Attestation Flow in IBM Secure Execution for Linux

Steffen Eiden
Software Engineer
Linux on IBM Z & KVM Development
steffen.eiden@ibm.com

Agenda

IBM Secure Execution

Run confidential workloads securely in a public, private, or hybrid cloud.

Explicit Attestation

Prove that a workload is secured with IBM Secure Execution

Agenda

IBM Secure Execution

Overview

Run confidential workloads securely in a public, private, or hybrid cloud.

Explicit Attestation

Prove that a workload is secured with IBM Secure Execution

IBM Secure Execution for Linux

Overview

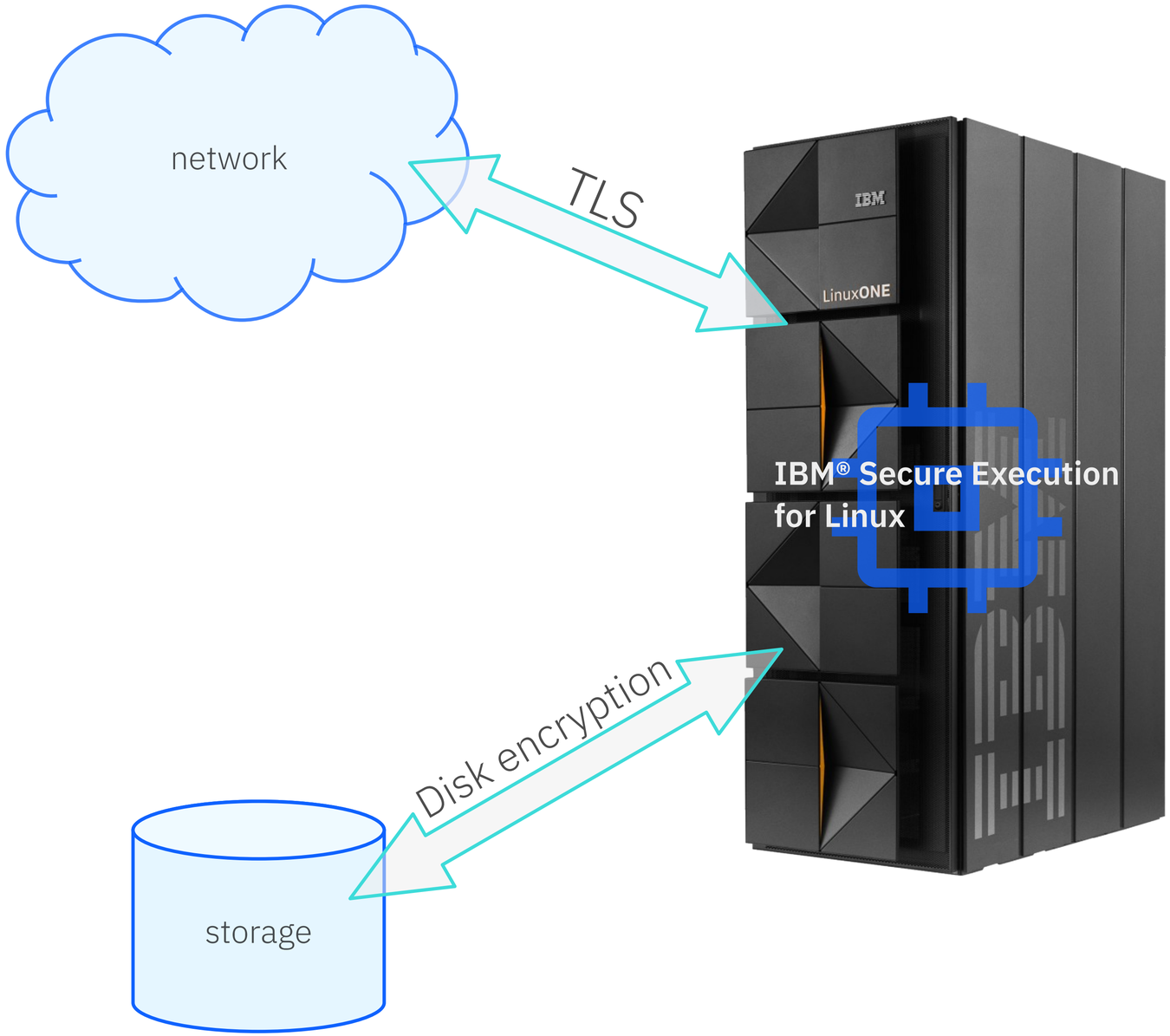
IBM Secure Execution

