IBM Secure Execution for Linux Overview

Viktor Mihajlovski
Product Owner KVM on IBM Z
mihajlov@de.ibm.com

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

CICS*
Db2*
GDPS*
HiperSockets
IBM*
IBM (logo)*
IBM Cloud Pak
ibm.com
IBM Z*
LinuxONE
WebSphere*
z14*
z15
z/OS*
z/VM*
z/VSE*

*** Registered trademarks of IBM Corporation**

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.

ITIL is a Registered Trade Mark of AXELOS Limited.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Kubernetes and Container Initiative™ are registered trademark of The Linux Foundation.

Red Hat and Red Hat OpenShift are registered trademarks of Red Hat, Inc. Open

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Other product and service names might be trademarks of IBM or other companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

This information provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g, zIIPs, zAAPs, and IFLs) ("SEs").   IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the “Authorized Use Table for IBM Machines” provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html   (“AUT”).   No other workload processing is authorized for execution on an SE. IBM offers SE at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

Agenda

- Value
- Technical Components
- Working Principles
- Protection Scope
- Additional Documentation

Value of IBM Secure Execution

Technical Perspective

Allows users to run their Linux workloads with maximum privacy by protecting system memory. Even the system administrator can't access customer data.

Business Perspective

Allows customers to run sensitive workloads off and on premise with the same level of data protection

Reduces the efforts of a cloud service provider or infrastructure department to establish and document procedures for compliance and certification

Basics

What is IBM Secure Execution for Linux

Orderable feature (115) of IBM Z15 or LinuxONE III

End-to-end memory protection realized in hardware

Trusted firmware controlling the separation and isolation of virtual machines

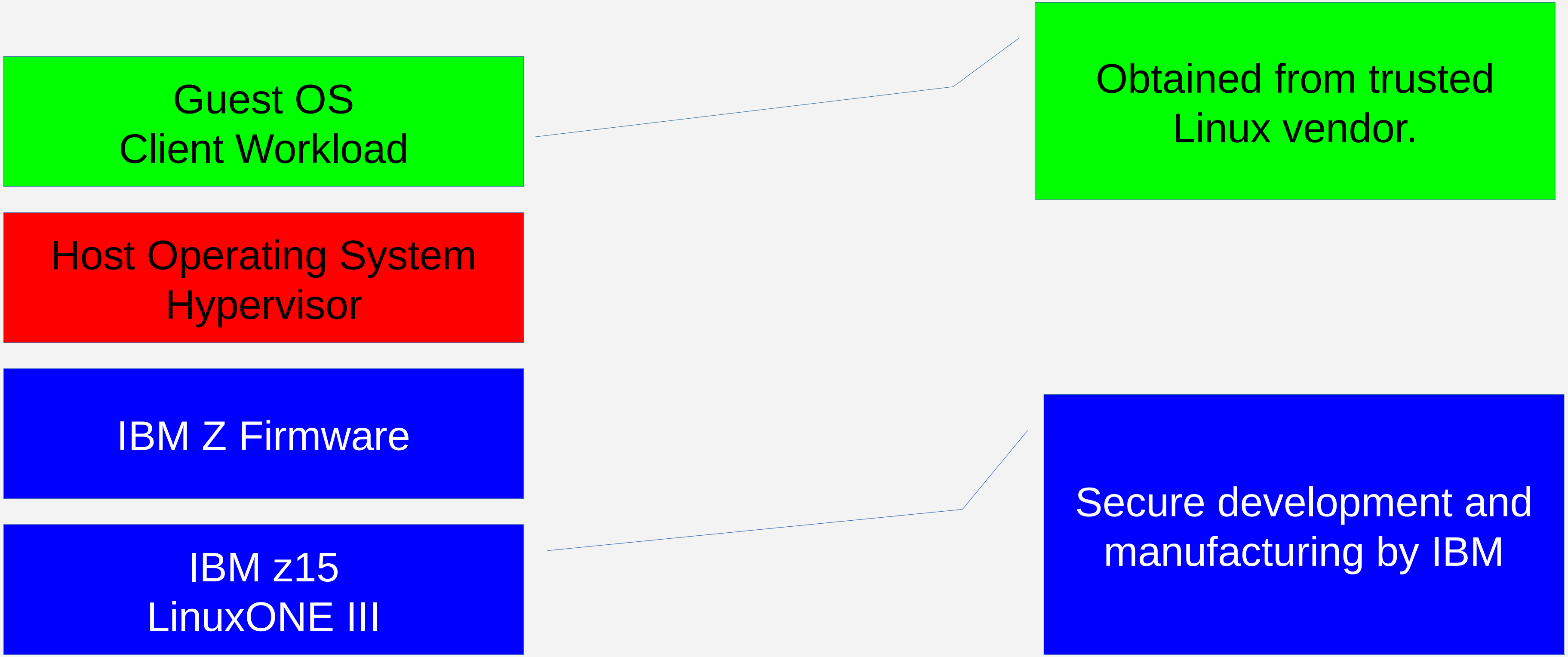
CA-certified public private keys to form a chain of trust

