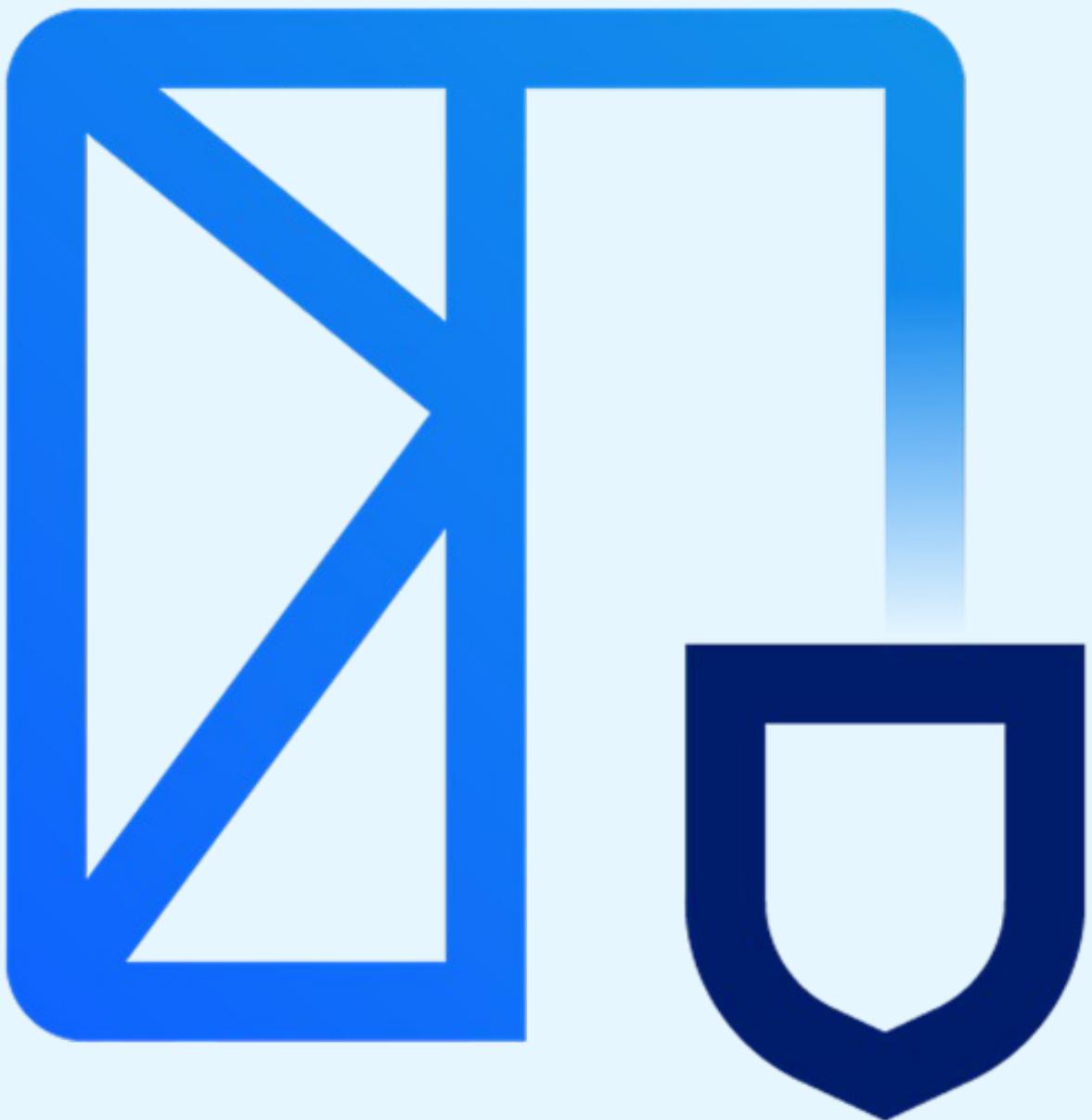


IBM®

# Confidential Computing on IBM zSystems and LinuxONE with Hyper Protect Virtual Servers

## 2.1.3 Wildfire Workshop – April 4, 2023

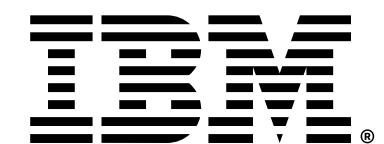


Barry Silliman  
Consulting IT Specialist

silliman@us.ibm.com  
240.674.7222

Garrett Woodworth  
Senior IT Specialist

garrett.lee.woodworth@ibm.com  
510.600.5652



---

## Definition of confidential computing

---

zSystems and LinuxONE and confidential computing

---

Hyper Protect Virtual Servers 2.1.x overview

---

Additional resources

---

Lab overview

---

# Confidential Computing...

## What is it?

*“The protection of data in use through a hardware-based technique”*

*Trusted Execution Environment (TEE) = hardware-based secure enclave where memory (data in use) is protected*

- [Confidential Computing Consortium](#)

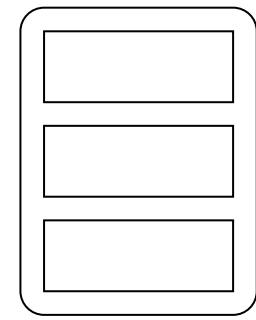


Trusted Execution Environment (TEE)

# Confidential computing completes the triad of data protection

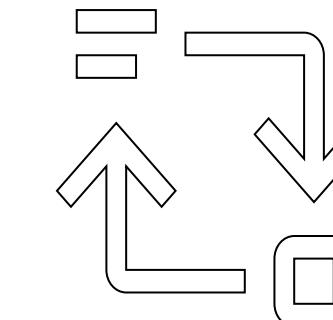
PREVALENT PROTECTIONS

INCREASING FOCUS



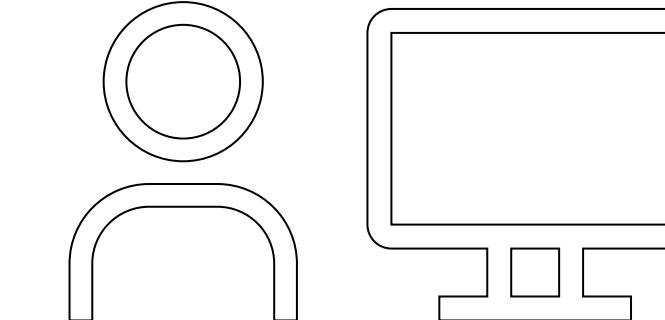
## Data at rest

Inactive data that is not currently being accessed or transferred



## Data in transit

Traveling between public or private networks



## Data in use

Actively being accessed by an application or a user and stored in memory



CONFIDENTIAL COMPUTING

# zSystems' and LinuxONE's first implementation of Confidential Computing: Secure Service Container LPAR

## IBM Secure Service Container

Provides the base infrastructure for an integration of operating system, middleware, and software components.

