GUIDE SHARE EUROPE
UK REGION

GSE UK Conference 2020
Virtually Unstoppable

Introducing IBM Hyper Protect

Jenn Francis
IBM

November 2020
Session 1AS

Agenda

- *What is Confidential Computing?*
- *What is IBM Hyper Protect?*
- *How can I leverage this technology?*

What is confidential computing?

trust

transitive verb
\ ˈtrəst \
1a: to rely on the truthfulness or accuracy of
b: to place confidence in
c: to hope or expect confidently soon

2a: to commit or place in one's care or keeping
b: to permit to stay or go or to do something without fear or misgiving

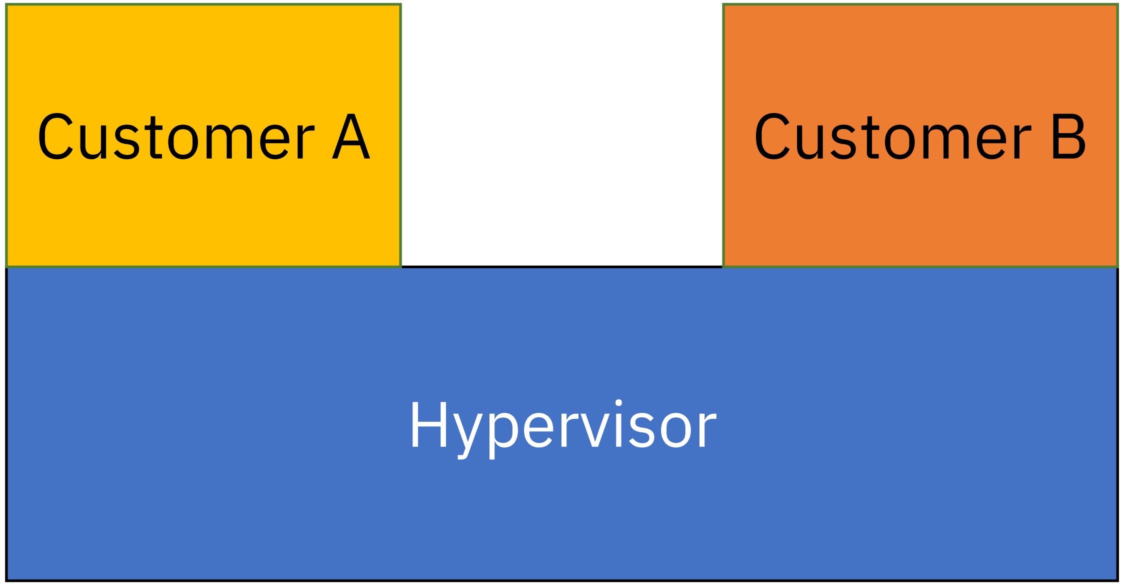
merriam-webster.com/dictionary/trust

In whom or what do you trust?

What is most important to you?

The issue . . .

Our scenario



Customer A

Running multiple applications in containers in an environment somewhere . . .

Customer B

Running multiple applications in containers in an environment somewhere . . .

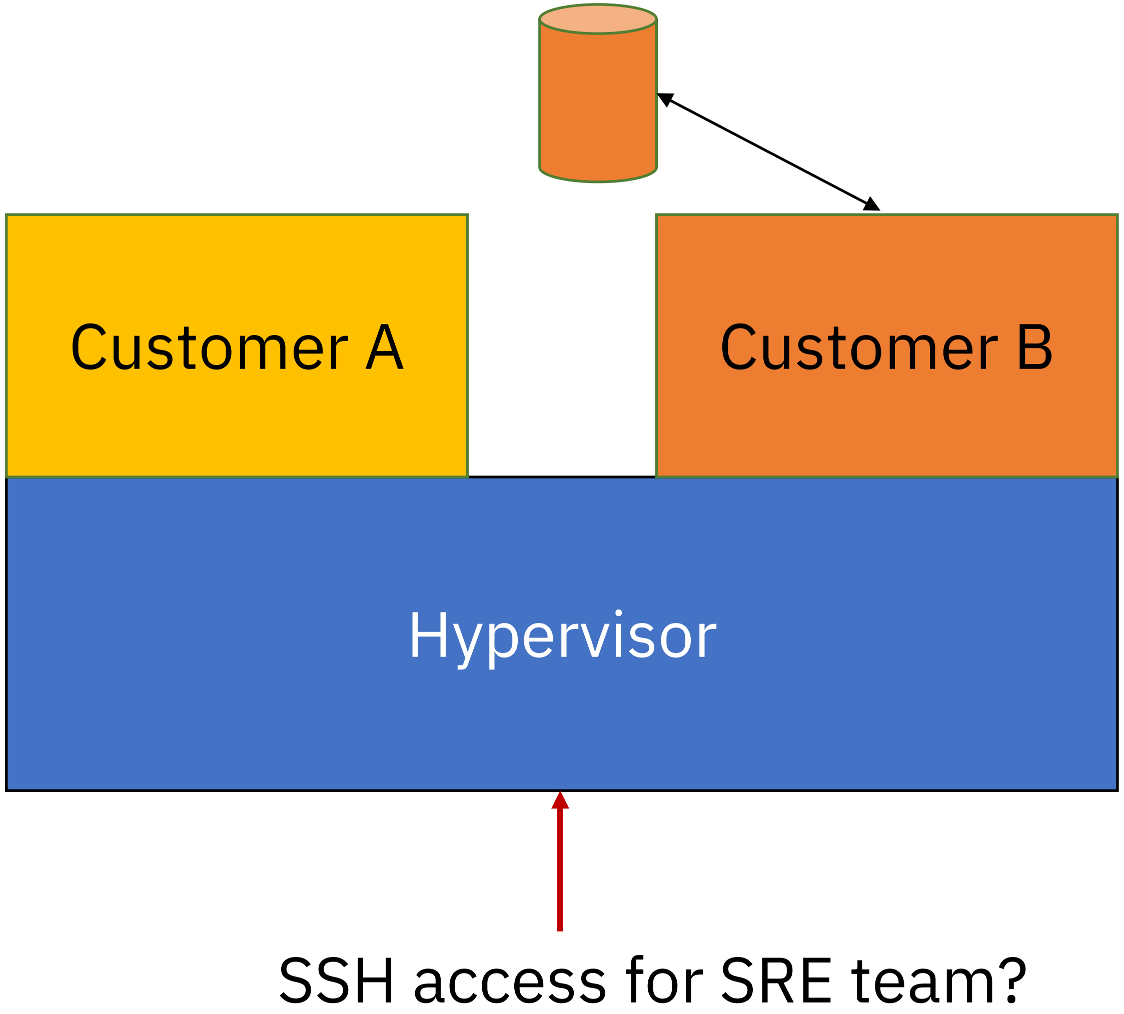
What do they have in common?