Software Requirements

By the machine owner: a Linux operating system with KVM supporting IBM Secure Execution (RHEL 8.3, SLES 15 SP2, Ubuntu 20.04)

By the workload owner: a Linux operating system which supports running as KVM guest in an IBM Secure Execution virtual machine (RHEL 7.8, RHEL 8.2, SLES 12 SP5, SLES 15 SP2, Ubuntu 20.04)

Trusted and untrusted parts



Guest OS
Client Workload

Host Operating System
Hypervisor

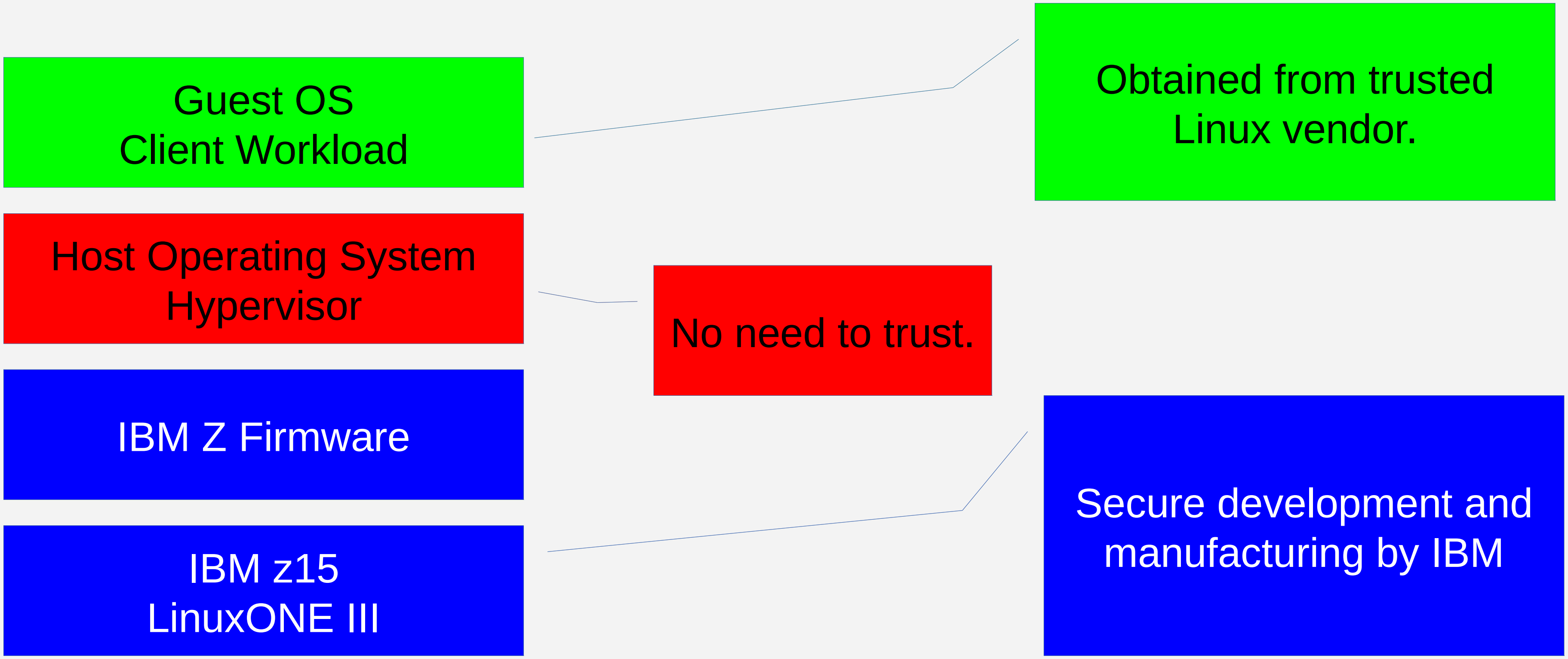
IBM Z Firmware

IBM z15
LinuxONE III

Obtained from trusted Linux vendor.