Protects data **in use** against malicious hypervisors

Requires

IBM z15/ Linux ONE III

IBM z16/ Linux ONE 4



IBM Secure Execution for Linux

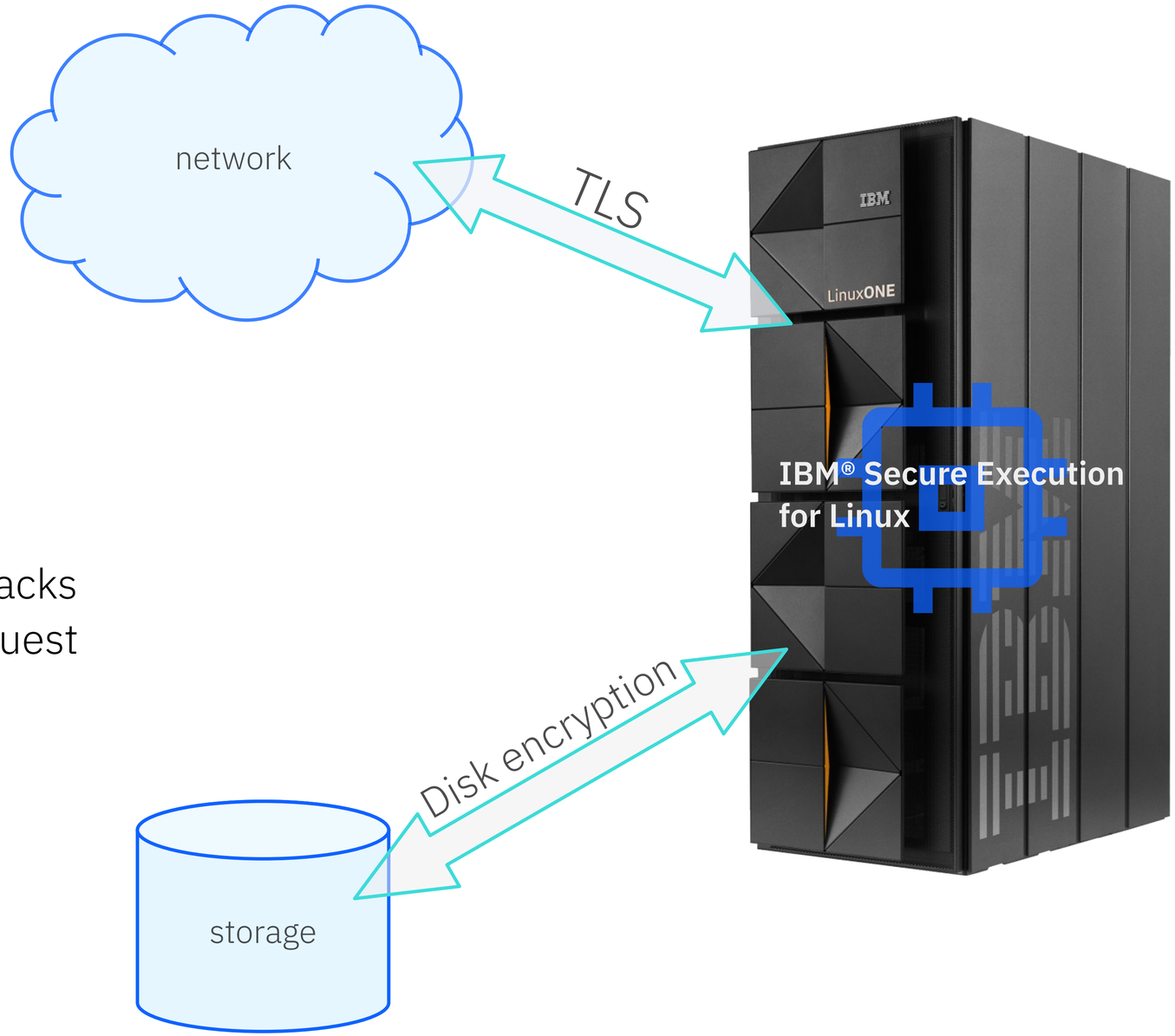
Thread model

Prevents

hosts from accessing or modifying the state of secure guests

Does not prevent

Denial of Service attacks
Bugs in the secure guest



IBM Secure Execution for Linux
Availability

Base features (IBM z15/ Linux ONE III)
2020

Encrypted image

Swapping/Memory over-provisioning

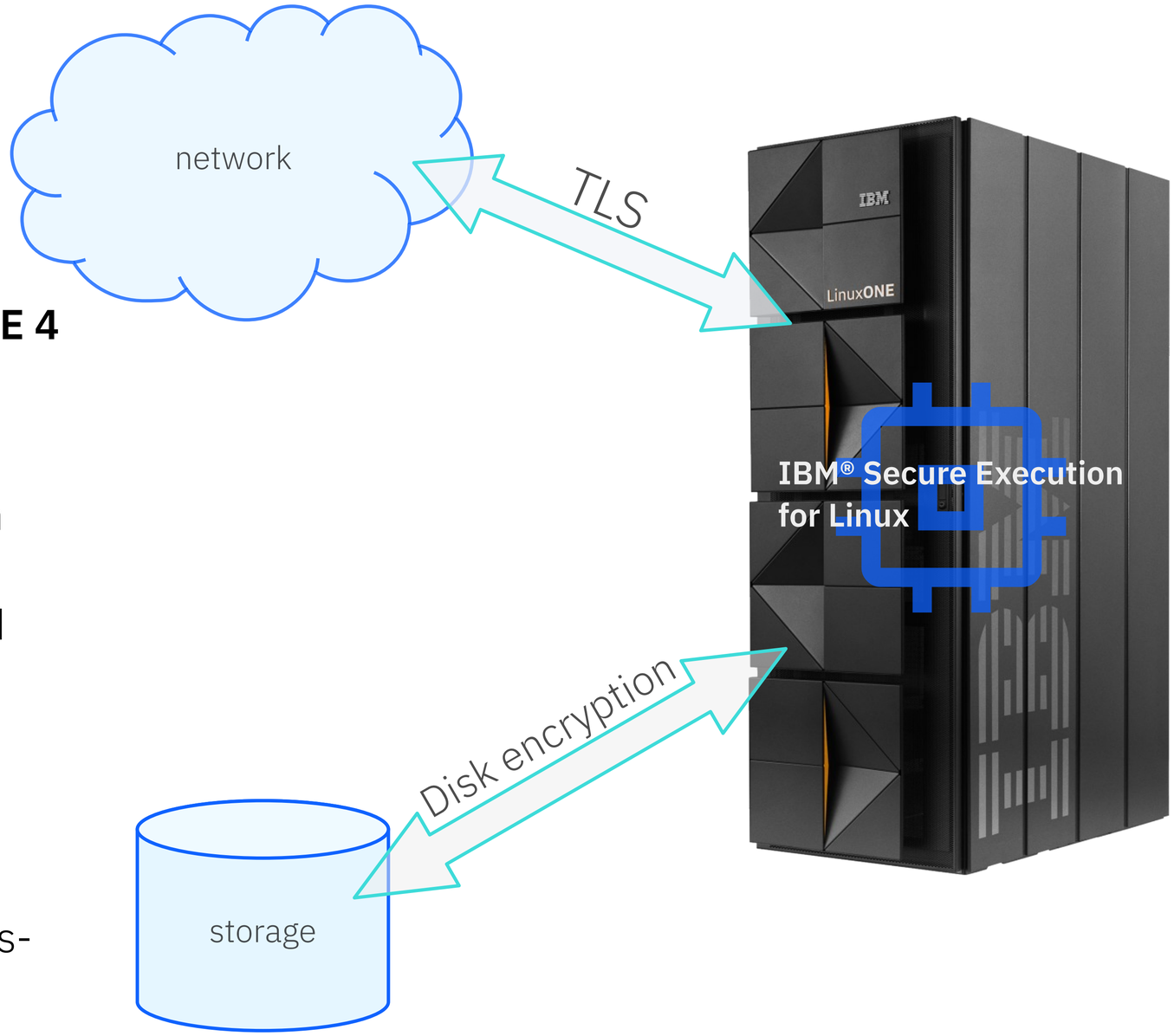
IBM z16/Linux ONE 4 features
2022

Remote Attestation

Hypervisor initiated Dump

2024
TCB secret-store

