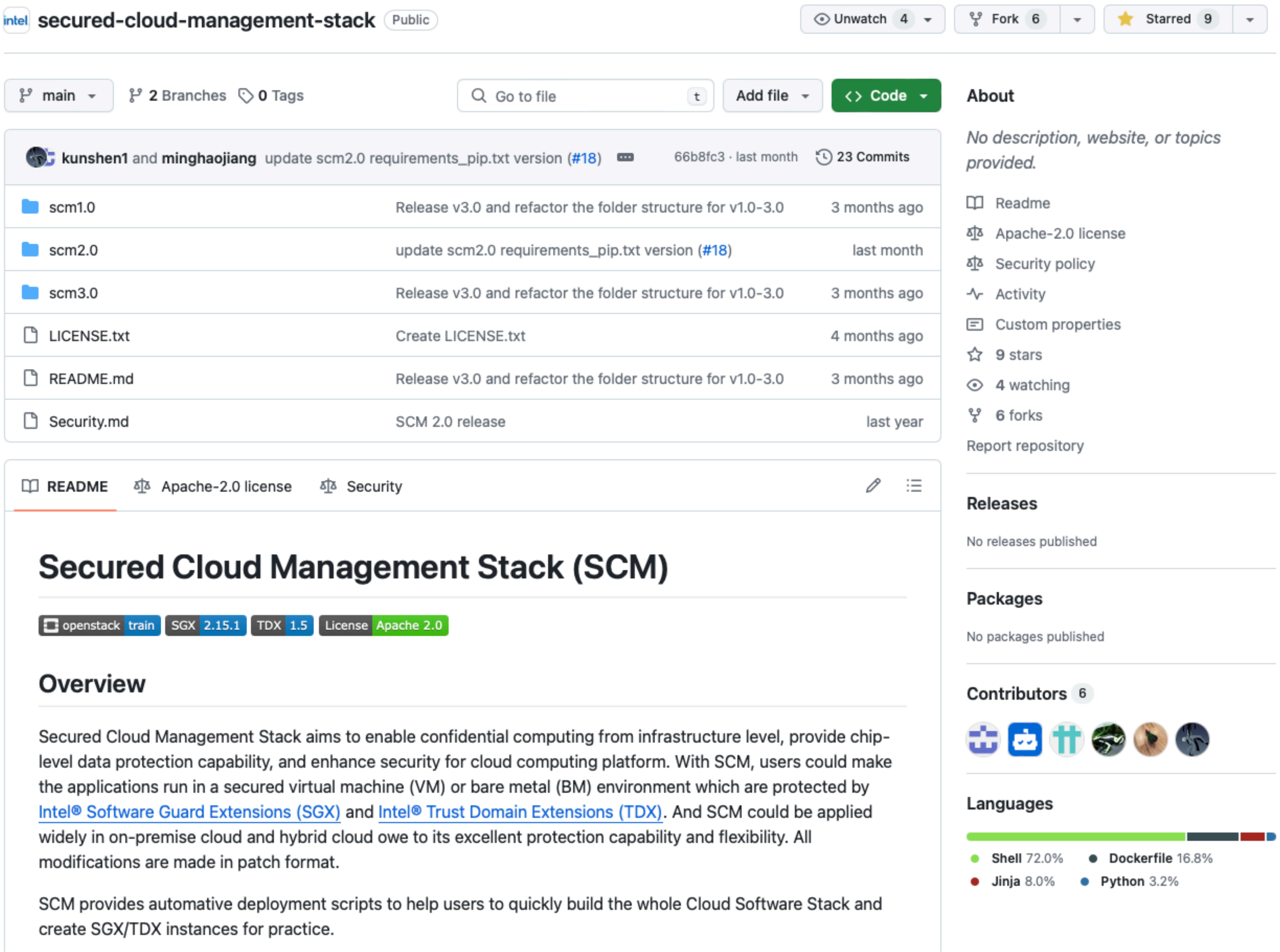
- 15 guests per hypervisor
- Guest OS needs to be SEV-capable

SGX

Timeline

Initial Work by Intel and 99cloud based on OpenStack Train

OPENSTACK
TRAIN



kunshen1 and minghaojiang update scm2.0 requirements_pip.txt version (#18) 66b8fc3 · last month 23 Commits

scm1.0	Release v3.0 and refactor the folder structure for v1.0-3.0	3 months ago
scm2.0	update scm2.0 requirements_pip.txt version (#18)	last month
scm3.0	Release v3.0 and refactor the folder structure for v1.0-3.0	3 months ago
LICENSE.txt	Create LICENSE.txt	4 months ago
README.md	Release v3.0 and refactor the folder structure for v1.0-3.0	3 months ago
Security.md	SCM 2.0 release	last year