Secure development and manufacturing by IBM

Trusted and untrusted parts



Guest OS
Client Workload

Host Operating System
Hypervisor

IBM Z Firmware

IBM z15
LinuxONE III

Obtained from trusted Linux vendor.

No need to trust.

Secure development and manufacturing by IBM

How Does it Work

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

A client can prepare an encrypted Linux image using the host public key and a customer-specific key

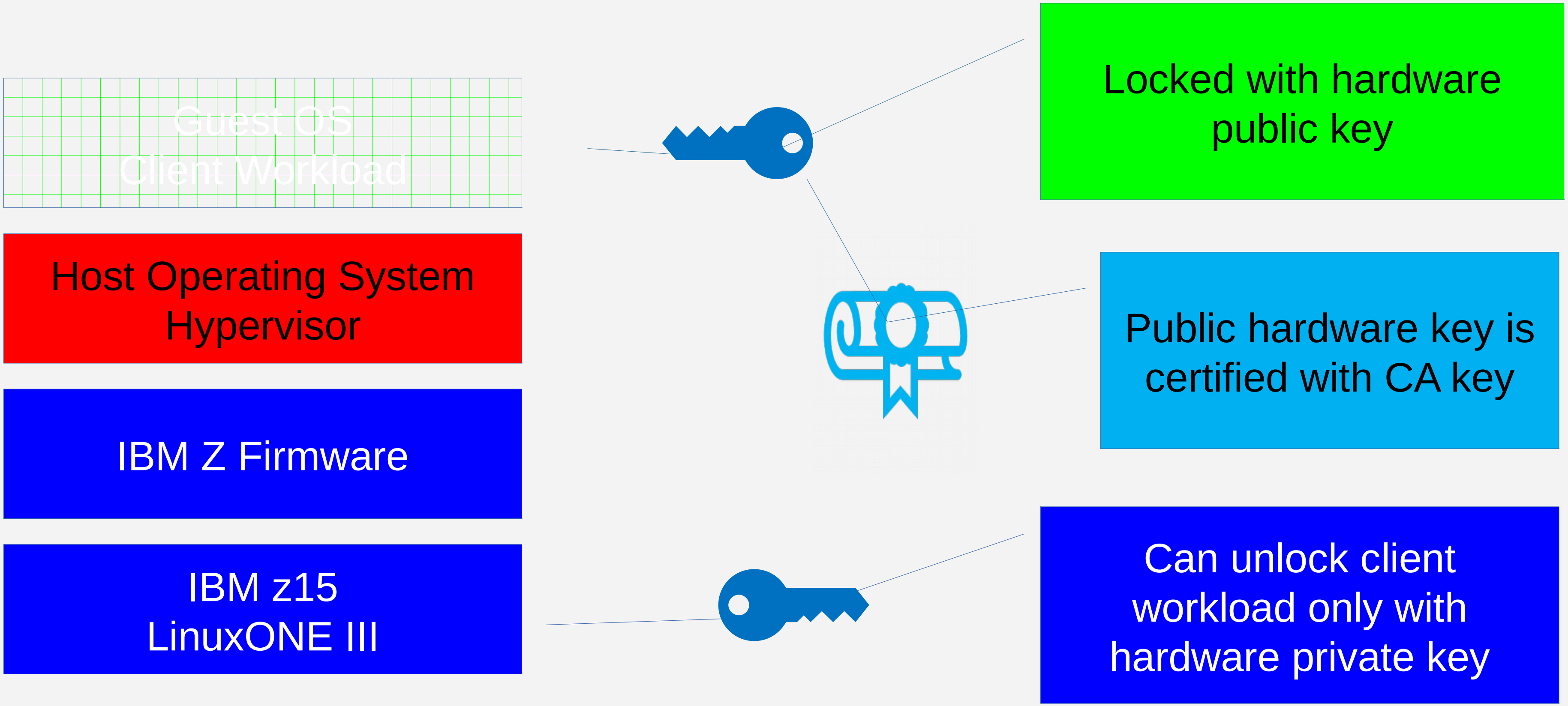
The encrypted image can only be executed in a virtual machine on the host(s) it has been prepared for

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

Z hardware and firmware ensure that unencrypted virtual machine memory can't be accessed by the host operating system or the administrator of the host computer system

The client has only to make sure disk and network data is encrypted (e.g., dm-crypt, TLS)