Crypto adapter pass-through



IBM Secure Execution for Linux
Availability

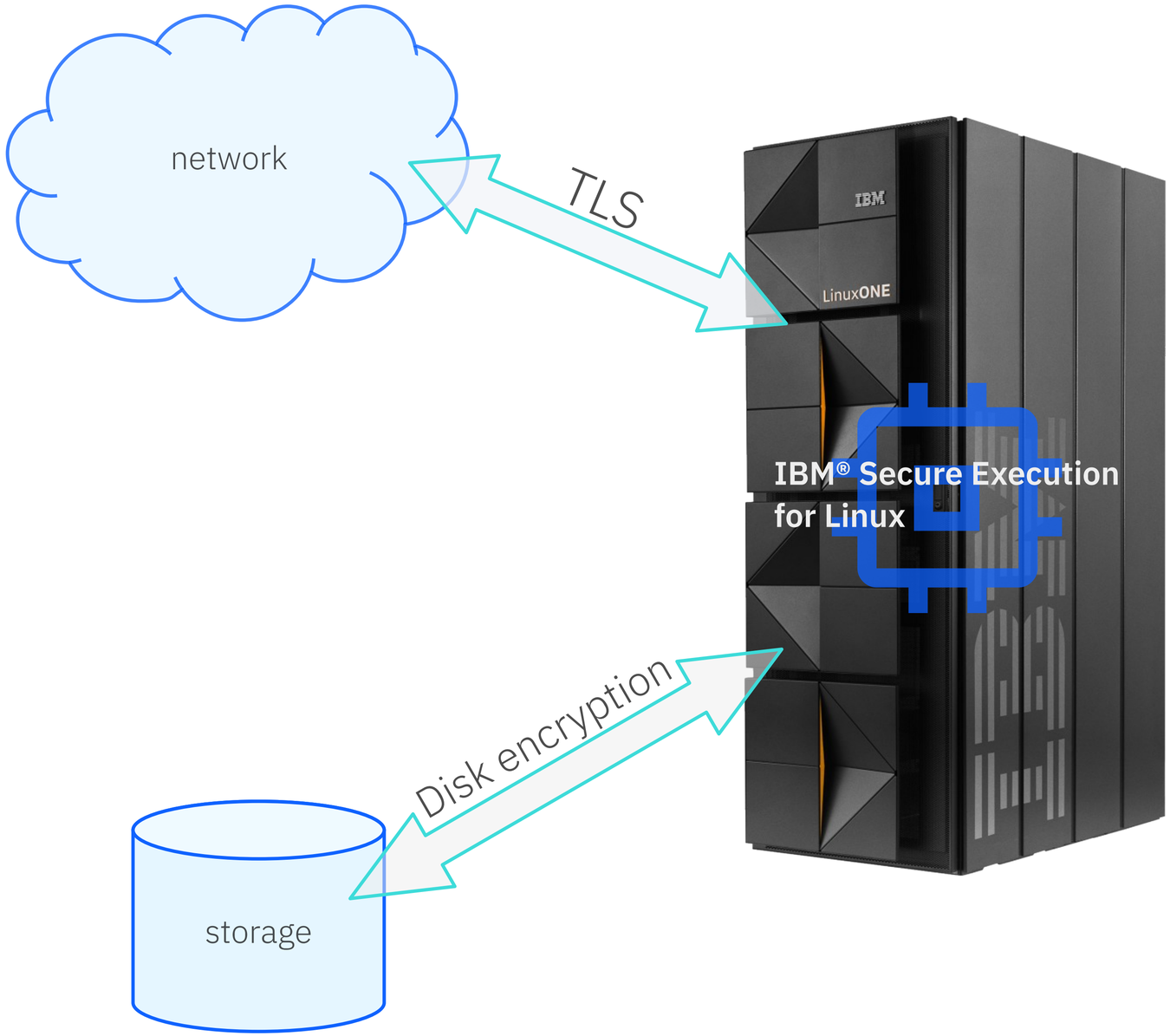
IBM Secure Execution

KVM+QEMU in distributions
Red Head Enterprise Linux, Ubuntu, SLES, Fedora

Confidential containers
enabled + maintained *March 2023*
showcase

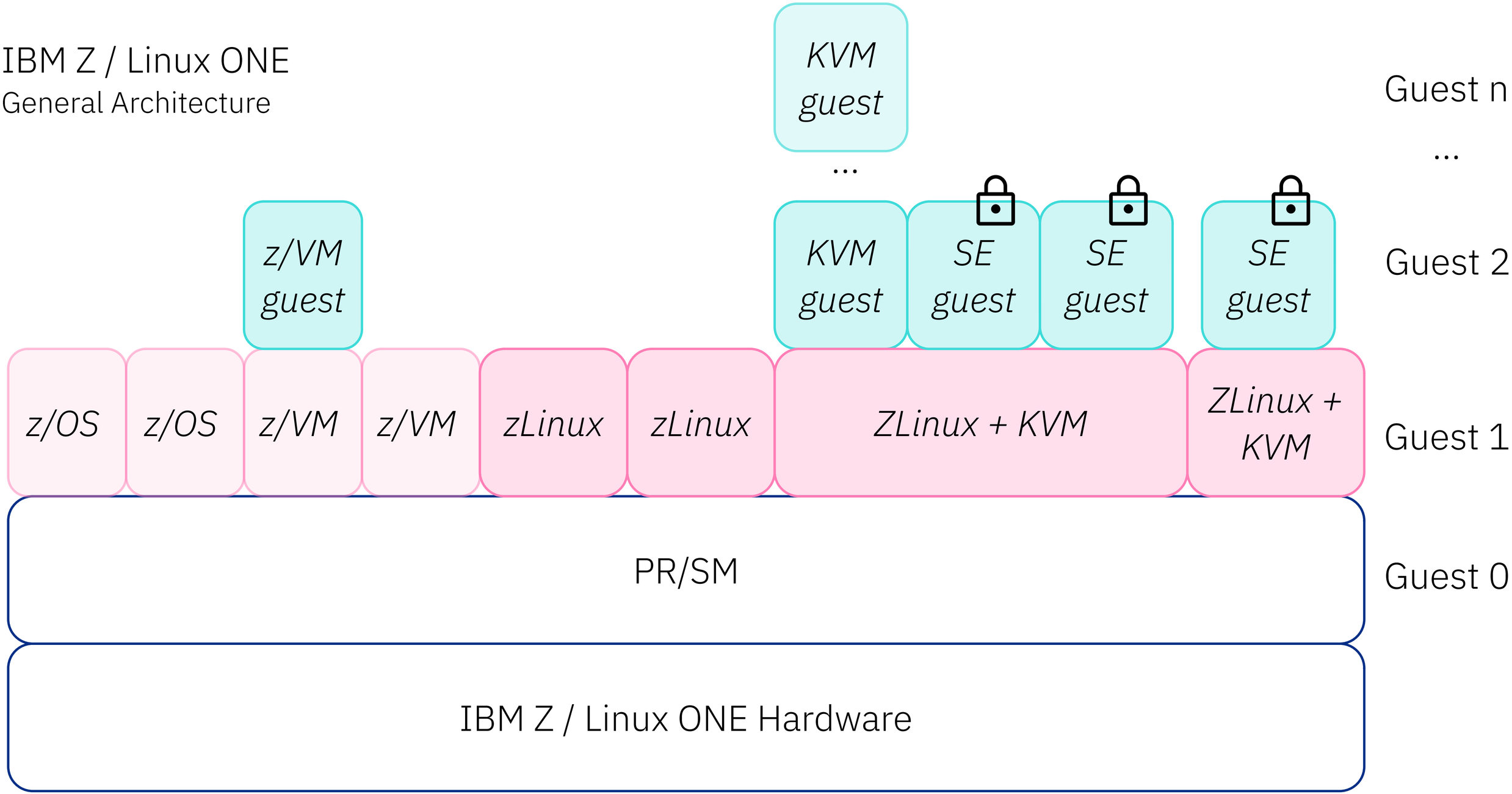
IBM Cloud
Hyper Protect Virtual Servers

Red Hat OpenShift Container Platform



IBM Z / Linux ONE

General Architecture



Agenda

IBM Secure Execution

Concepts

Run confidential workloads securely in a public, private, or hybrid cloud.

Explicit Attestation

Prove that a workload is secured with IBM Secure Execution