It provides the key security capabilities for Hyper Protect Services, both in the public cloud and on-premises



**Secure  
Service  
Container**

### Secure Boot

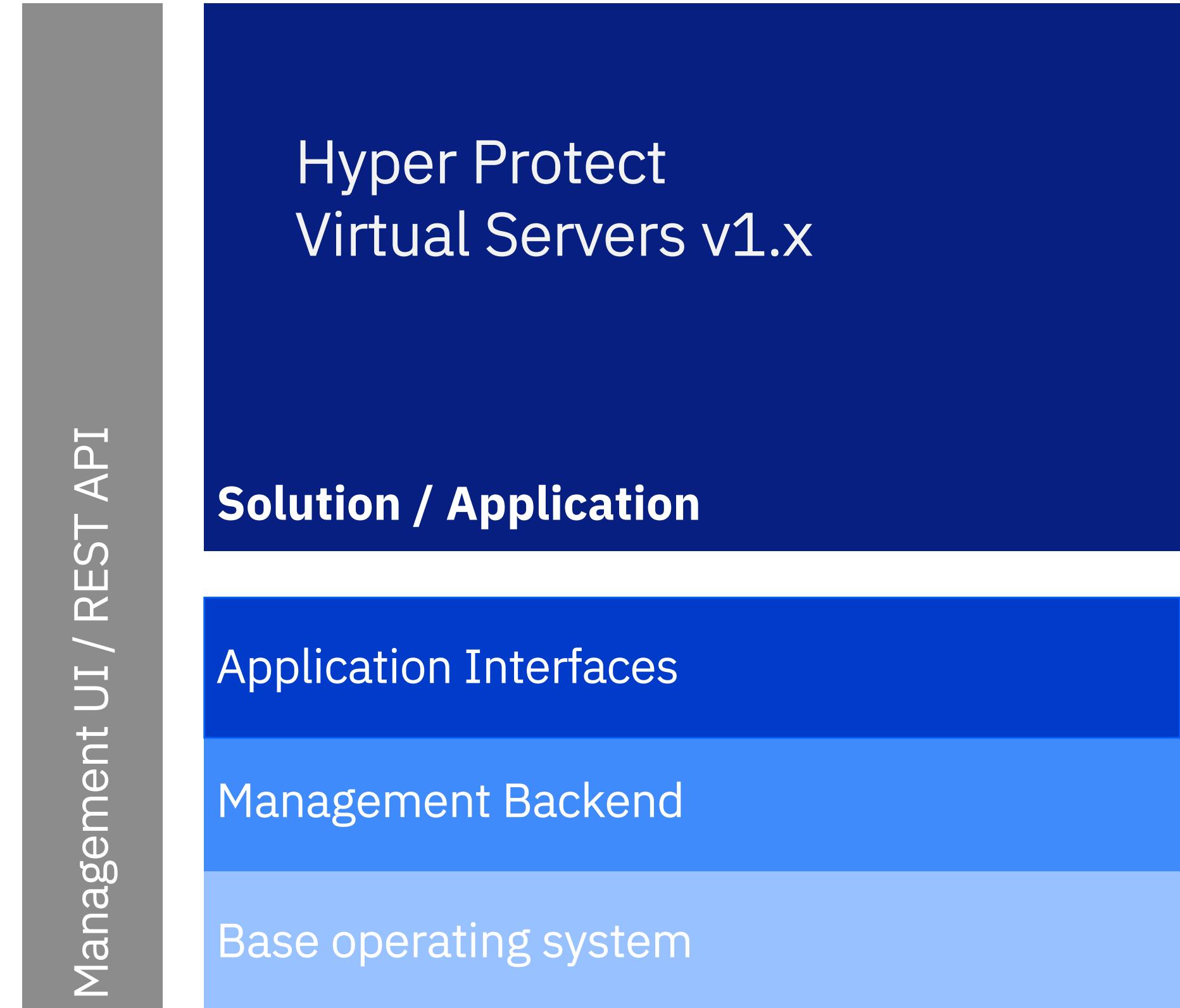
- Only boots authorized workloads

### Data Encryption

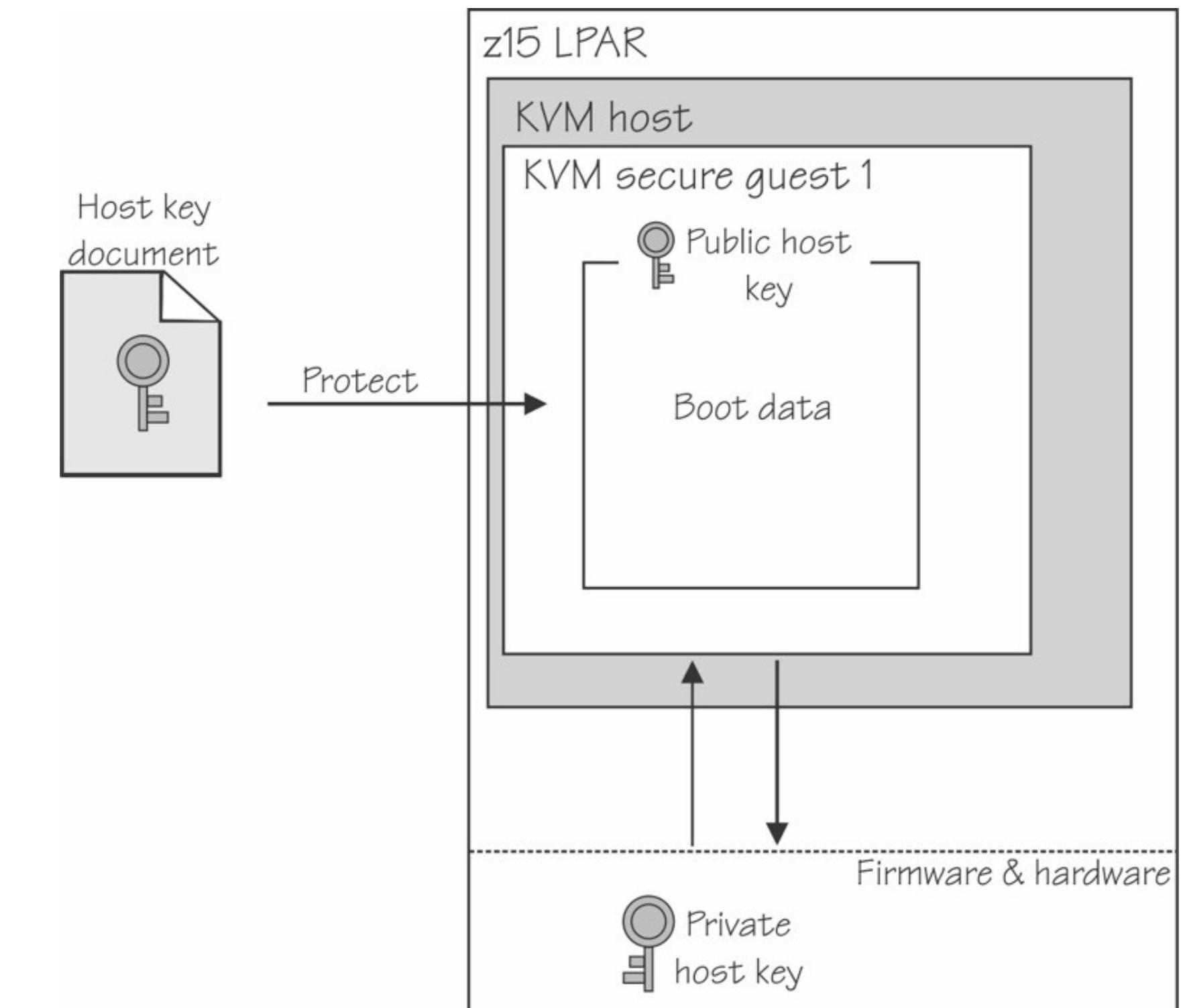
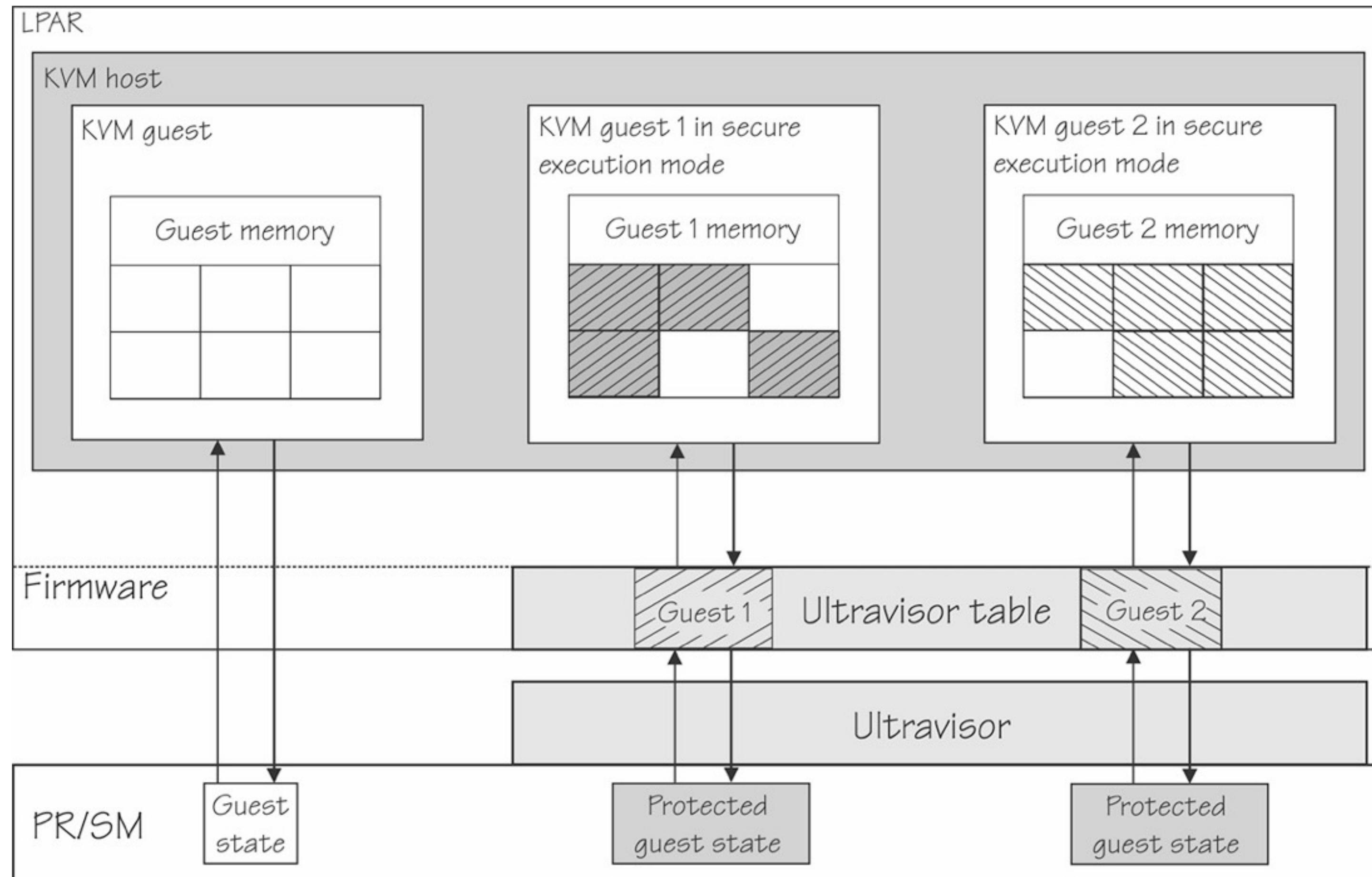
- All data and code in flight and at rest
- Debug data i.e., dumps, diagnostic log files