They’re unknowingly, but approvingly sharing the same hypervisor that is hosting their containers.

It’s a bit like sitting next to someone while commuting (remember those days!?), you’re sharing a host (train, plane, bus, etc.). As long as you stay seated and don’t talk, cough or touch things, you’re generally self contained.

But that isn’t real . . . So you may leave your commute with a new bestie or unknowingly with a horrible cold.

Questions we should be asking

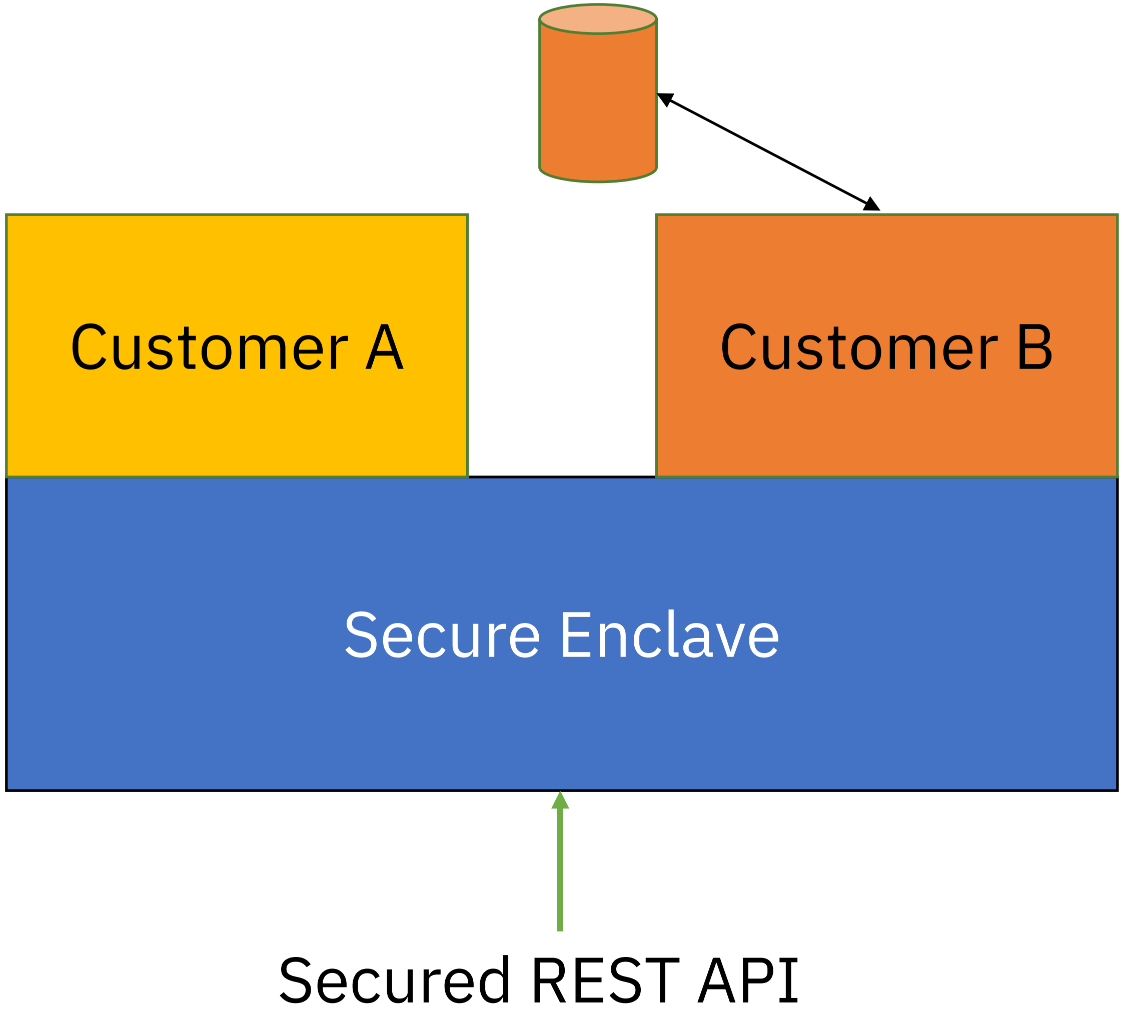


- Is my storage encrypted?
- Are the application images correct? What about verified?
- Can the Site Reliability Engineer (SRE) access my customers' data?
- How thick are the walls?
- Am I on a shared Hypervisor?
- Who has access to the hypervisor?

Addressing concerns . . .

At this point it’s all about mitigating risks.

Mitigating risks



Concern	Solution
Is my storage encrypted?	An offering with keys that never leave the box
Are application images correct? What about verified?	The ability to deploy applications through offerings like Docker Content Trust
Can the SRE access my customers' data?	A solution that removes all access methods
How thick are the walls?	Build thicker walls by utilizing options other then runc
What about the hypervisor?	Add defined, restrictive, secured REST API for the hypervisor