IBM Secure Execution for Linux

Concepts

Each physical machine is associated with a host public key, with the private key only accessible to hardware and firmware

Client encrypts the image with certified host public keys

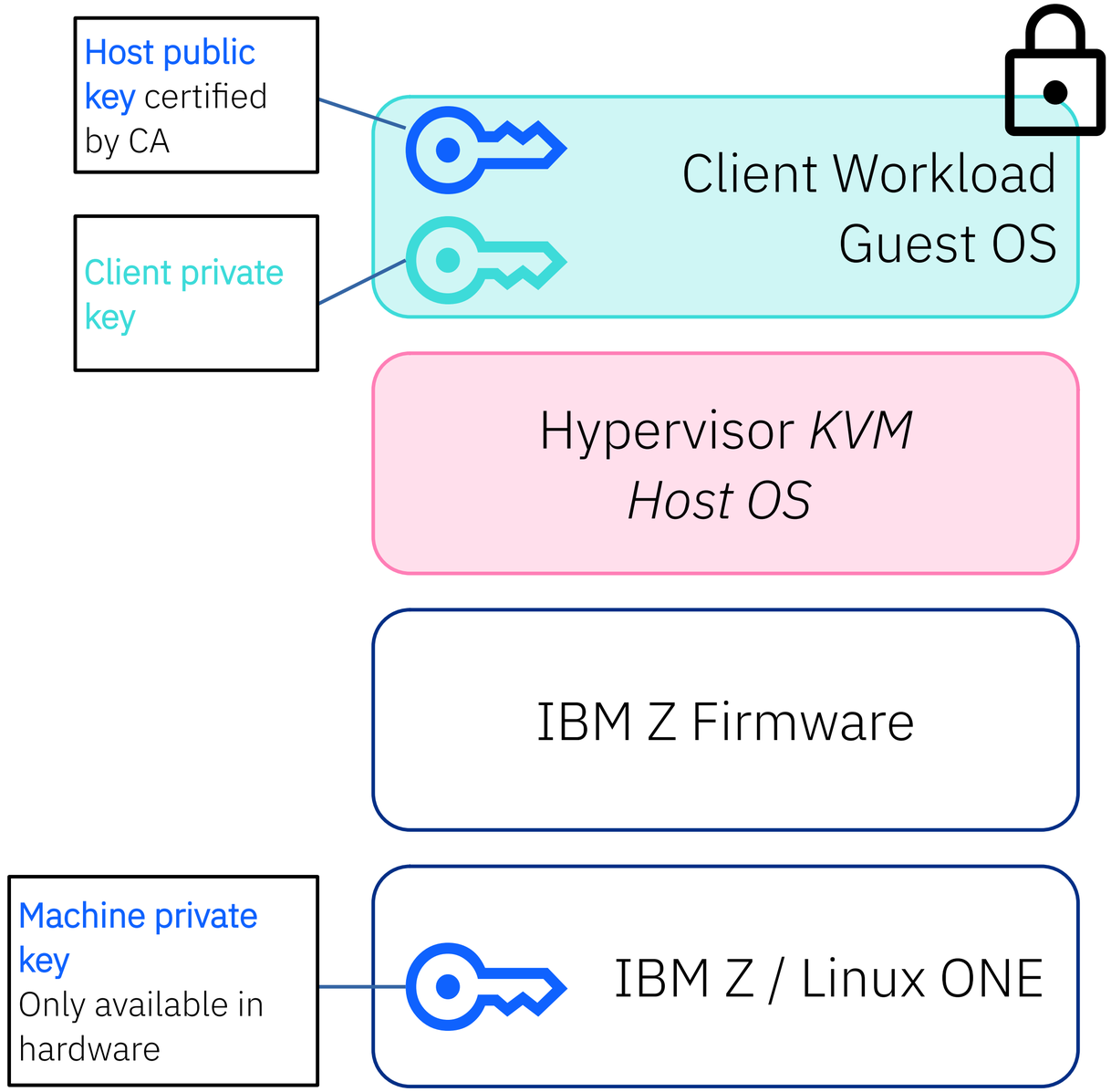
The image **can't be decrypted** outside of the designated host(s) or tampered with

Hypervisor cannot access SE-guest memory unless explicitly shared by that guest

Hardware and firmware ensure that unencrypted virtual machine memory or CPU state cannot be accessed by the host operating system or the administrator of the host machine.