### Restricted Access

- Encrypted communication via REST APIs
- No direct operating system level access
- No infrastructure administrator access to memory or processor state



# zSystems' and LinuxONE's newest implementation of Confidential Computing: Secure Execution for Linux

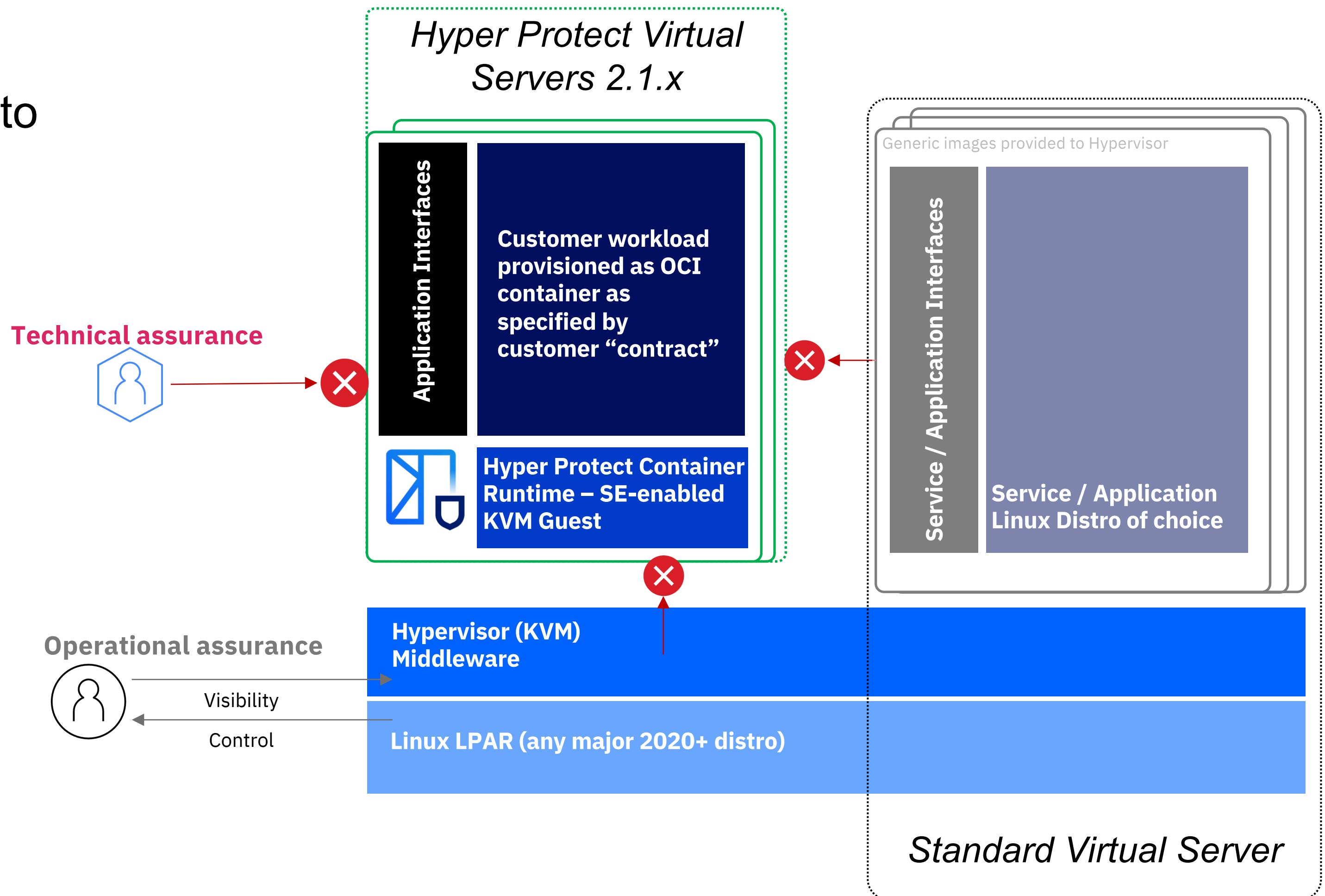


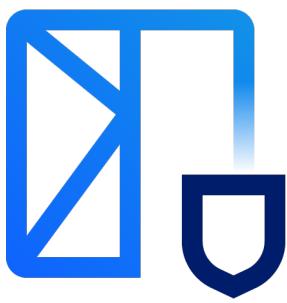
No hardware administrator, no KVM code, and no KVM administrator can access the data in a guest that was started as an IBM Secure Execution guest. Read more here: <https://www.ibm.com/docs/en/linux-on-systems?topic=virtualization-secure-execution>