Trusted and untrusted parts



Guest OS
Client Workload

Host Operating System
Hypervisor

IBM Z Firmware

IBM z15
LinuxONE III

Locked with hardware public key

Public hardware key is certified with CA key

Can unlock client workload only with hardware private key

IBM Secure Execution Protection

Protects against

bad operation of a hardware console by rogue hardware administrators

bad operation of a hypervisor by rogue hypervisor admins

compromised hypervisors (e.g. from a neighboring guest)

corrupt or buggy hypervisors

Doesn’t protect against

damage due to inappropriate physical operations

stealing memory (and inspecting its contents)

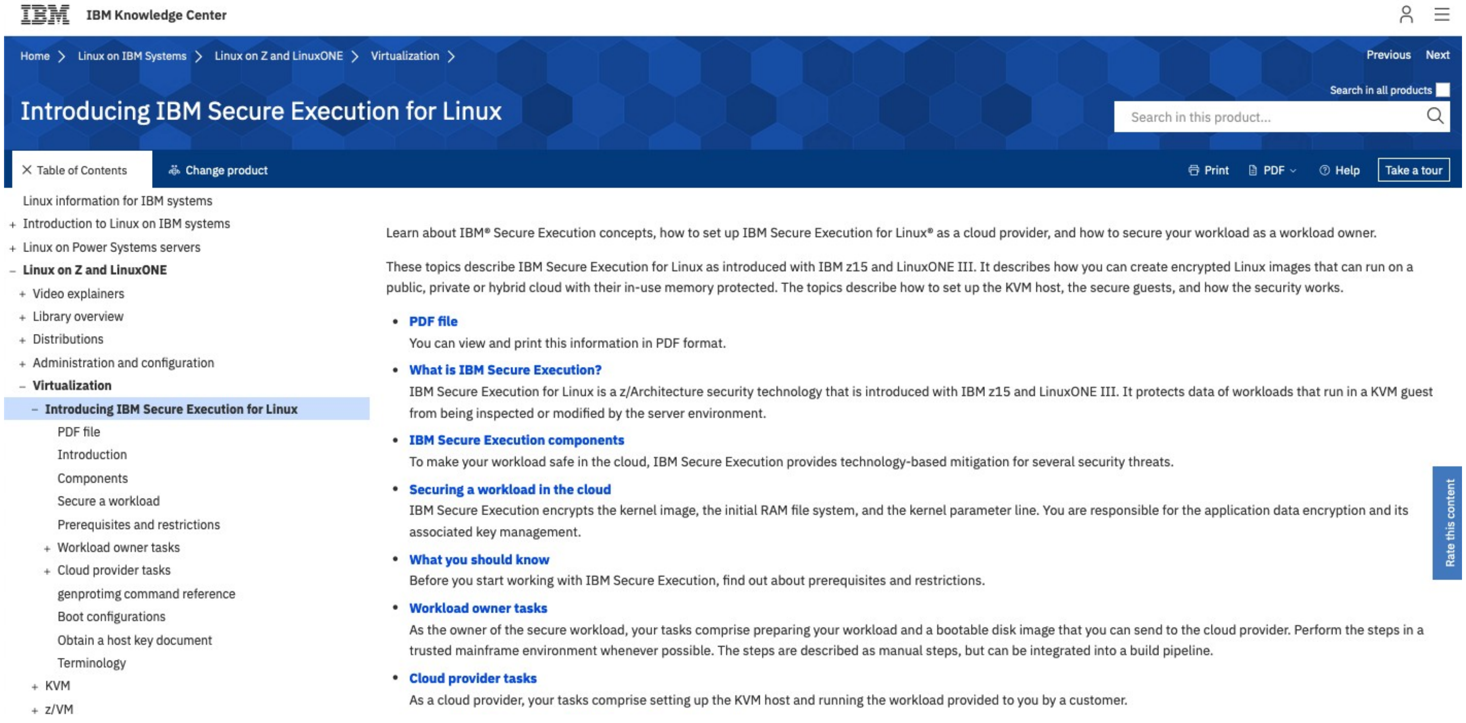
denial of service attacks

bad operation or configuration of the guest by guest administrators

attacking the guest through guest I/O channels

More Information

https://www.ibm.com/support/knowledgecenter/linuxonibm/com.ibm.linux.z.lxse/lxse_t_secureexecution.html


IBM Knowledge Center
Home > Linux on IBM Systems > Linux on Z and LinuxONE > Virtualization >
Previous Next
Search in all products
Search in this product...
Table of Contents
Change product
Print
PDF
Help
Take a tour
Linux information for IBM systems
+ Introduction to Linux on IBM systems
+ Linux on Power Systems servers
− Linux on Z and LinuxONE
+ Video explainers
+ Library overview
+ Distributions
+ Administration and configuration
− Virtualization
− Introducing IBM Secure Execution for Linux
PDF file
Introduction
Components
Secure a workload
Prerequisites and restrictions
+ Workload owner tasks
+ Cloud provider tasks
genprotimg command reference
Boot configurations
Obtain a host key document
Terminology
+ KVM
+ z/VM
Rate this content

Introducing IBM Secure Execution for Linux

Learn about IBM® Secure Execution concepts, how to set up IBM Secure Execution for Linux® as a cloud provider, and how to secure your workload as a workload owner.