Secured Cloud Management Stack (SCM)

Overview

Secured Cloud Management Stack aims to enable confidential computing from infrastructure level, provide chip-level data protection capability, and enhance security for cloud computing platform. With SCM, users could make the applications run in a secured virtual machine (VM) or bare metal (BM) environment which are protected by Intel® Software Guard Extensions (SGX) and Intel® Trust Domain Extensions (TDX). And SCM could be applied widely in on-premise cloud and hybrid cloud owe to its excellent protection capability and flexibility. All modifications are made in patch format.

SCM provides automative deployment scripts to help users to quickly build the whole Cloud Software Stack and create SGX/TDX instances for practice.

About

No description, website, or topics provided.

Releases

No releases published

Packages

No packages published

Contributors 6

Languages

- Shell 72.0%
- Dockerfile 16.8%
- Jinja 8.0%
- Python 3.2%

Sovereign Cloud Stack

Sovereign
Cloud Stack

One Platform - standardised, built and operated by many.

Sovereign Cloud Stack

Sovereign Cloud Stack Deliverables

Certifiable Standards

Modular Open Source Reference Implementation

Operational Knowledge

Sovereign
Cloud Stack

Supported by:

Federal Ministry
for Economic Affairs
and Climate Action

on the basis of a decision
by the German Bundestag

OSB Open Source Business
ALLIANCE
Bundesverband für digitale Souveränität e.V.

SPRIN-D

Tender 01

IaaS
Referenceimplementation

LCM / Day-2 OPS

Automated Testing of IaaS

OSISM

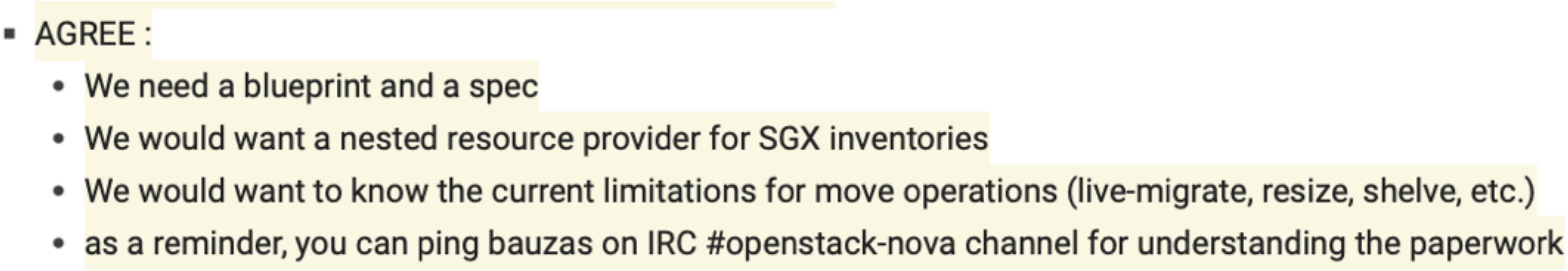
Sovereign
Cloud Stack

Back to SGX

Everything avail. in Libvirt (8.10.0), Qemu (7.0) and Kernel (5.13.0)