Hypervisor is still responsible for:

- Actual I/O and device model
- Housekeeping for some instructions
- Scheduling
- Memory management



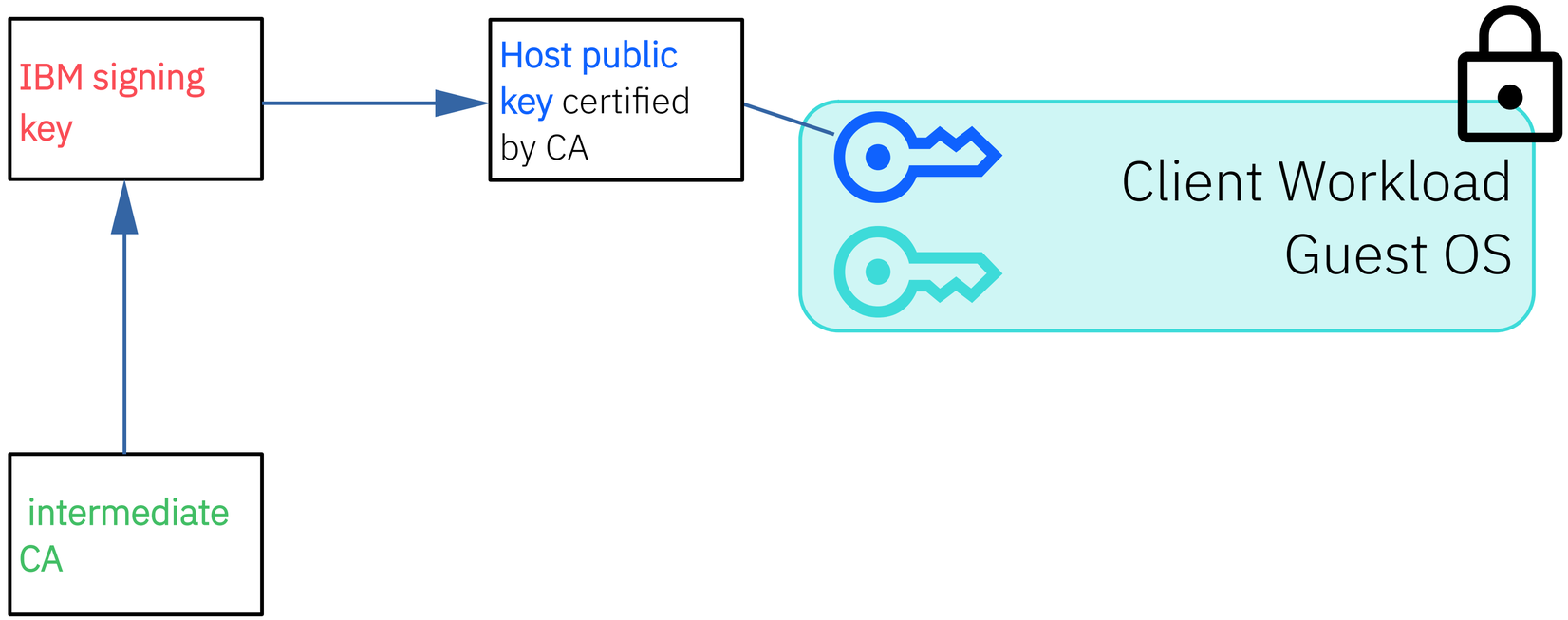
IBM Secure Execution for Linux

Chain of trust

Each physical machine is associated with a host public key, with the private key only accessible to hardware and firmware

Host public key is signed by the IBM signing key.

The IBM signing key is singed by an intermediate CA (from DigiCert).



IBM Secure Execution for Linux

SE Image (simplified)

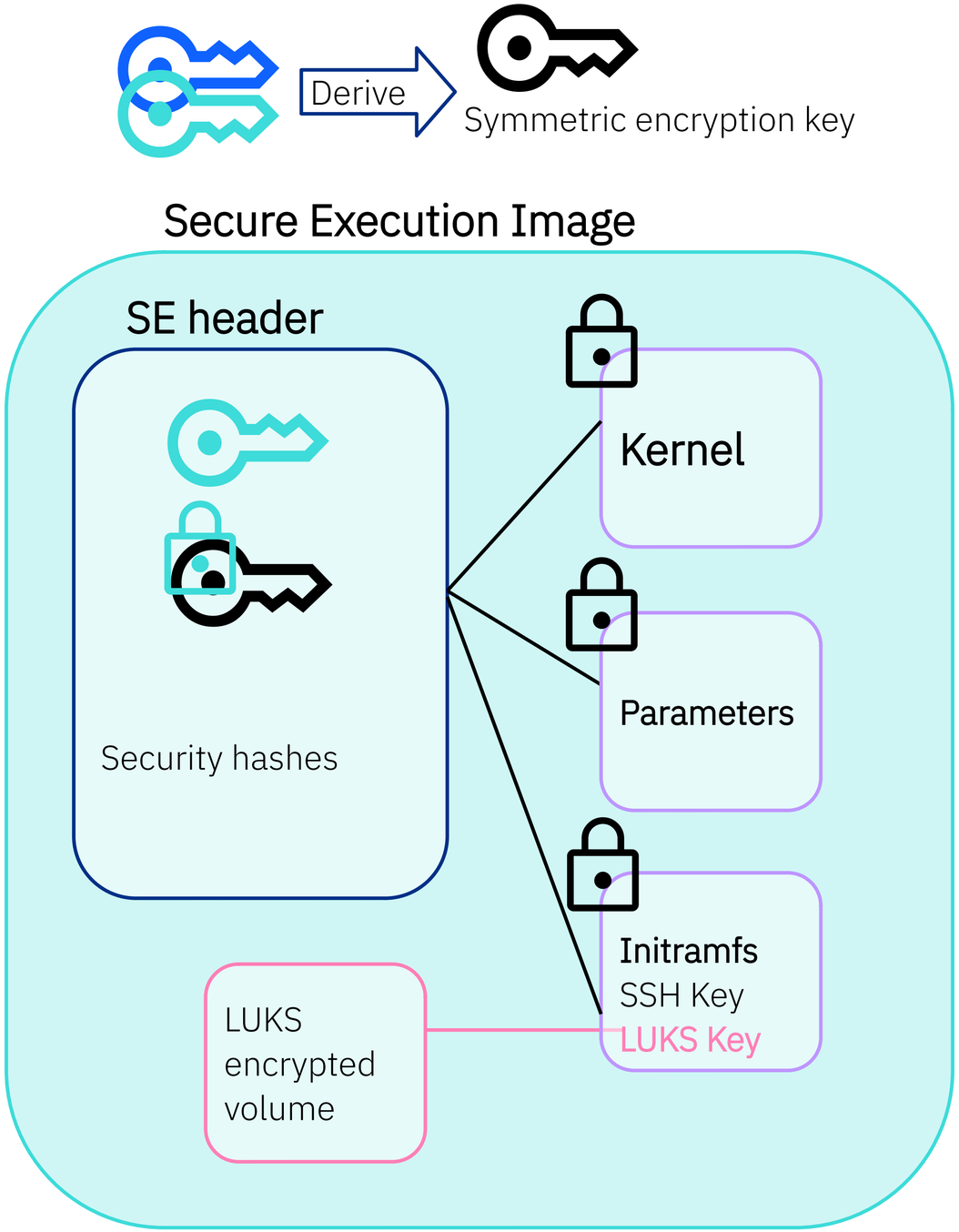
Protected components
Kernel
Kernel paremeters
Initial RAM filesystem