These topics describe IBM Secure Execution for Linux as introduced with IBM z15 and LinuxONE III. It describes how you can create encrypted Linux images that can run on a public, private or hybrid cloud with their in-use memory protected. The topics describe how to set up the KVM host, the secure guests, and how the security works.

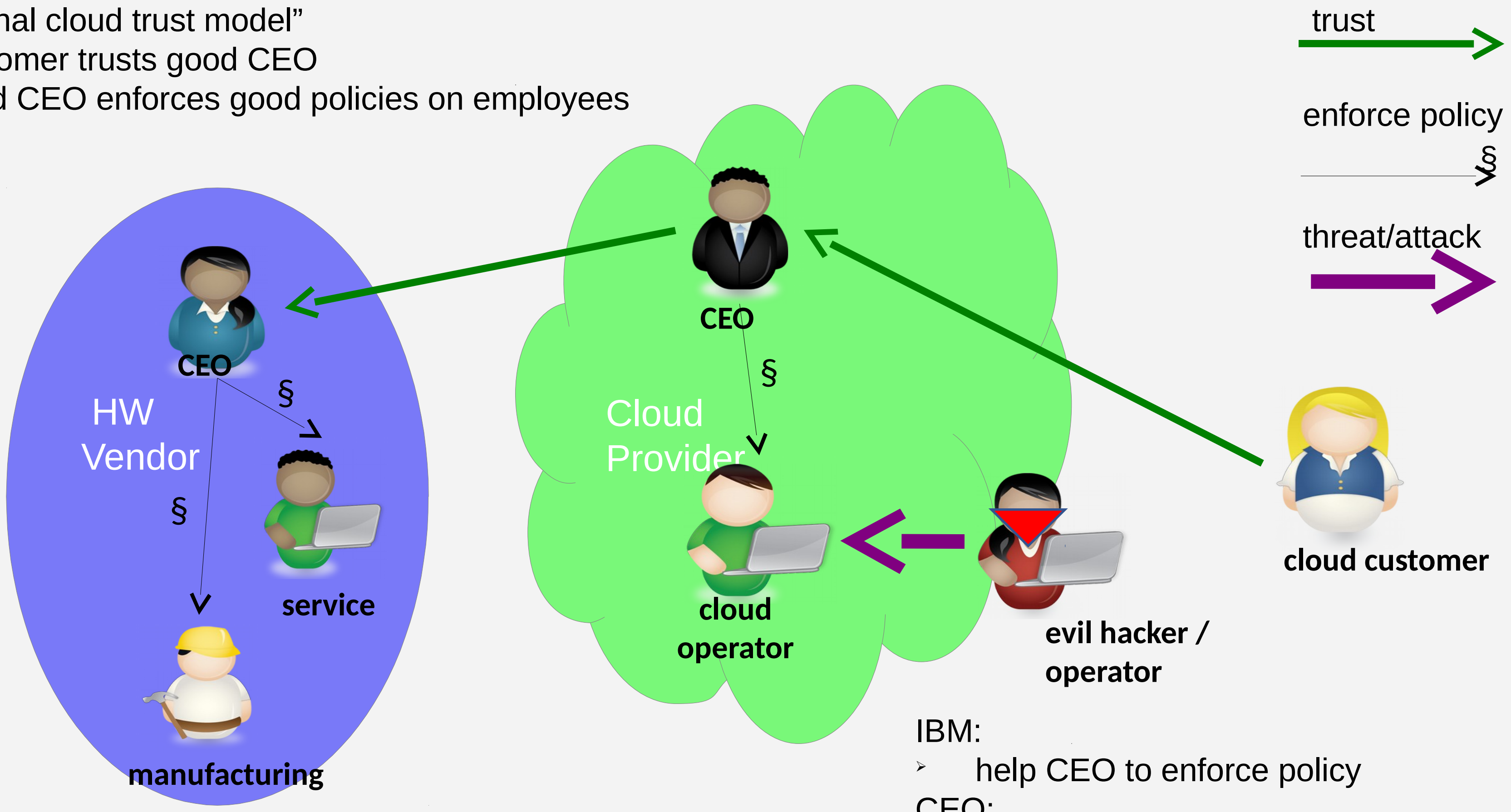
- **PDF file**
  You can view and print this information in PDF format.
- **What is IBM Secure Execution?**
  IBM Secure Execution for Linux is a z/Architecture security technology that is introduced with IBM z15 and LinuxONE III. It protects data of workloads that run in a KVM guest from being inspected or modified by the server environment.
- **IBM Secure Execution components**
  To make your workload safe in the cloud, IBM Secure Execution provides technology-based mitigation for several security threats.
- **Securing a workload in the cloud**
  IBM Secure Execution encrypts the kernel image, the initial RAM file system, and the kernel parameter line. You are responsible for the application data encryption and its associated key management.
- **What you should know**
  Before you start working with IBM Secure Execution, find out about prerequisites and restrictions.
- **Workload owner tasks**
  As the owner of the secure workload, your tasks comprise preparing your workload and a bootable disk image that you can send to the cloud provider. Perform the steps in a trusted mainframe environment whenever possible. The steps are described as manual steps, but can be integrated into a build pipeline.
- **Cloud provider tasks**
  As a cloud provider, your tasks comprise setting up the KVM host and running the workload provided to you by a customer.