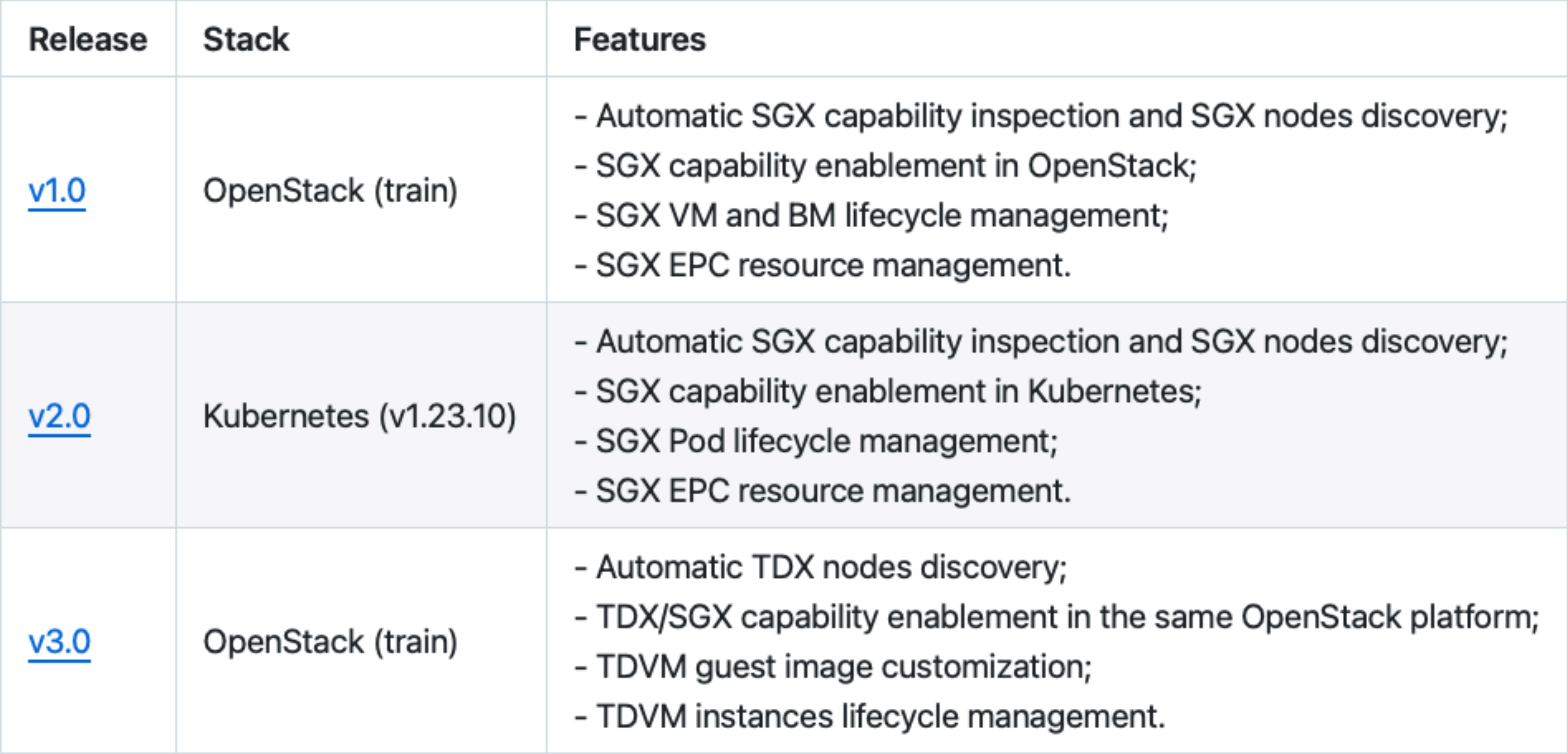
- Work done by Nils and Christian from OSISM
- Works in devstack
- Was brought to last vPTG
- Possibly replace qemu cli usage by native libvirt interface

Dalmation nova vPTG



- AGREE :
  - We need a blueprint and a spec
  - We would want a nested resource provider for SGX inventories
  - We would want to know the current limitations for move operations (live-migrate, resize, shelve, etc.)
  - as a reminder, you can ping bauzas on IRC #openstack-nova channel for understanding the paperwork