Introducing Confidential Computing

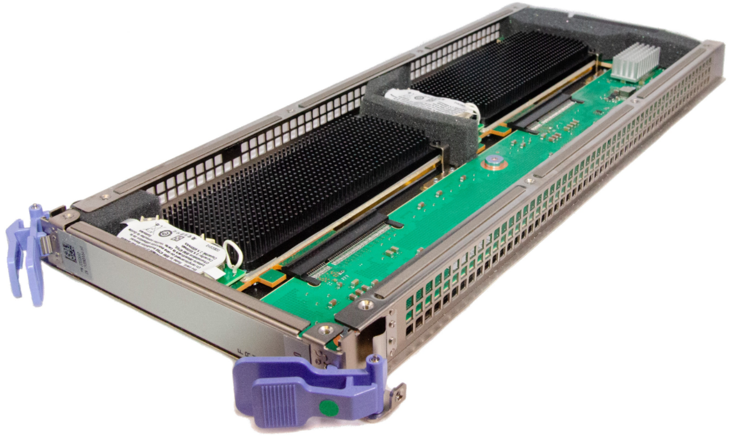
"Confidential computing uses hardware-based techniques to isolate data, specific functions, or an entire application from the operating system, hypervisor or virtual machine manager, and other privileged processes. Data is stored in the trusted execution environment (TEE), where it's impossible to view the data or operations performed on it from outside, even with a debugger."

IEEE's definition

Introducing IBM Hyper Protect

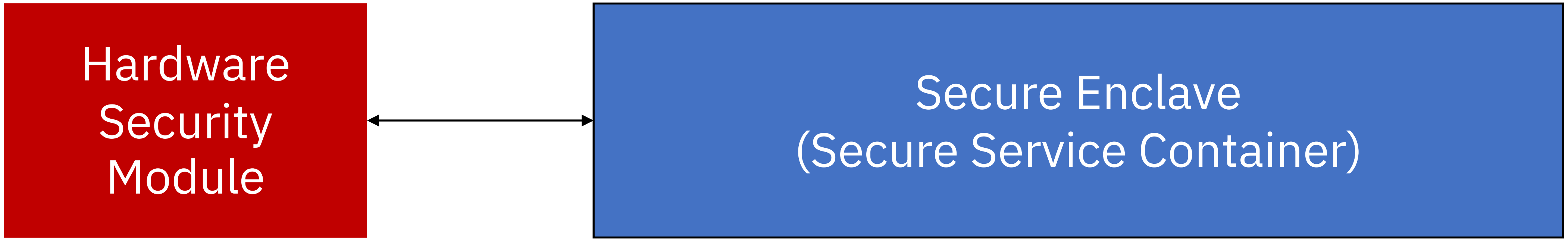
Cryptography necessitates secure key storage

Purpose built hardware device to securely store keys



Hardware Security Module
FIPS 140-2 Level 4 Certified

1. No specific physical security mechanisms are required
2. Requires features that show evidence of tampering, including tamper-evident coatings or seals
3. Attempts to prevent the intruder from gaining access, zero plaintext, etc.
4. Provide a complete envelope of protection around the cryptographic module including environmental protection



Hardware Security Module

Secure Enclave
(Secure Service Container)

Secure Enclave
(Secure Service Container)

Dynamic workloads

- Deployed as virtual machine
- Packaged and signed as docker

Backup & Restore

- Fast local snapshots
- Export/import encrypted workload backups to Cloud Object Store