# Hyper Protect Virtual Servers 2.1.x is based on Secure Execution for Linux

Hyper Protect Virtual Servers 2.1.x takes advantage of Secure Execution technology to provide a secure boundary around each instance

- Isolation from the OS and Hypervisor vulnerabilities
- Isolation between instances
- Technical assurance that host administrator cannot access the environment





# Reduce common attack vectors with Hyper Protect Virtual Servers

## Remote Attack

- No interactive access (SSH) into protected Trusted Execution Environment

## Privilege Escalation

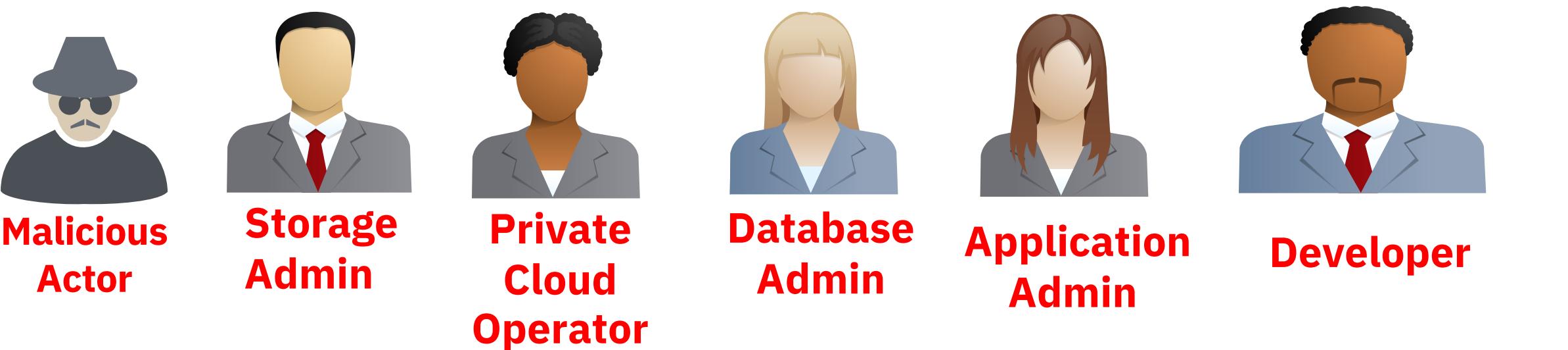
- Workload isolation against OS/Hypervisor/Middleware
- Isolation between Secure Execution Virtual Machines/Enclaves

## Insider Attack

- Access to hardware does not mean data is compromised
- Only authorized workload can access customer data  
(confidential computing: data-in-use protected)

## Image Tampering/Malware

- Encrypted image and only deployable on systems with Secure Execution
- Multi-party encrypted contract with optional attestation

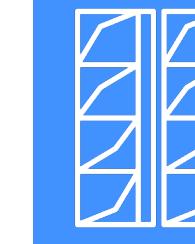
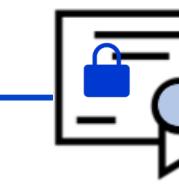




## Encrypted Multi-Party Contract

Enables customer to enforce Zero-Trust concepts  
Individual secrets of workload, deployment and more

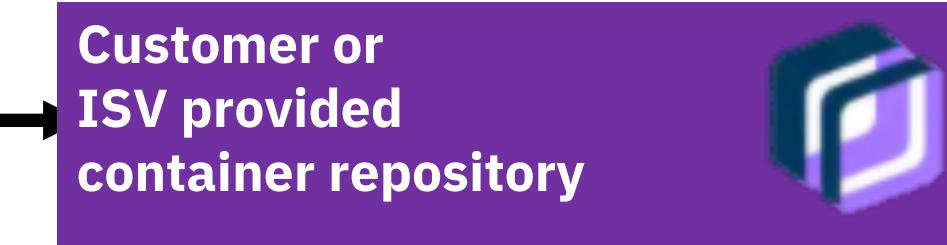
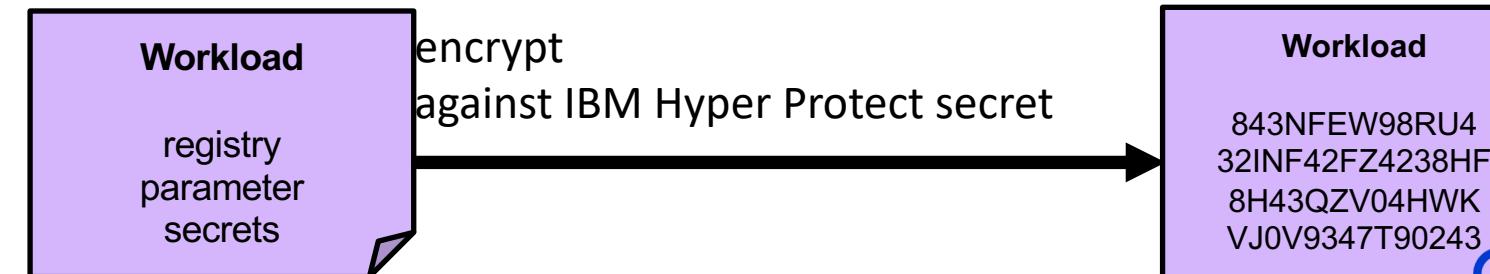
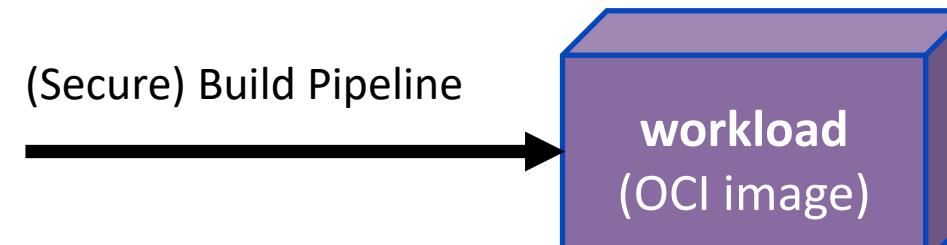
## IBM Hyper Protect