All are encrypted and measured during image preparation

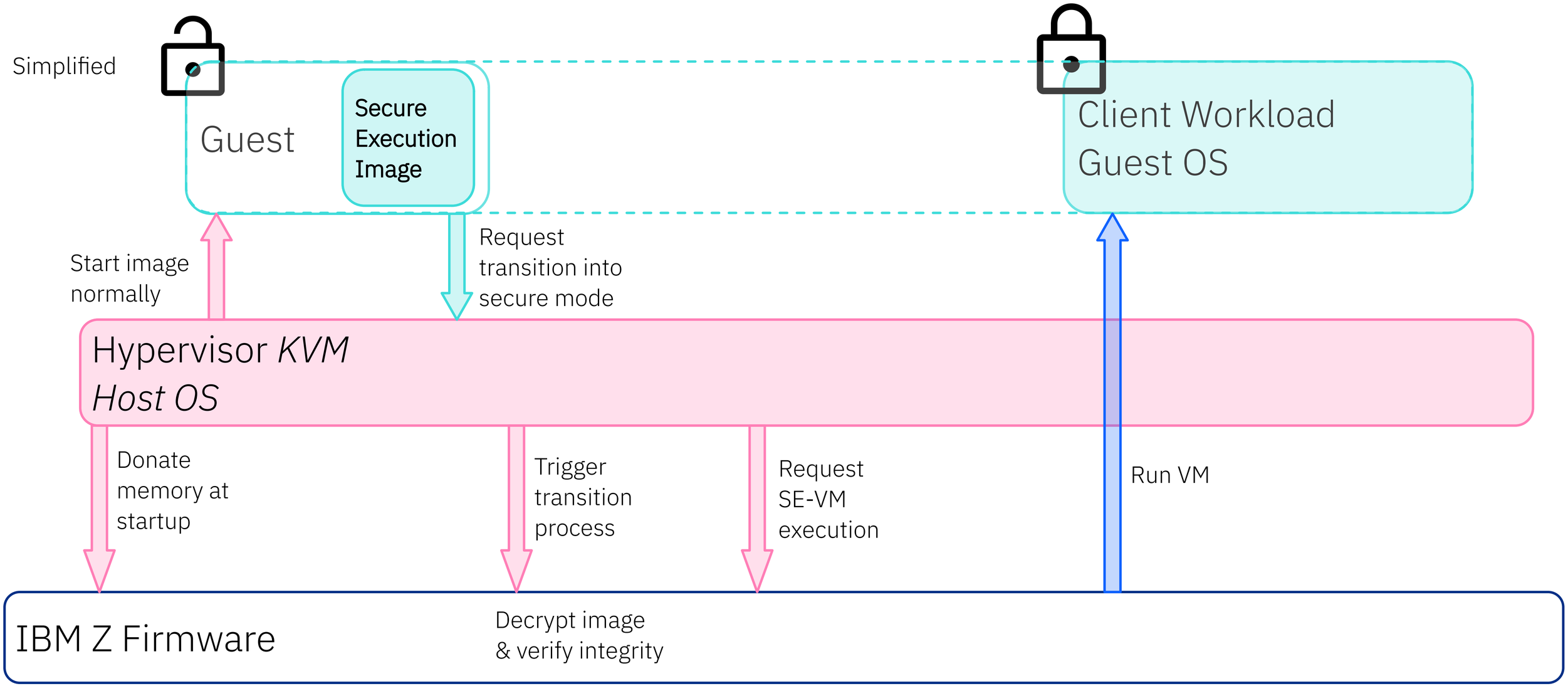
Keys and integrity values are stored in the IBM Secure Execution Header

Additional secrets can be stored safely in the initial RAM filesystem

Ultravisor will **verify the image** component against the measurements in the header and only start execution if the image is found to be valid



Livecycle


Simplified
Guest
Secure Execution Image
Client Workload Guest OS
Start image normally
Request transition into secure mode
Hypervisor *KVM*
Host OS
Donate memory at startup
Trigger transition process
Request SE-VM execution
Run VM
IBM Z Firmware
Decrypt image & verify integrity

Agenda

IBM Secure Execution

Run confidential workloads securely in a public, private, or hybrid cloud.