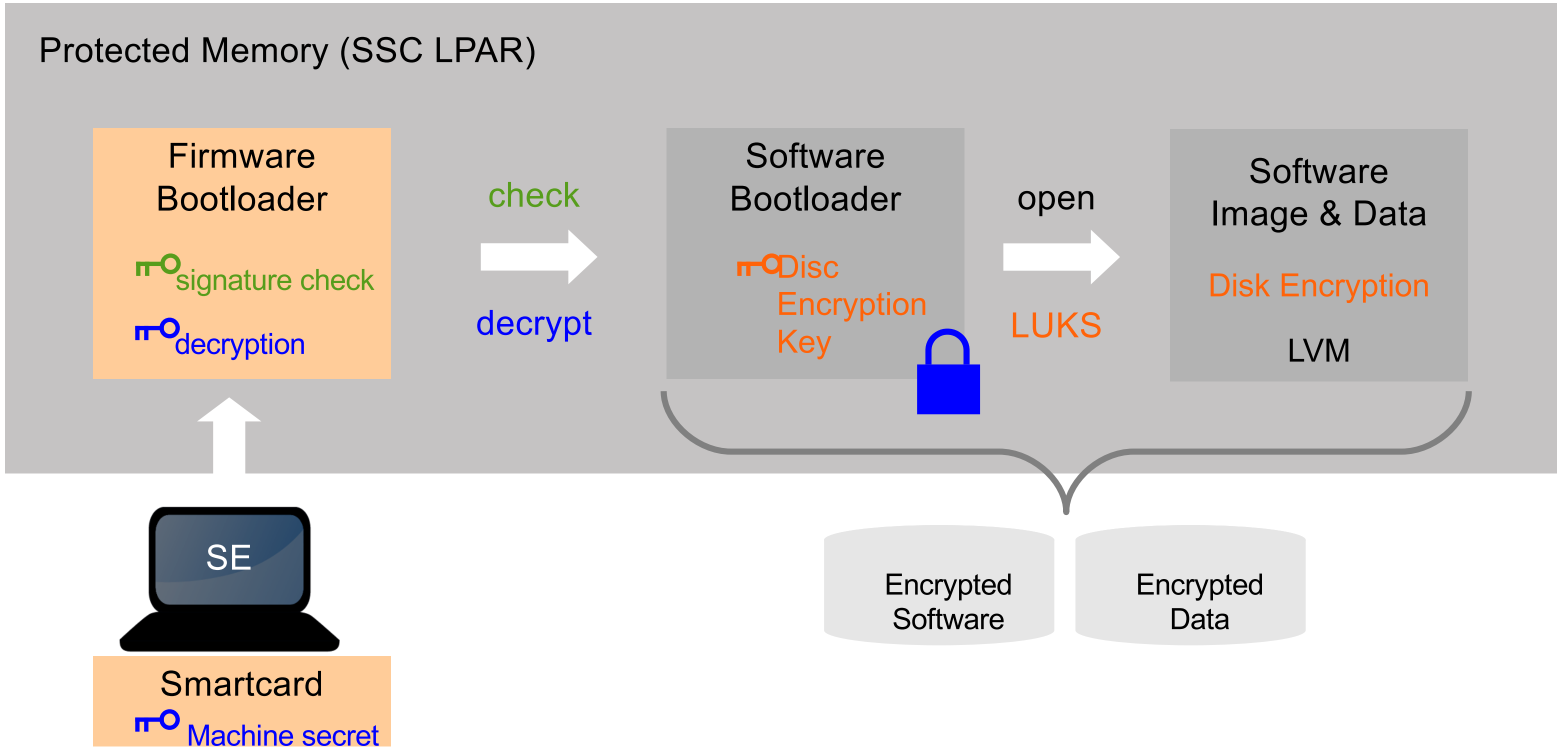
Code and data protection

- Hosting Appliance signed and encrypted at build time
    - Built in a Secure Built running on another Hosting Appliance
    - Secure boot with root key in HW/FW and protected memory
- All data disks are encrypted with Secure Service Container managed keys
    - Hosting Appliance root keys inserted by secure build

Appliance experience

- Ready to run image with all required Software
- Locked down for security and easy of use
- Updates replace all code while preserving data
- Data in separated volumes