data-in-use protection  
through Secure Execution  
HW-based protected keys



### Workload (Provider)



### IBM Hyper Protect Container Runtime

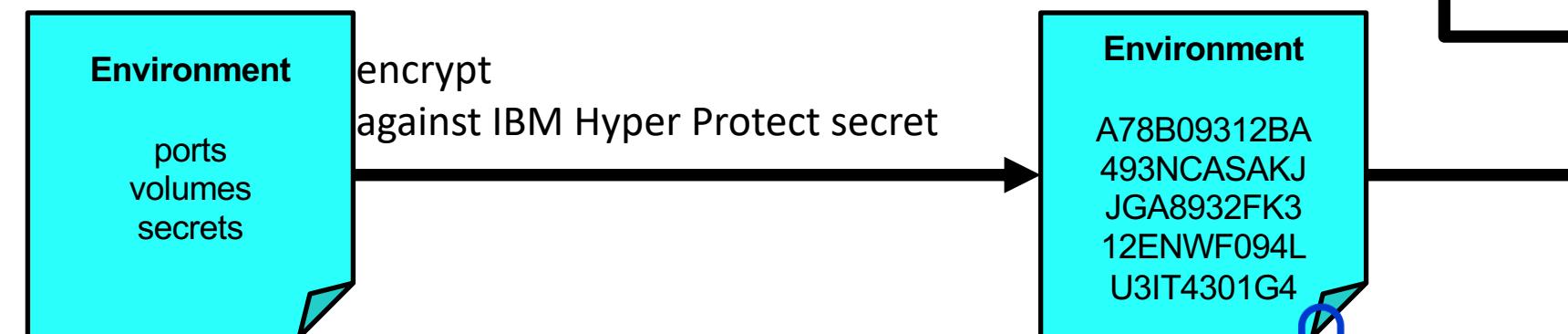


validate



### Customer specific

#### Environment



#### Hyper Protect Contract

**Workload**

843NFEW98RU4  
32INF42FZ4238HF  
8H43QZV04HWK  
VJ0V9347T90243

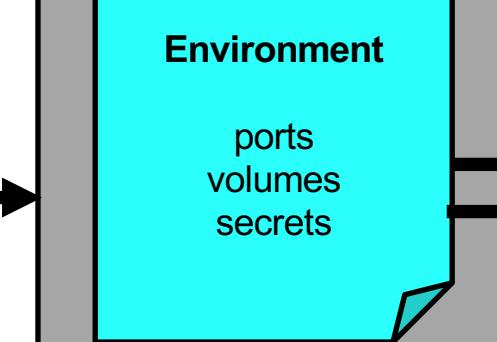
**Environment**

A78B09312BA  
493NCASAKJ  
JGA8932FK3  
12ENWF094L  
U3IT4301G4

**Attestation**

7841AHABCAC

#### Hyper Protect Contract



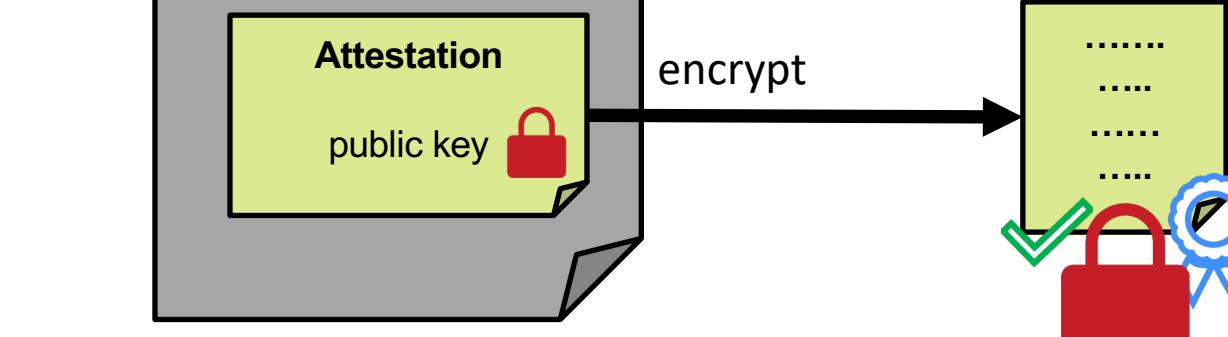
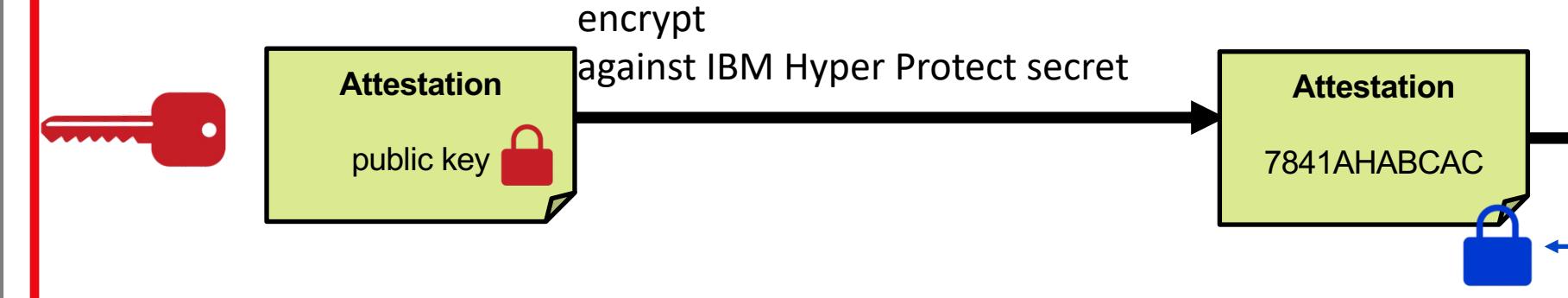
provide/deploy