Hurdles

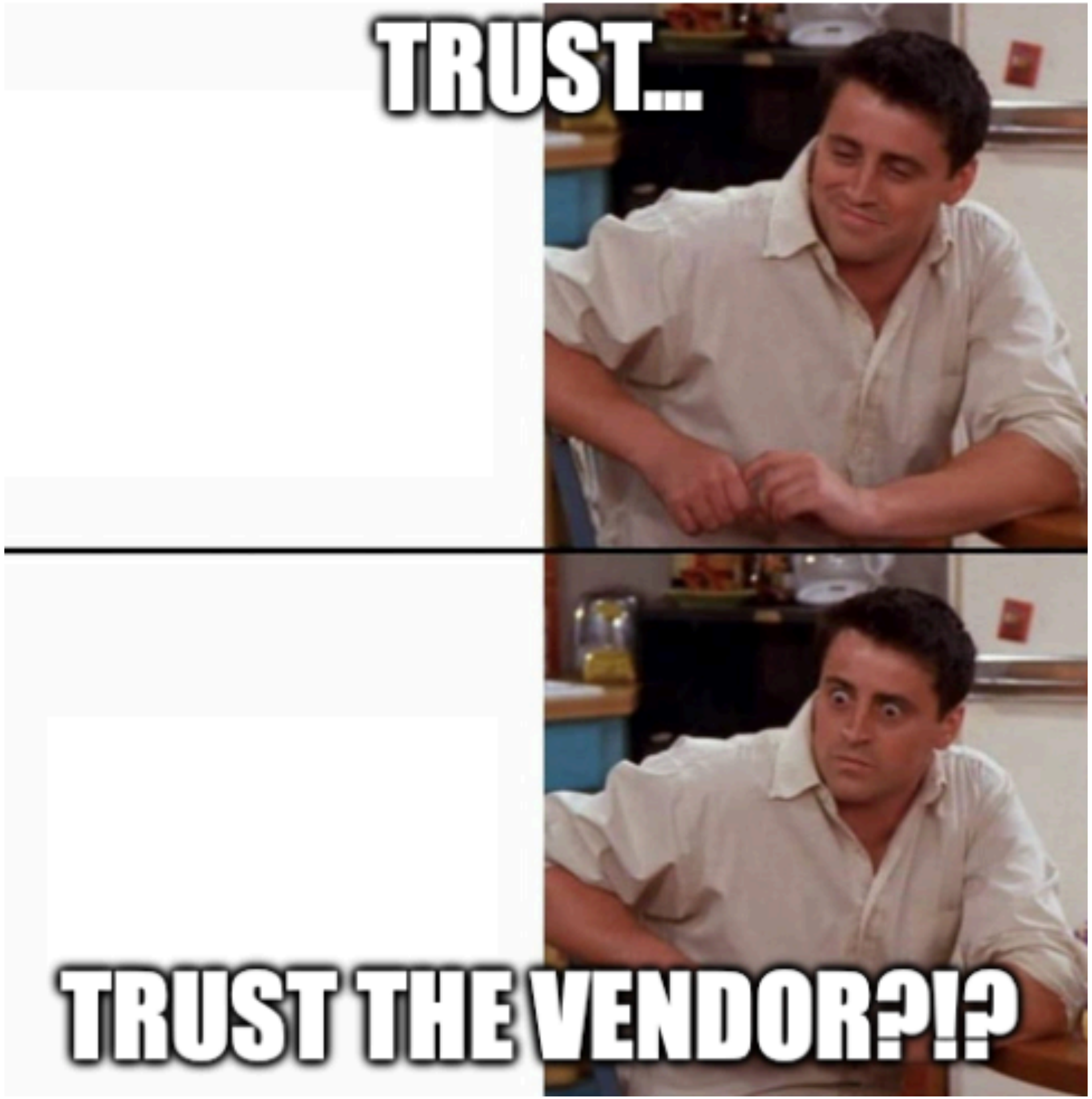


Release	Stack	Features
v1.0	OpenStack (train)	- Automatic SGX capability inspection and SGX nodes discovery; - SGX capability enablement in OpenStack; - SGX VM and BM lifecycle management; - SGX EPC resource management.
v2.0	Kubernetes (v1.23.10)	- Automatic SGX capability inspection and SGX nodes discovery; - SGX capability enablement in Kubernetes; - SGX Pod lifecycle management; - SGX EPC resource management.
v3.0	OpenStack (train)	- Automatic TDX nodes discovery; - TDX/SGX capability enablement in the same OpenStack platform; - TDVM guest image customization; - TDVM instances lifecycle management.

TDX

The one about trust

Sovereign
Cloud Stack



Sovereign Cloud Stack

CCFE
HMA

SGX Vulnerabilities

Name	Year	Description
Prime+Probe attack	2017	proof-of-concept that can grab RSA keys from SGX enclaves running on the same system within five minutes by using certain CPU instructions in lieu of a fine-grained timer to exploit cache DRAM side-channels.
Foreshadow (L1TF) - Spectre-like	2018	Allows attackers to access information in the L1 data cache.
Enclave attack	2019	possible to run malicious code from within the enclave itself. - Debatable
Plundervolt	2018 (updated: 2020)	inject timing specific faults into execution within the enclave, resulting in leakage of information.
LVI (Load Value Injection)	2020 (updated 2021)	injects data into a program aiming to replace the value loaded from memory which is then used for a short time before the mistake is spotted and rolled back
SGAxe	2020	speculative execution attack on cache, leaking content of the enclave
ÆPIC leak	2022	allows for an attacker with root/admin privileges to gain access to encryption keys via the APIC by inspecting data transfers from L1 and L2 cache
MicroScope replay attack	2022	Side-channel attack