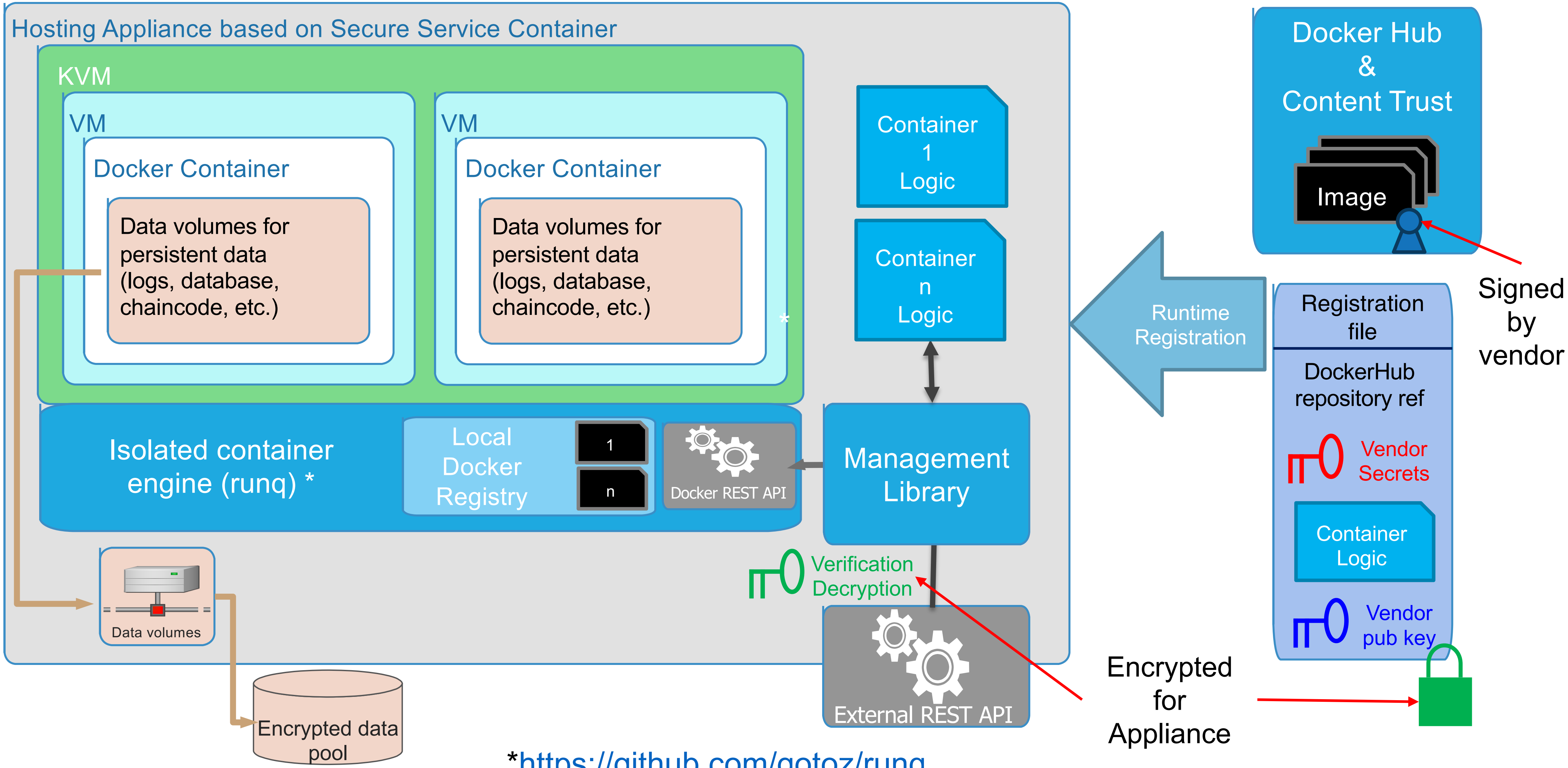
Encrypted, Signed, Tamper Resistant, Protected



Boot sequence

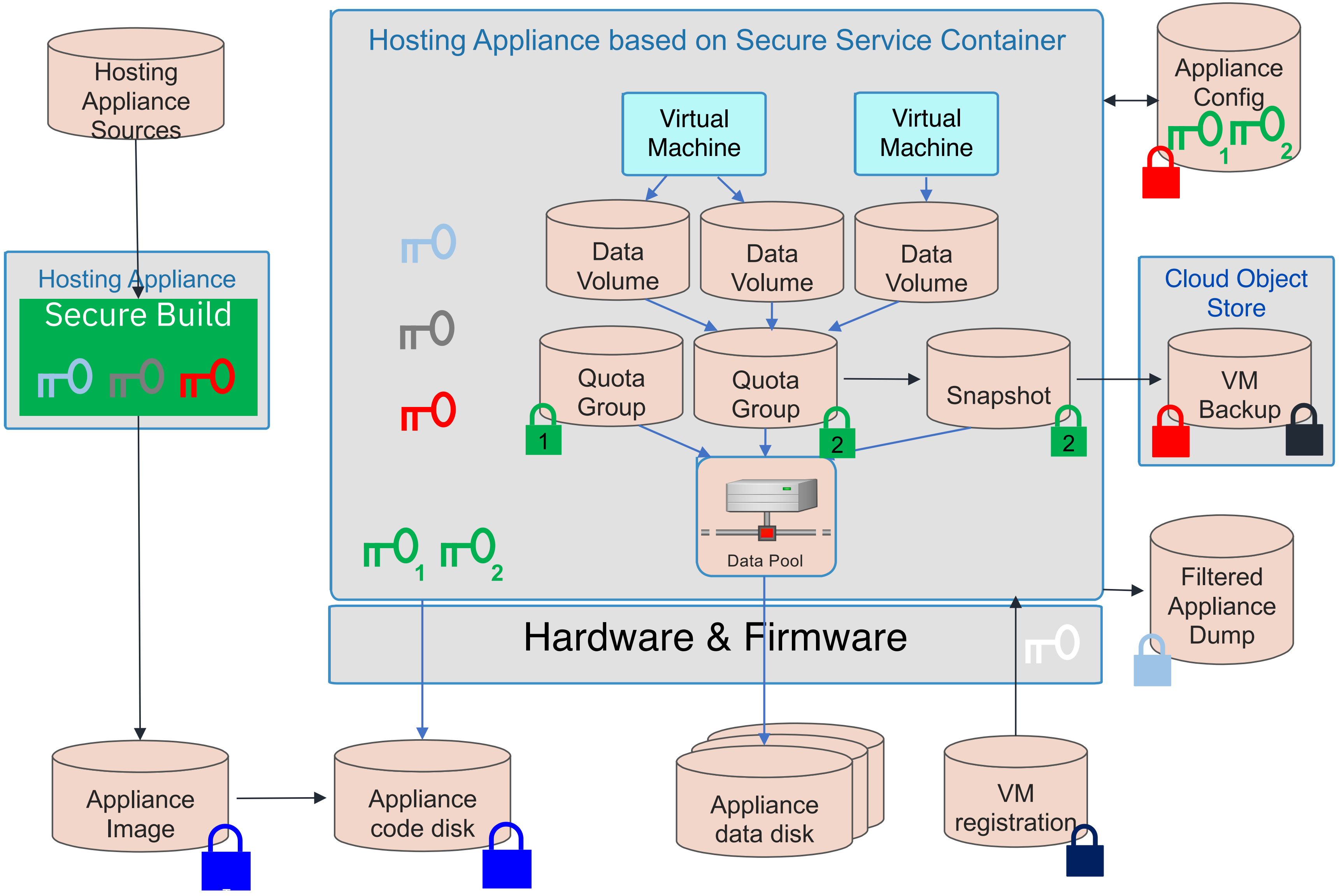
1. Firmware bootloader is loaded in memory
2. Firmware loads the software bootloader from disk
   1. Check integrity of software bootloader
   2. Decrypt software bootloader
3. Software bootloader activate encrypted disks
   1. Key stored in software bootloader (encrypted)
   2. Encryption/decryption done on the flight when accessing appliance code & data
4. Appliance designed to be managed by remote APIs only
   - REST APIs to configure Linux and apps
   - No ssh (allowed in dev mode)