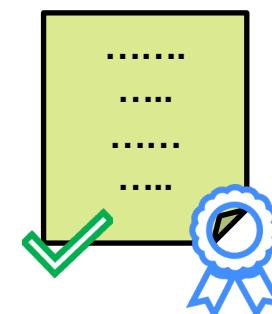
decrypt

deploy

attest

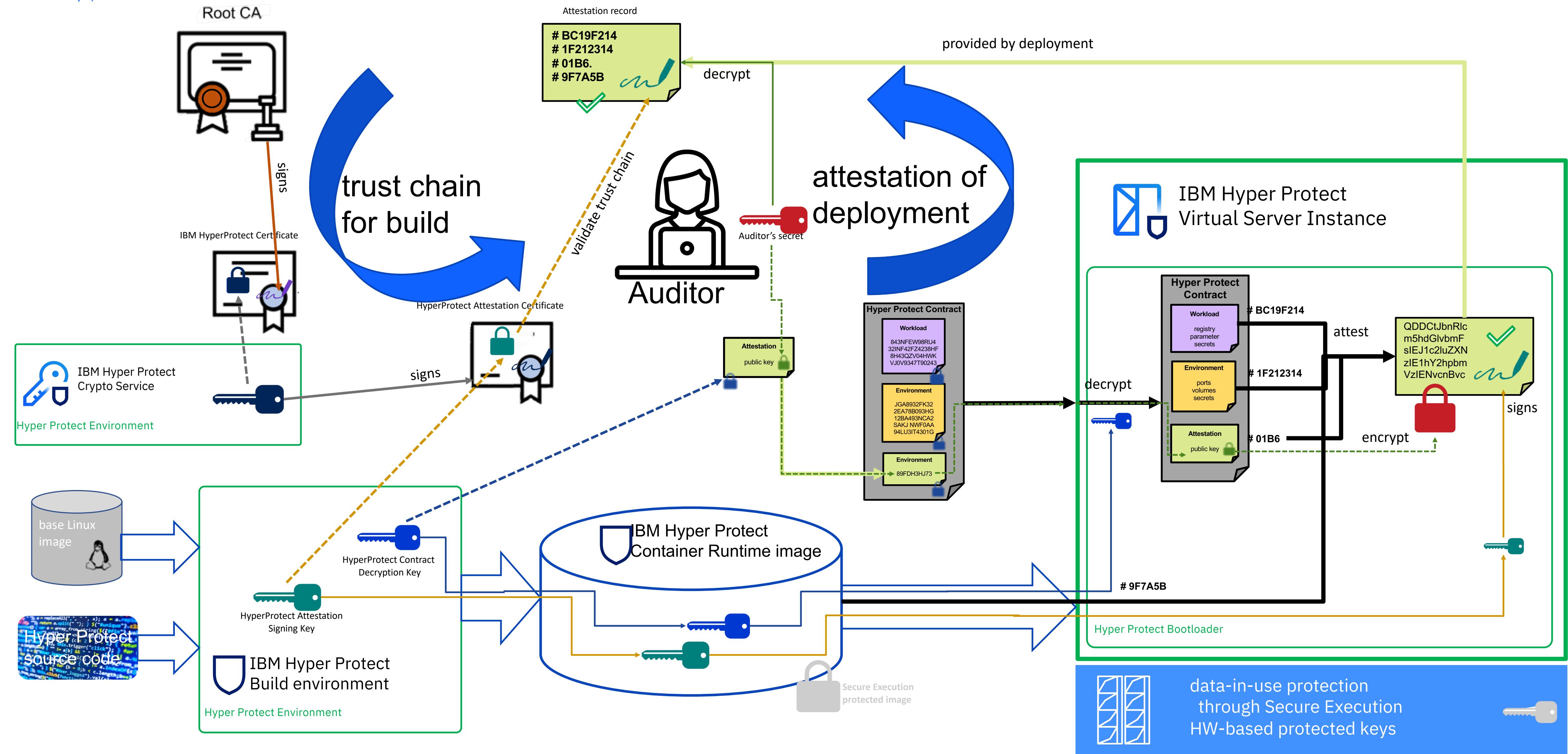
### Attestation (Auditor specific)





## Attestation record

Enables validation and proof by auditor with root of trust based in third party authority





# Built-in Data-at-rest encryption

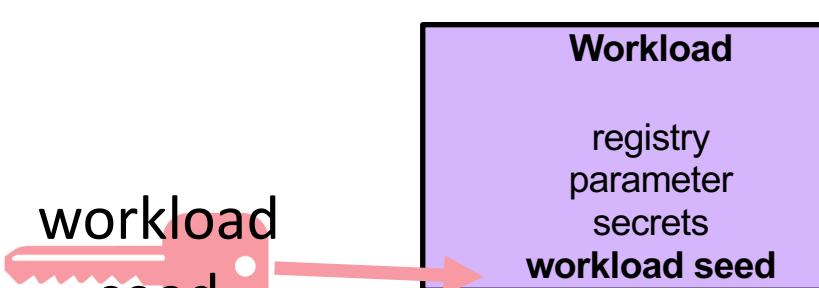
encryption key derivation within enclave with customer and workload provided seeds

## IBM Hyper Protect



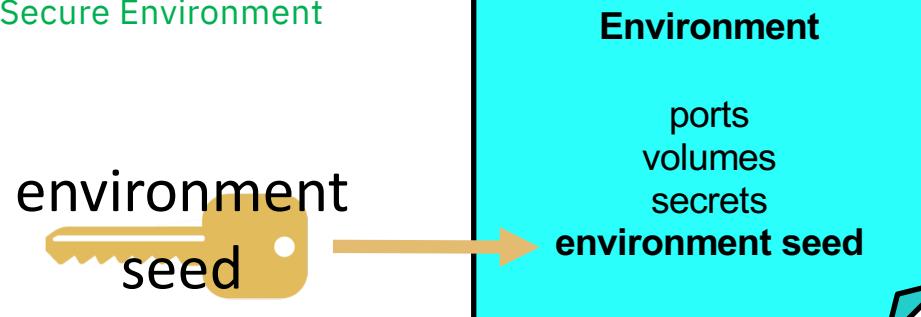
## Workload (Provider)

Secure Environment



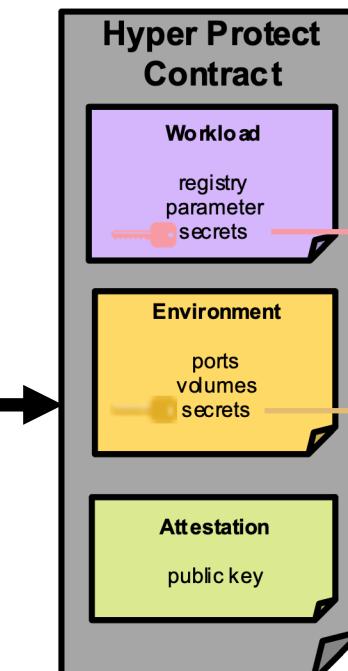
## Customer specific Environment

Secure Environment



IBM Hyper Protect  
Container Runtime

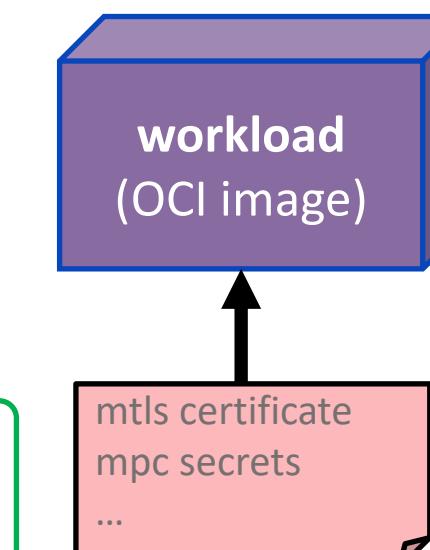
decrypt



one-way derivation

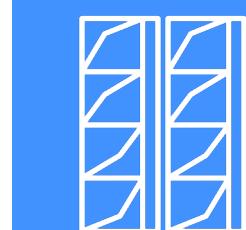
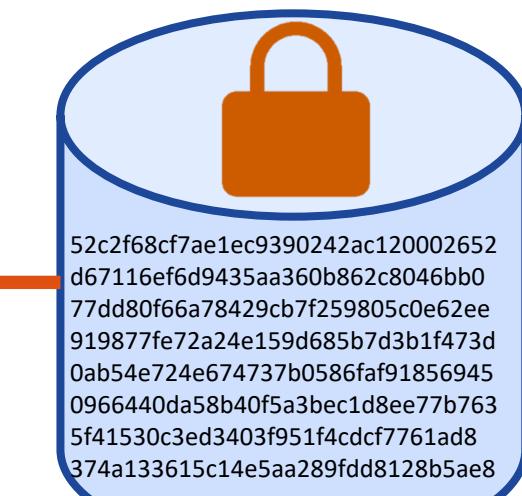
workload seed

environment seed



de/encrypt on  
LUKS layer

persistent  
data-at-rest volume  
provided by VPC



datainuse protection  
through Secure Execution  
HWbased protected keys

# Application workload provisioning

IBM Hyper Protect Container Runtime image provides the Secure KVM guest

This image provides a container runtime and starts your OCI container image

You specify a “contract” at instance provisioning that contains a Docker Compose file specifying your application workload

This contract can be in plain text, or encrypted by one or more parties, or encrypted and signed

Auditors can be given the ability to attest that the workload deployed is the expected workload and has not been tampered with