Backup

Traditional Cloud Trust Model: Trust the CEOs

“Traditional cloud trust model”

- customer trusts good CEO
- good CEO enforces good policies on employees



IBM:

- help CEO to enforce policy

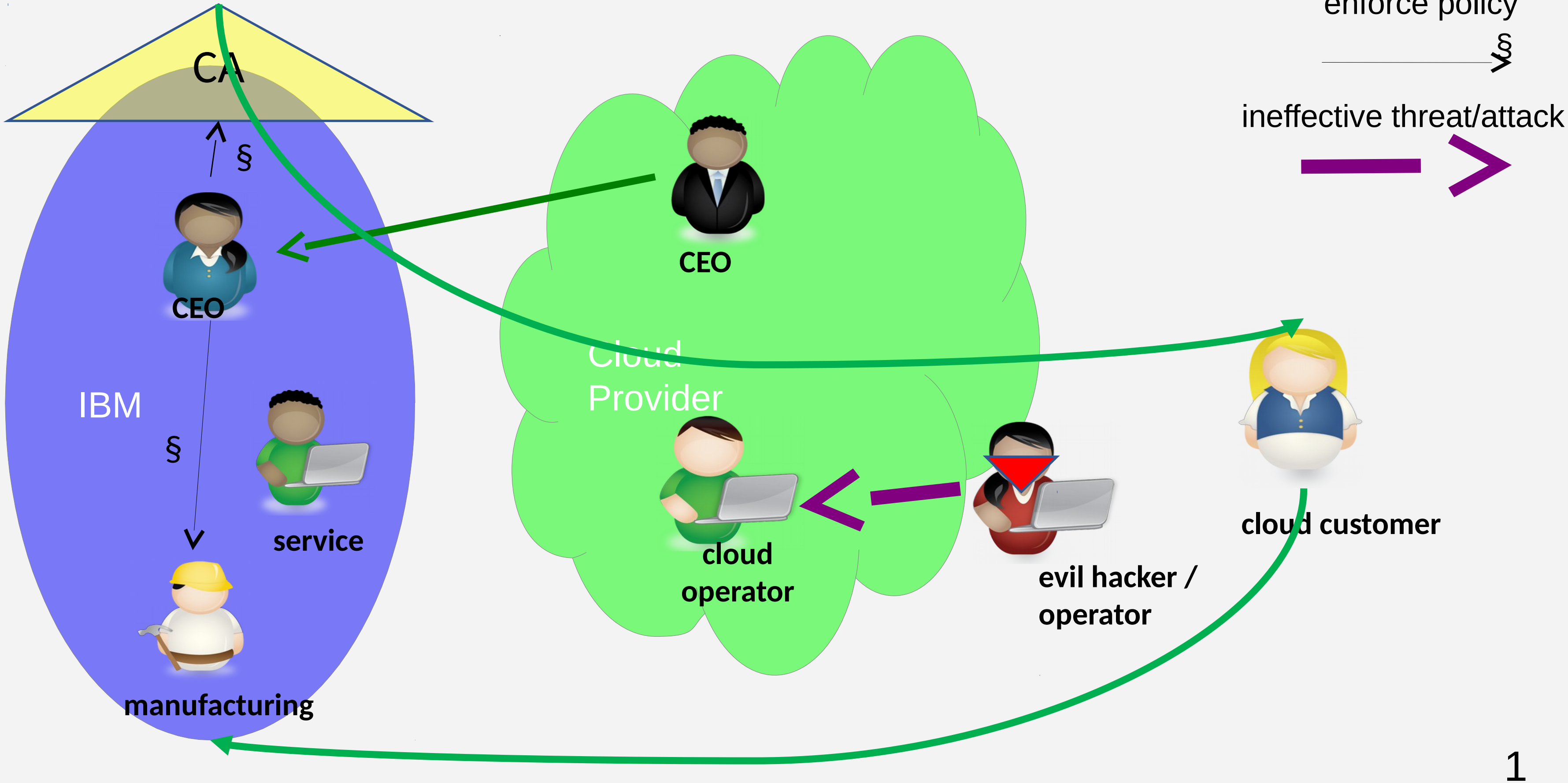
CEO:

- publishes policy and means of enforcements

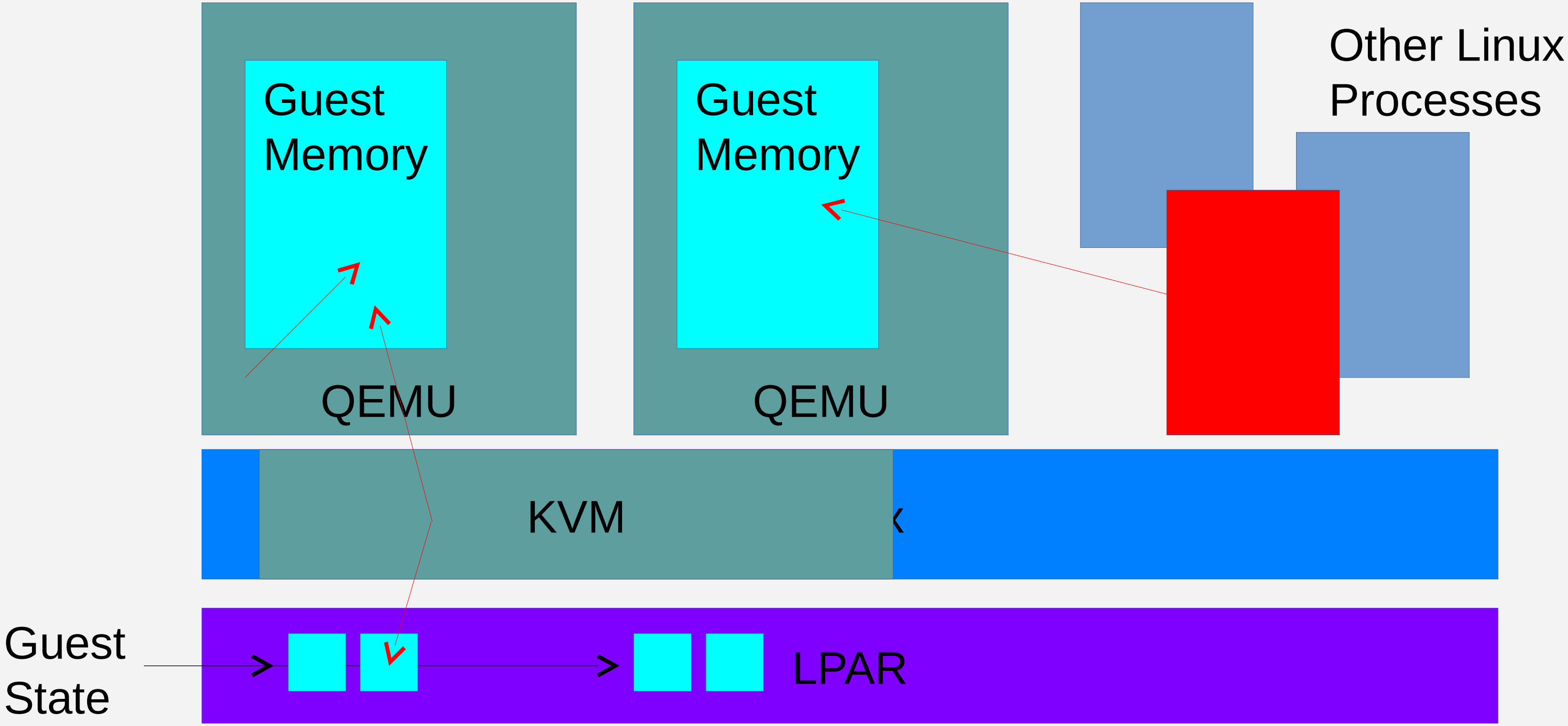
Secure Execution trust model: Trust HW vendor