Deploying workloads at runtime



*https://github.com/gotoz/runq

Code and data encryption flows



Hosting Appliance keys (inserted at secure build)

- Appliance2Vendor communication
- Vendor2Appliance communication
- Appliance2Appliance communication

Data Keys (created at runtime)

- $_1$ Quota group (logical volume)

IBM Hyper Protect Offerings

IBM Cloud Hyper Protect Services

Industry-leading security for Cloud data, digital assets and workloads

Hyper Protect Crypto Services

GA

Keep your own keys for cloud data encryption protected by a dedicated cloud HSM*

* Industry's only FIPS 140-2 level 4 certified HSM

Hyper Protect DBaaS

GA

Complete data confidentiality for your sensitive data

(PostgreSQL, MongoDB EE)

Hyper Protect Virtual Servers

GA

Instantiate Linux VMs with own public SSH key to maintain exclusive access to code and data

(Ubuntu) (BYOI)

Also available to run on-premises

IBM Cloud Hyper Protect Built On IBM LinuxONE LinuxONE secure enclaves Secure Service Container

IBM Cloud Hyper Protect Crypto Service is built on the Secure Service Container

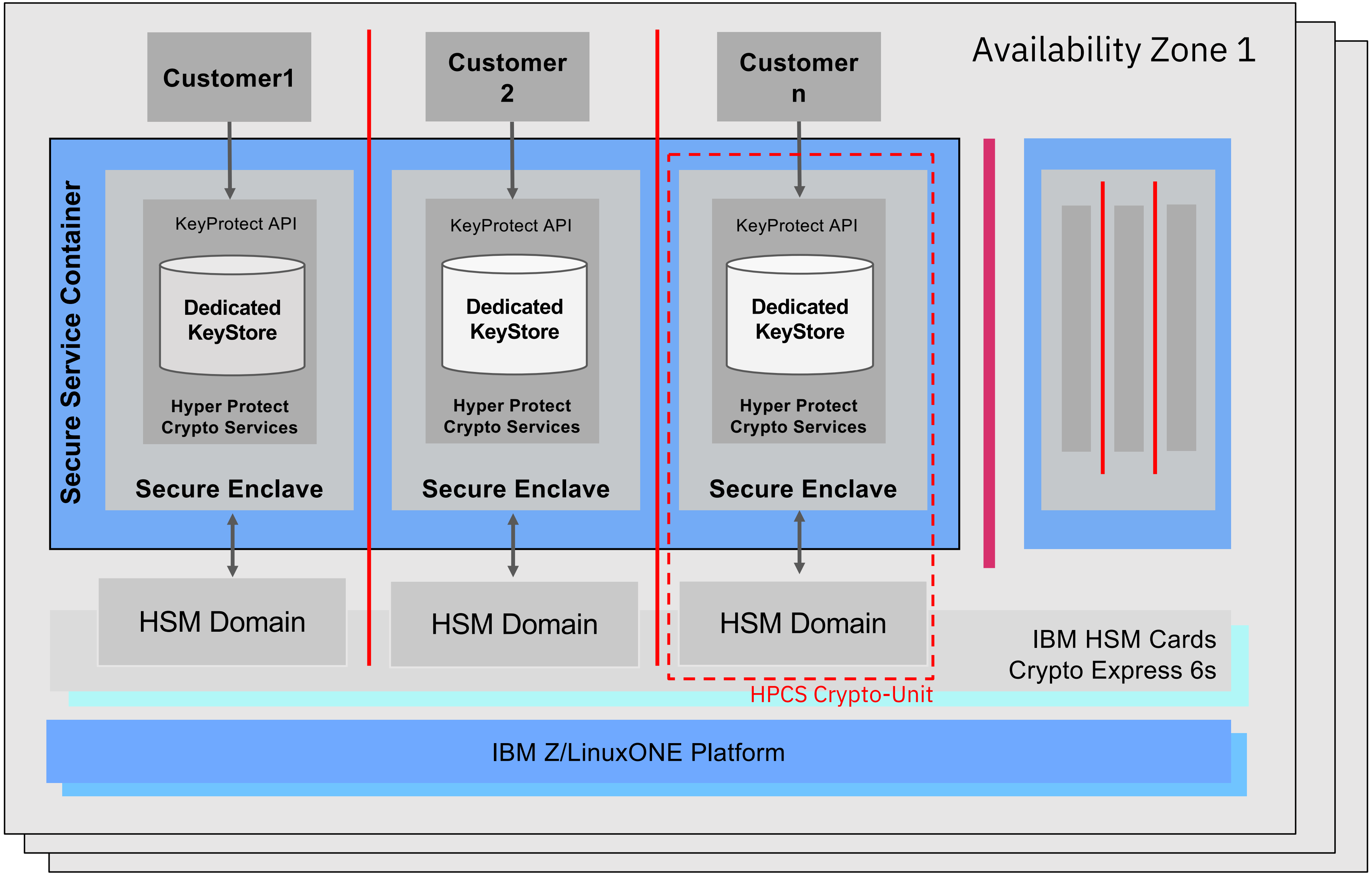
Applications and Data Services connect via KeyProtect APIs