# The “contract” allows you to specify...

Docker Compose file *required*

Logging information *required*

Environmental variables for your workload

Signature over the contract

- You specify your public key so that the container runtime image can verify your signature

Credentials for registry if your OCI image is in a private registry

Public key to verify your OCI image’s signature if it is signed

Public key for auditor which allows the attestation record to be encrypted

Seeds for data volume encryption—two seeds are used to create a LUKS key, provided by different personas (workload provider and workload deployer)

IBM Hyper Protect Virtual Server - zSystems and LinuxONE		Version 1 (Secure Service Container-based)	Version 2 (Secure Execution-based)
<b>Foundational</b>	<b>Billing Granularity</b>	IFL	VCPU <sup>7)</sup>
	<b>Deployment Granularity</b>	Logical Partition (LPAR) <sup>5)</sup>	Kernel Virtual Machine (KVM)
	<b>Logging / Monitoring – customer choice</b>	No	Yes <sup>8)</sup>
	<b>BYOI<sup>1)</sup> for customer workload in OCI format</b>	Yes single container in enclave	Yes <i>multiple container in enclave (on roadmap)</i>
	<b>IBM provided base images for Linux Distro<sup>3)</sup></b>	Ubuntu 18.04 <sup>4)</sup>	Not Applicable <sup>9)</sup>
	<b>Container Repository supported<sup>3) 4)</sup></b>	IBM Cloud Container Registry DockerHub SUSE base container registry	Customer-provided Repository IBM Cloud Container Registry DockerHub SUSE base container registry
	<b>System generation</b>	z14 and beyond	z15 and beyond
	<b>Network infrastructure support</b>	OSA adapter w/ VLAN only	hypervisor virtualization provided (virtio,...) based on OSA or RoCE cards
<b>Security</b>	<b>Data-in-use protection</b>	Secure Service Container Confidential Computing on LPAR level	Secure Execution Confidential Computing on KVM level
	<b>Workload Integrity protection</b>	Docker Content Trust	Docker Content Trust Container Digest <i>RedHat Simple Signing (on roadmap)</i>
	<b>Security Value Prop</b>	Encrypted Image Boot	Encrypted Image AND Attested Boot
	<b>KYOK<sup>2)</sup> for data-at-rest</b>	Technical assured random <sup>6)</sup>	Customer Provided <i>CryptoExpress HSM-backed (on roadmap)</i>
	<b>Secure Build Service</b>	Available	Available
	<b>EP11 API (Crypto Express (CEX) Adapter)</b>	PCI Passthrough within SSC enclave	CEX Network API for Secure Execution enclaves

<sup>1)</sup> BYOI=Bring-Your-Own-Image

<sup>2)</sup> KYOK=Keep-Your-Own-Key

<sup>3)</sup> customer provided workload support and subscription

<sup>4)</sup> workload and distro related support limitation may apply

<sup>5)</sup> LPAR limitation of system applies (max. 85 LPAR/system)

<sup>6)</sup> HSM-backed only available for IBM Cloud HPVS

<sup>7)</sup> additional per IFL S&S for distro support of  
Hypervisor/LPAR applies

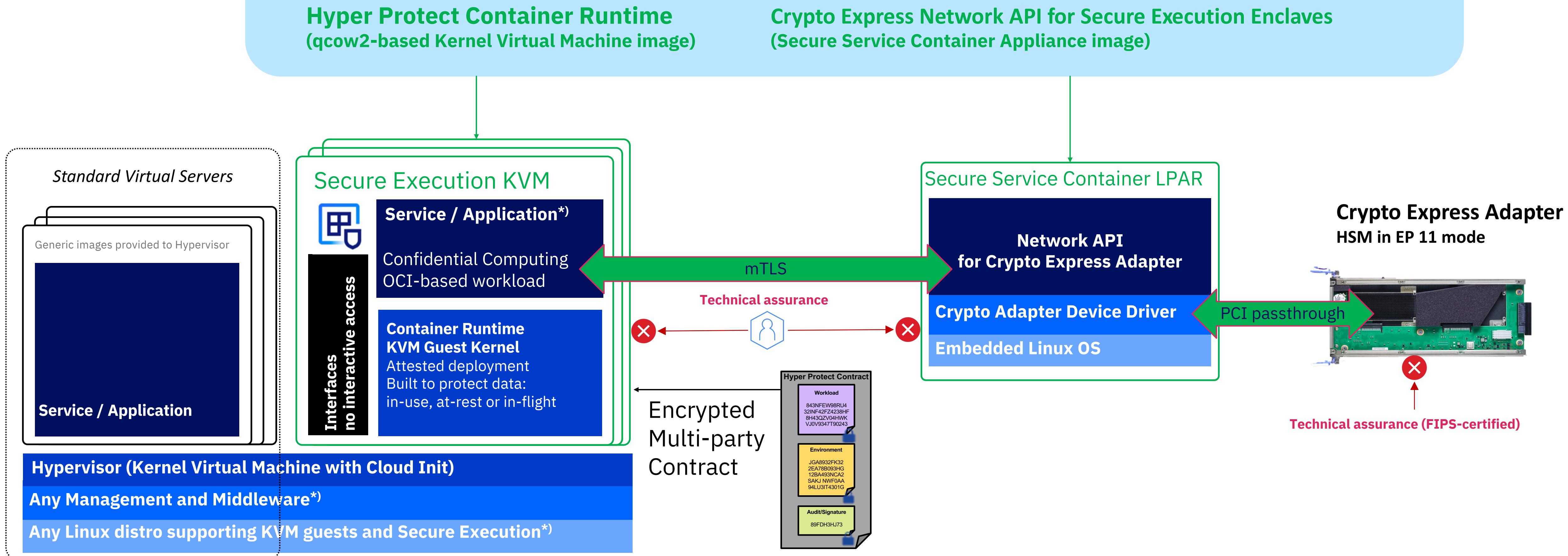
<sup>8)</sup> Flexible integration into customer provided endpoints as well as  
customer provided middleware on LPAR level

<sup>9)</sup> IBM provided and encrypted Linux image w/ container runtime  
customer provided workload through OCI image only



# IBM Hyper Protect Virtual Servers v2.1

downloadable from Passport Advantage



\*) Customer-provided. Support restrictions by 3rd party and Linux distribution provider may apply

# Additional resources

3

IBM view of Confidential Computing

<https://www.ibm.com/topics/confidential-computing>

4

Secure Execution for Linux documentation

<https://www.ibm.com/docs/en/linux-on-systems?topic=virtualization-secure-execution>

1

Today's lab:

<https://ibm-wsc.github.io/ConfidentialComputingOnLinuxONE/lab>

2

Hyper Protect Virtual Servers 2.1.x product documentation

<https://www.ibm.com/docs/en/hpvs/2.1.x>

5

GREP11 documentation

<https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-grep11-intro>

6

Hyper Protect Virtual Servers for Virtual Private Cloud on IBM Cloud

<https://cloud.ibm.com/docs/vpc?topic=vpc-about-se>

## Lab overview

Create a Secure Execution-enabled HPVS 2.1.3 guest running the GREP11 Server. Test end-to-end functionality of GREP11 client code which calls GREP11 Server which in turn calls Crypto Express Network API for Secure Execution Enclaves

1

On your own standard Ubuntu KVM guest, configure rsyslogd service to enable it to receive log messages from your HPVS 2.1.3 GREP11 Server.

2

Perform X509 certificate work to enable mutual TLS authentication between your rsyslogd service and your GREP11 Server.