Explicit Attestation

Prove that a workload is secured with IBM Secure Execution

Explicit Attestation for IBM Secure Execution

Overview

Explicit Attestation usecases

Let a 3rd party attest without passing image secrets

Attest without unique image secrets

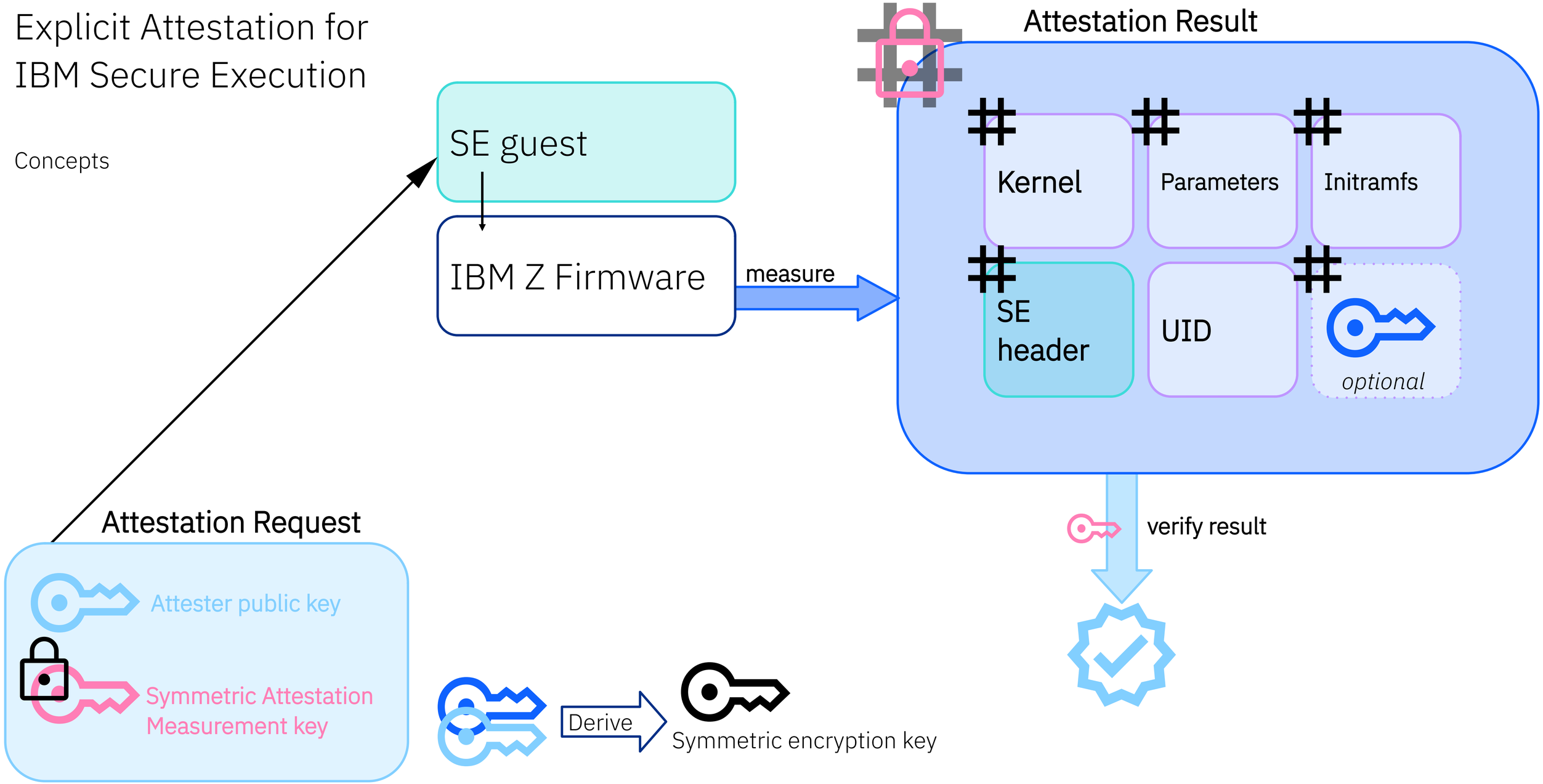
Verify that a SE running guest is a specific instance

IBM Secure Execution does not require external attestation to prove that a guest is secure.

If the image contains a unique ssh key, a successful login implicitly *attests* a SE guest image

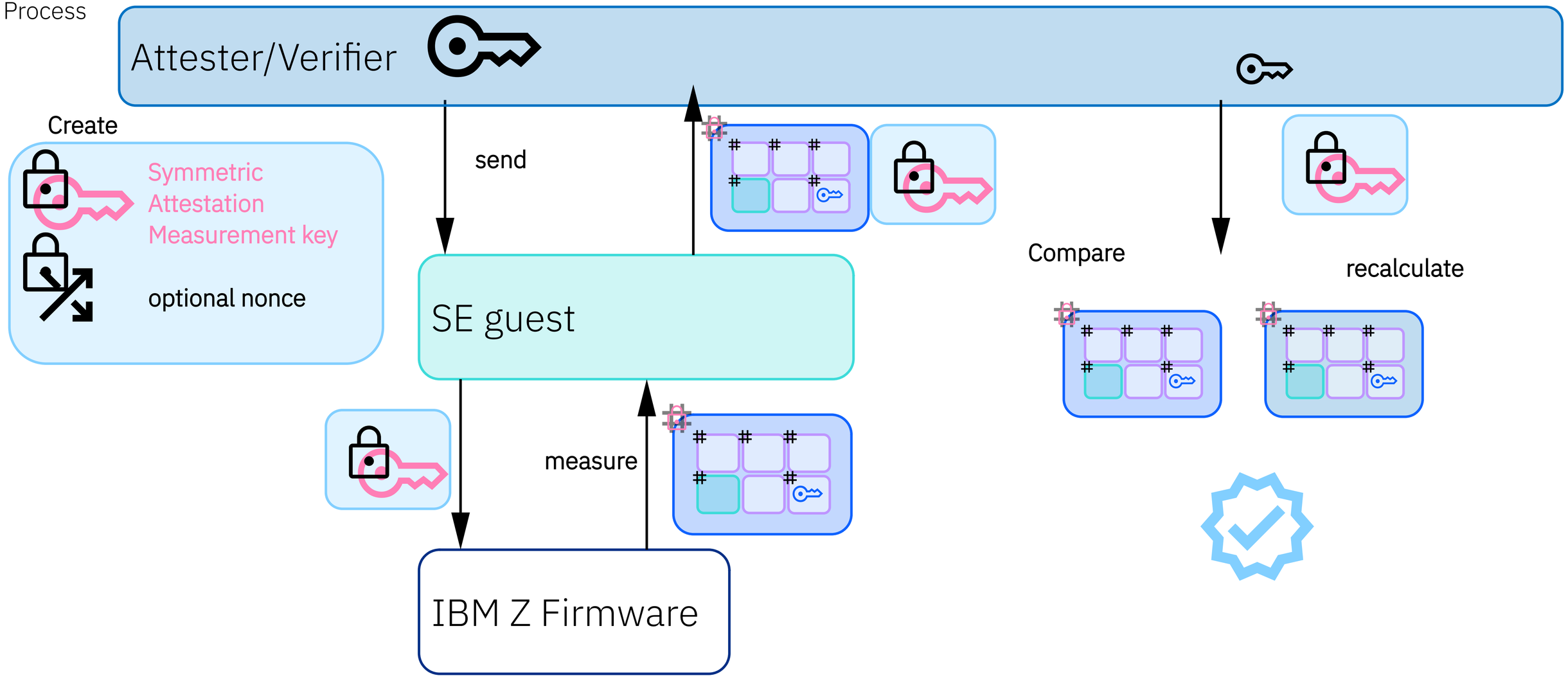
Explicit Attestation for IBM Secure Execution