Dedicated KeyStore per Tenant encrypted with customer unique HSM Domain master key

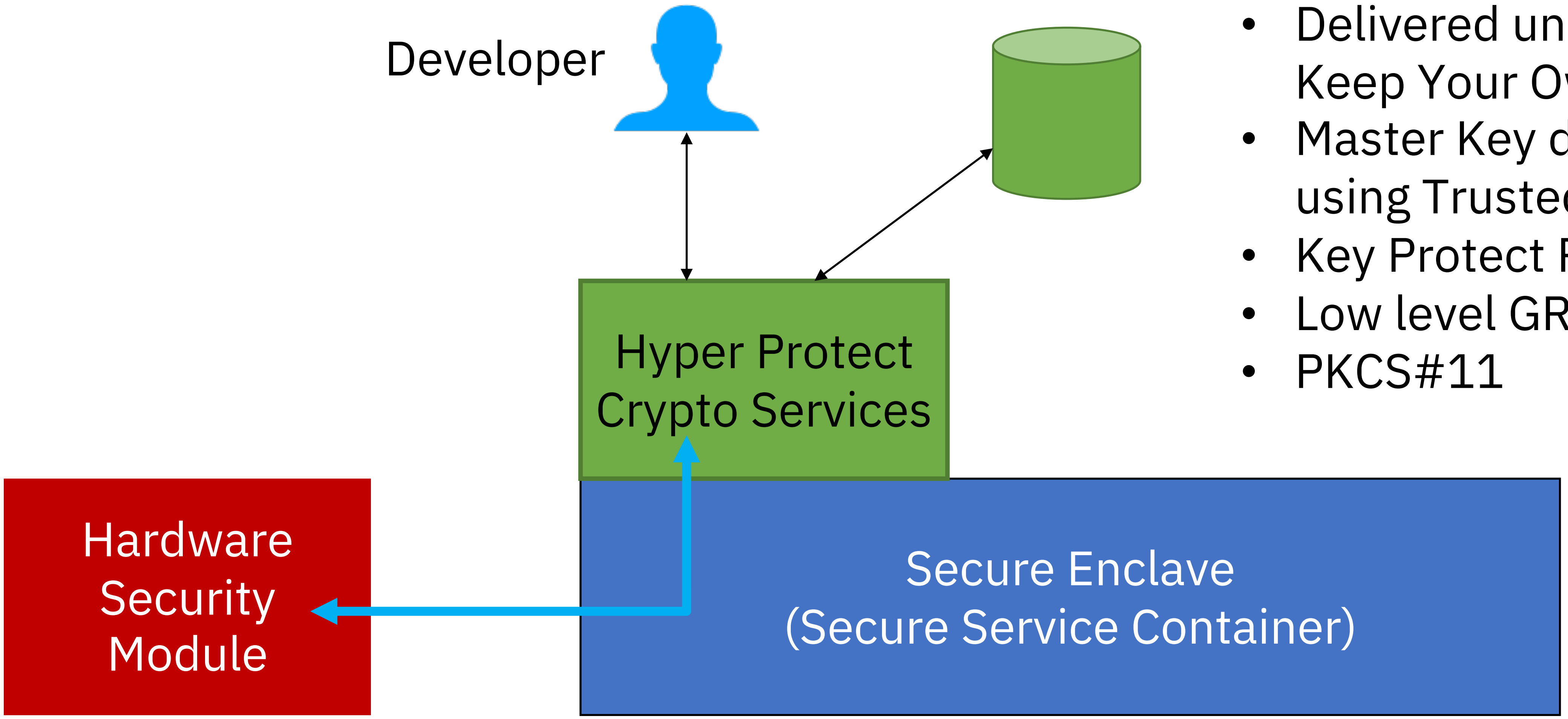
Secure enclaves ensure keys are never leaked