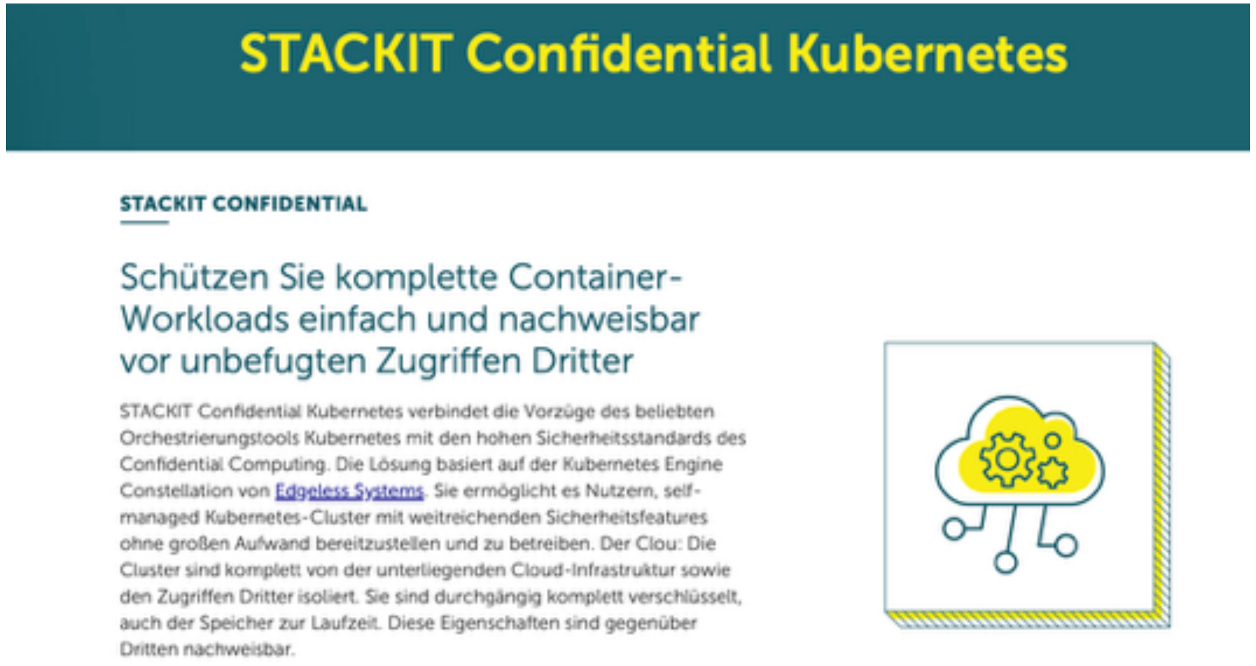
The one about digital sovereignty

DIGITAL SOVEREIGNTY
LIGHTYEAR
SPACE RANGER
DIGITAL SOVEREIGNTY EVERYWHERE

Relevance of Confidential Computing on IaaS-Level?

Confidential Kubernetes

https://www.edgeless.systems/products/constellation



STACKIT Confidential Kubernetes

STACKIT CONFIDENTIAL

Schützen Sie komplette Container-Workloads einfach und nachweisbar vor unbefugten Zugriffen Dritter

STACKIT Confidential Kubernetes verbindet die Vorzüge des beliebten Orchestrierungstools Kubernetes mit den hohen Sicherheitsstandards des Confidential Computing. Die Lösung basiert auf der Kubernetes Engine Constellation von Edgeless Systems. Sie ermöglicht es Nutzern, self-managed Kubernetes-Cluster mit weitreichenden Sicherheitsfeatures ohne großen Aufwand bereitzustellen und zu betreiben. Der Clou: Die Cluster sind komplett von der unterliegenden Cloud-Infrastruktur sowie den Zugriffen Dritter isoliert. Sie sind durchgängig komplett verschlüsselt, auch der Speicher zur Laufzeit. Diese Eigenschaften sind gegenüber Dritten nachweisbar.

Sovereign Cloud Stack

Thanks :)
Questions?

Sovereign
Cloud Stack

https://scs.community/
fkr@osb-alliance.com

Sovereign
Cloud Stack