Concepts



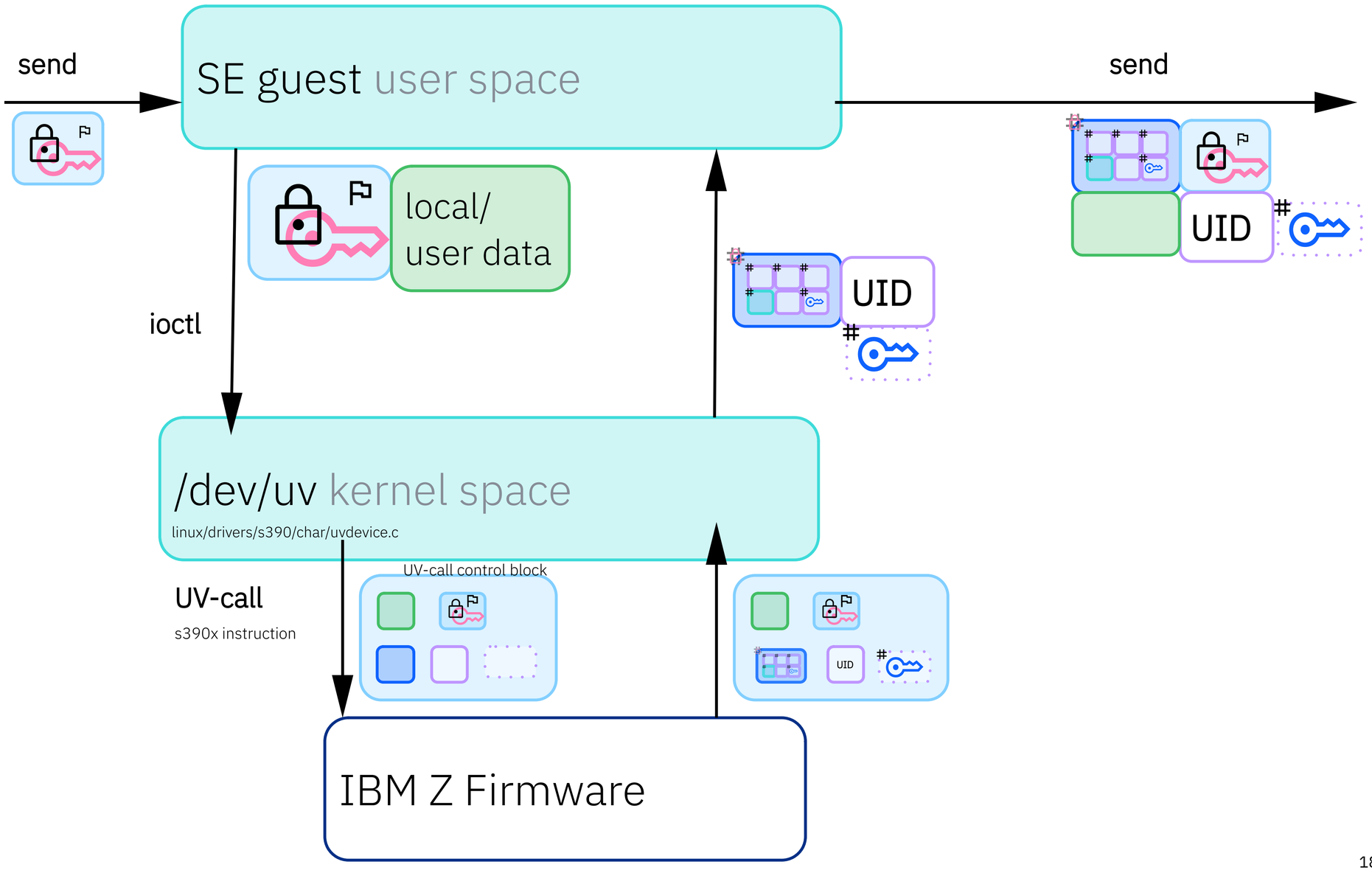
Explicit Attestation for IBM Secure Execution

Process



Explicit Attestation for IBM Secure Execution

Guest Details



Feature Matrix

Version numbers are minimal requirements

Feature	Hardware	RHEL	SLES	Ubuntu
Base Secure Execution	IBM z15 LinuxONE III	7.8 (guest) 8.2 9.0	12 SP 5(guest) 15 SP 2	20.04
Explicit Attestation (SE guest)	IBM z16 LinuxONE 4	8.7 9.1	15 SP 4	22.04
Tooling for non-s390 systems *generating requests and images*	n/a	8.10 9.4	TBA	23.10

More information

Content	Type	Link
Secure Execution documentation	Documentation	IBM Documentation
SE KVM Forum 2022	Presentation	YouTube
Secure Execution FOSDEM 23	Presentation	Fosdem archive
SE KVM Forum 2019	Presentation	YouTube
SE for RedHat CoreOS DevConf.CZ 2023	Presentation	YouTube
Important note on verifying host keys	What's new: Linux for IBM systems	IBM Documentation

Thank you