3

Perform X509 certificate work to enable mutual TLS authentication between your GREP11 Server and the Crypto Express Network API for Secure Execution Enclaves server on the SSC LPAR.

4

Create a signed and encrypted contract in the format HPVS 2.1.3 expects in order to launch your own GREP11 Server as a Secure Execution-enabled HPVS 2.1.3 KVM guest.

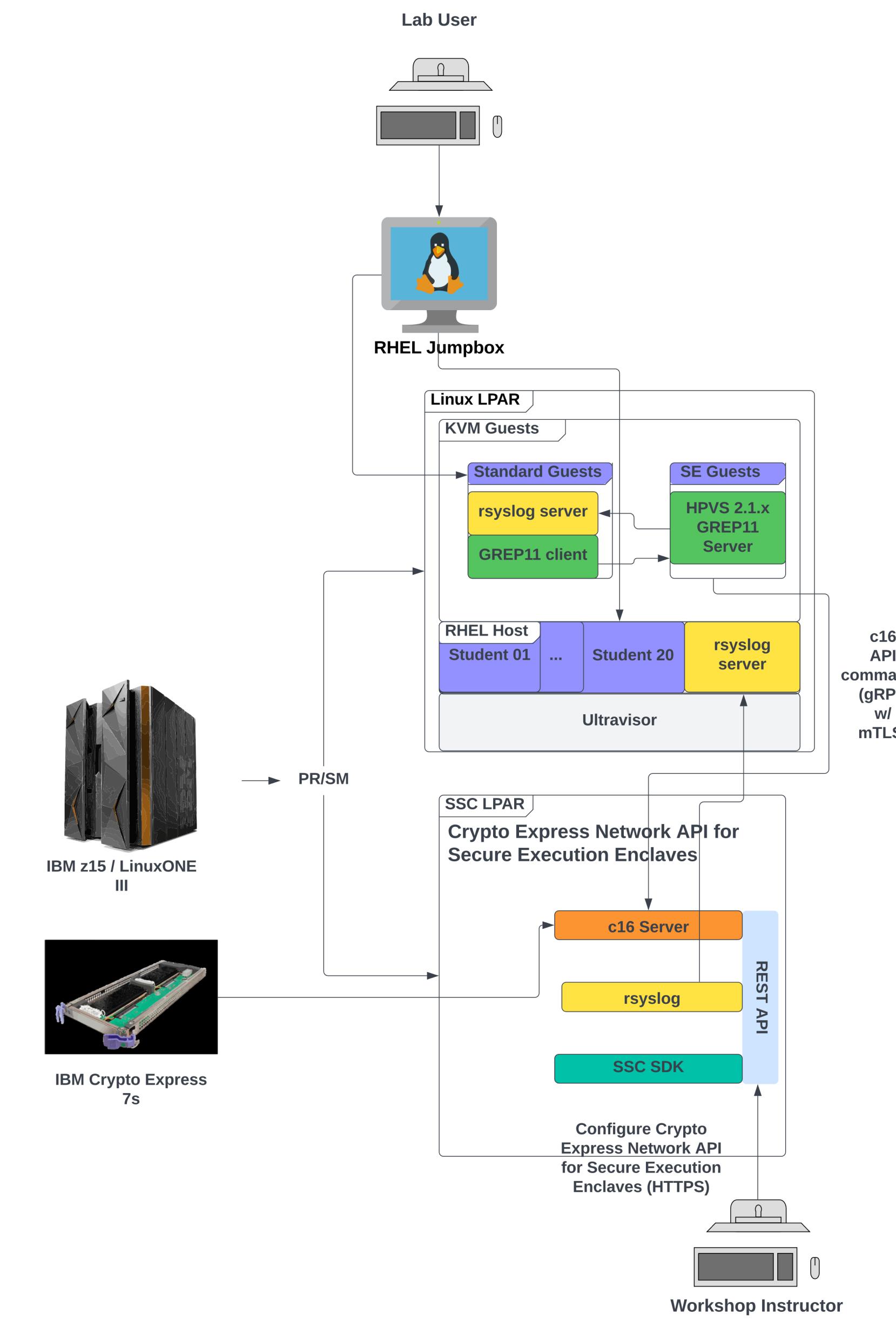
5

Perform X509 certificate work to enable mutual TLS authentication between GREP11 client code and your GREP11 Server.

6

Configure GREP11 client code to request service from your GREP11 Server and perform an end-to-end test of your setup.

# Lab topology



# The IBM Hyper Protect Platform Generation 2

## A technical overview

by Stefan Amann, Timo Kußmaul, Carsten Leue, Stefan Liesche,  
Anbazhagan Mani, Asha Shekarappa, Divya Knoor, Nicolas Mäding, James  
Magowan, Peter Morjan and Stefan Schmitt

### Table of Contents

<b>1. MOTIVATION</b>	<b>3</b>
<b>2. INTRODUCTION</b>	<b>4</b>
<b>3. UNDERLAYING TECHNOLOGY – SECURE EXECUTION FOR LINUX</b>	<b>5</b>
<b>4. HYPER PROTECT PLATFORM</b>	<b>7</b>
<b>4.1. ARCHITECTURAL CONCEPTS</b>	<b>8</b>
4.1.1. <i>Personas</i>	8
4.1.2. <i>Contract</i>	9
4.1.3. <i>Data Volume Encryption</i>	11
4.1.4. <i>3<sup>rd</sup> party Attestation of boot</i>	12
<b>4.2. HYPER PROTECT CONTAINER RUNTIME</b>	<b>14</b>
4.2.1. <i>Bootloader</i>	14
4.2.2. <i>Hyper Protect Layer Services</i>	16
4.2.3. <i>Data Volume Encryption Services</i>	17
4.2.4. <i>Workload Deployment and Considerations</i>	19
<b>5. CONSIDERATION OF TRUST</b>	<b>21</b>
5.1. <i>Leveraging Secure Execution for the Hyper Protect Platform</i>	21
5.2. <i>Hyper Protect Build Environment</i>	21
5.3. <i>Contract</i>	24
5.4. <i>Secure Build for Hyper Protect Container Runtime</i>	26
<b>6. LEVERAGE THE SECURE PLATFORM</b>	<b>27</b>
<b>6.1. IBM HYPER PROTECT VIRTUAL SERVERS FOR zSYSTEMS AND IBM® LINUXONE</b>	<b>27</b>
<b>6.2. IBM CLOUD VIRTUAL PRIVATE CLOUD (VPC)</b>	<b>27</b>
<b>7. USE CASES OF THE HYPER PROTECT PLATFORM</b>	<b>29</b>
7.1. <i>DIGITAL ASSETS</i>	29
7.2. <i>MULTI-PARTY COMPUTE</i>	30
7.3. <i>DATA PROTECTION</i>	31
7.4. <i>KUBERNETES AND CONFIDENTIAL CONTAINERS</i>	32
<b>8. SUMMARY</b>	<b>34</b>



<https://www.ibm.com/downloads/cas/GPVMWPM3>

# Thank you.

© 2023 International Business Machines Corporation  
IBM and the IBM logo are trademarks of IBM  
Corporation, registered in many jurisdictions  
worldwide. Other product and service names might be  
trademarks of IBM or other companies. A current list  
of IBM trademarks is available on  
[ibm.com/trademark](http://ibm.com/trademark).

Internal only. Do not distribute outside of IBM.  
This document is current as of the initial date of  
publication and may be changed by IBM at any time.