“SE Trust Model”

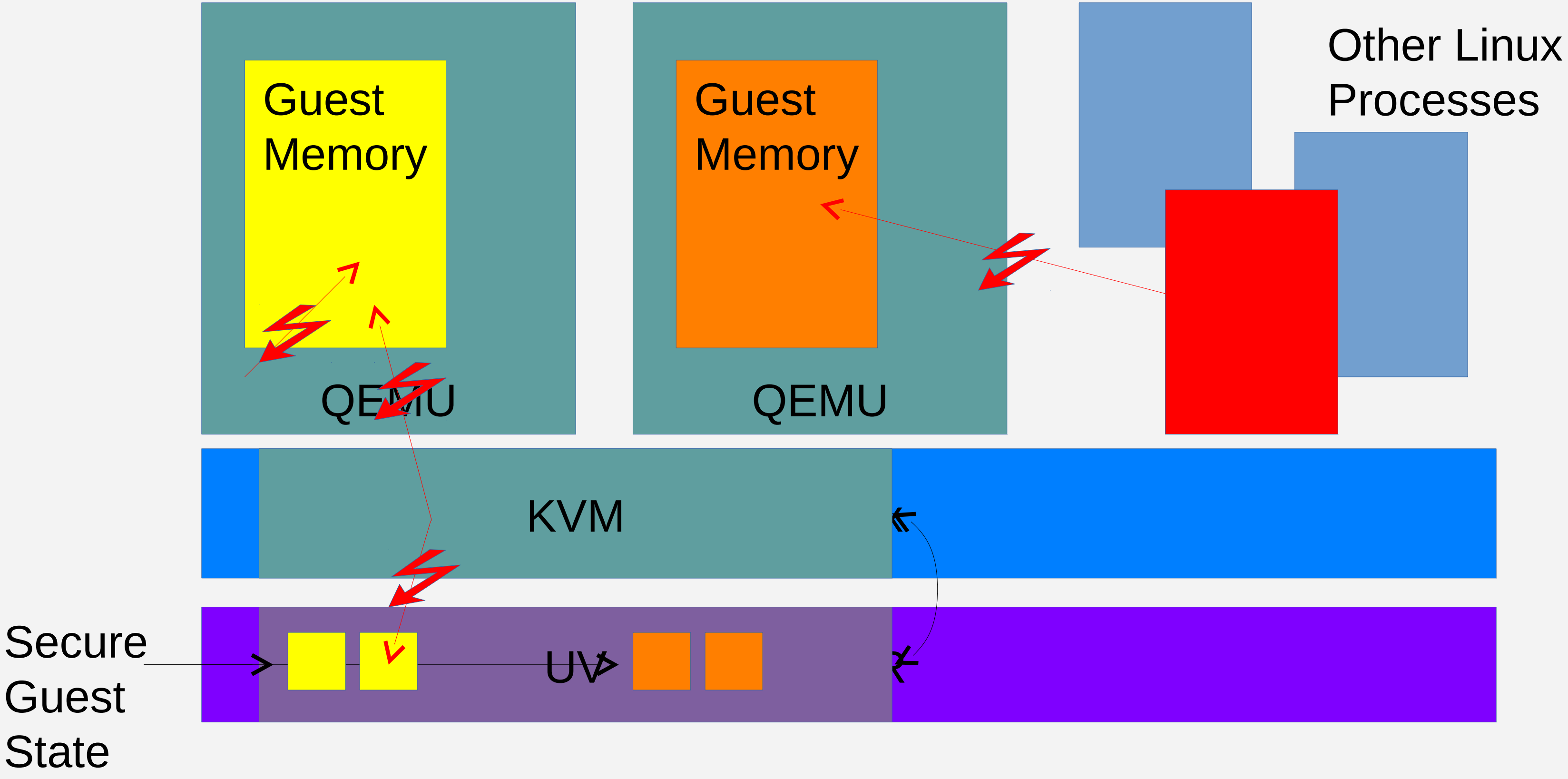
- customer trusts HW vendor
  - CEO + manufacturing process



Without IBM Secure Execution



IBM Secure Execution Protection


Guest
Memory
QEMU
Guest
Memory
QEMU
Other Linux
Processes
KVM
UV
Secure
Guest
State