Secure Service Container Locked-down, tamper-resistant installation and runtime. No technical way for IBM to access runtimes or data

FIPS 140-2 Level 4 compliant HSM Domains for highest physical protection of secrets. No export of master key at all and customer root keys in clear possible.



IBM Cloud Hyper Protect Crypto Services



- Delivered unprimed: Keep Your Own Key
- Master Key defined using Trusted Key Entry
- Key Protect REST API
- Low level GREP11 API
- PKCS#11

For more information on IBM Cloud Hyper Protect Services:

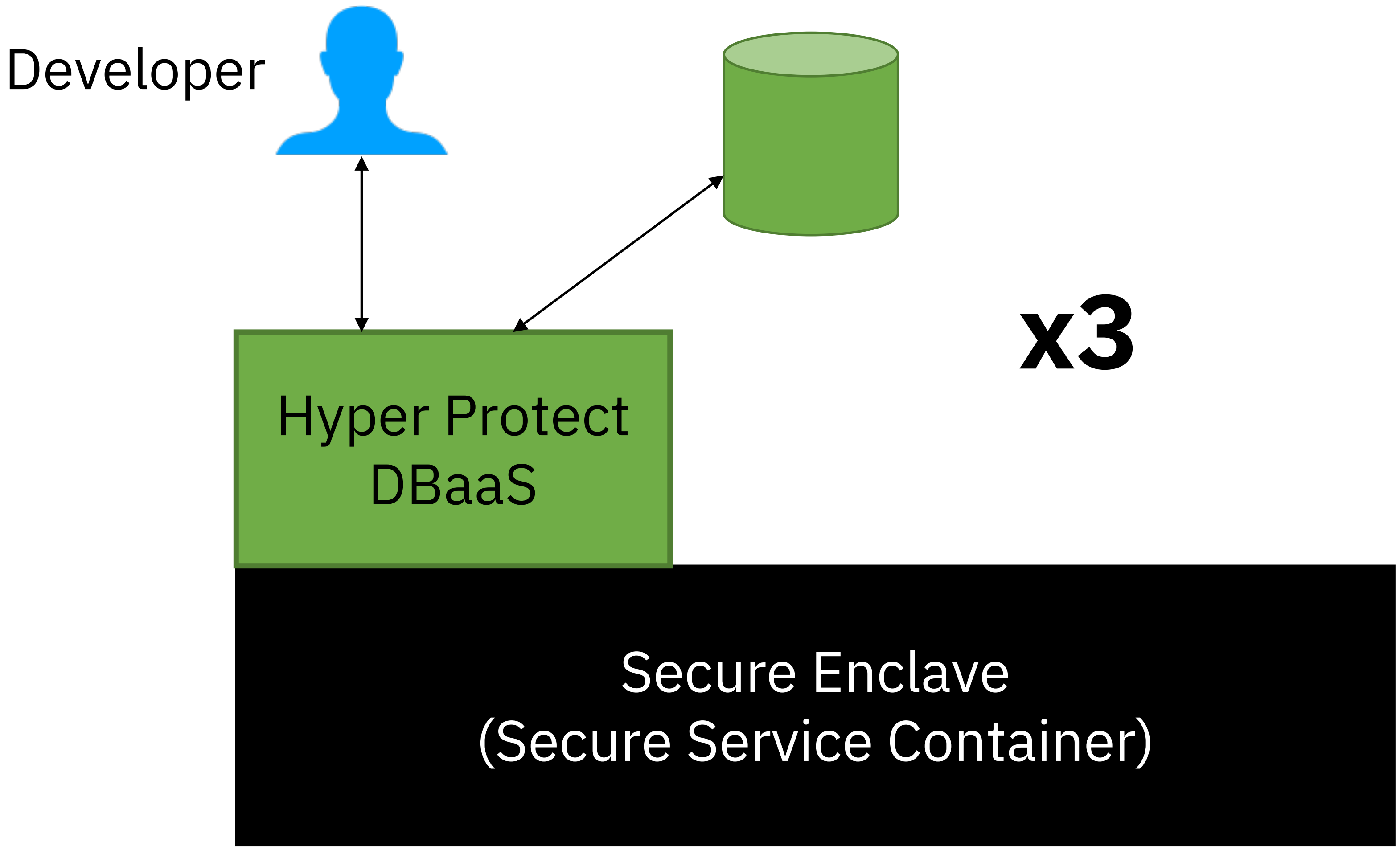
Secret Management with IBM Cloud Hyper Protect Crypto Services

Sandeep Batta

Wednesday, November 11 @ 3PM GMT

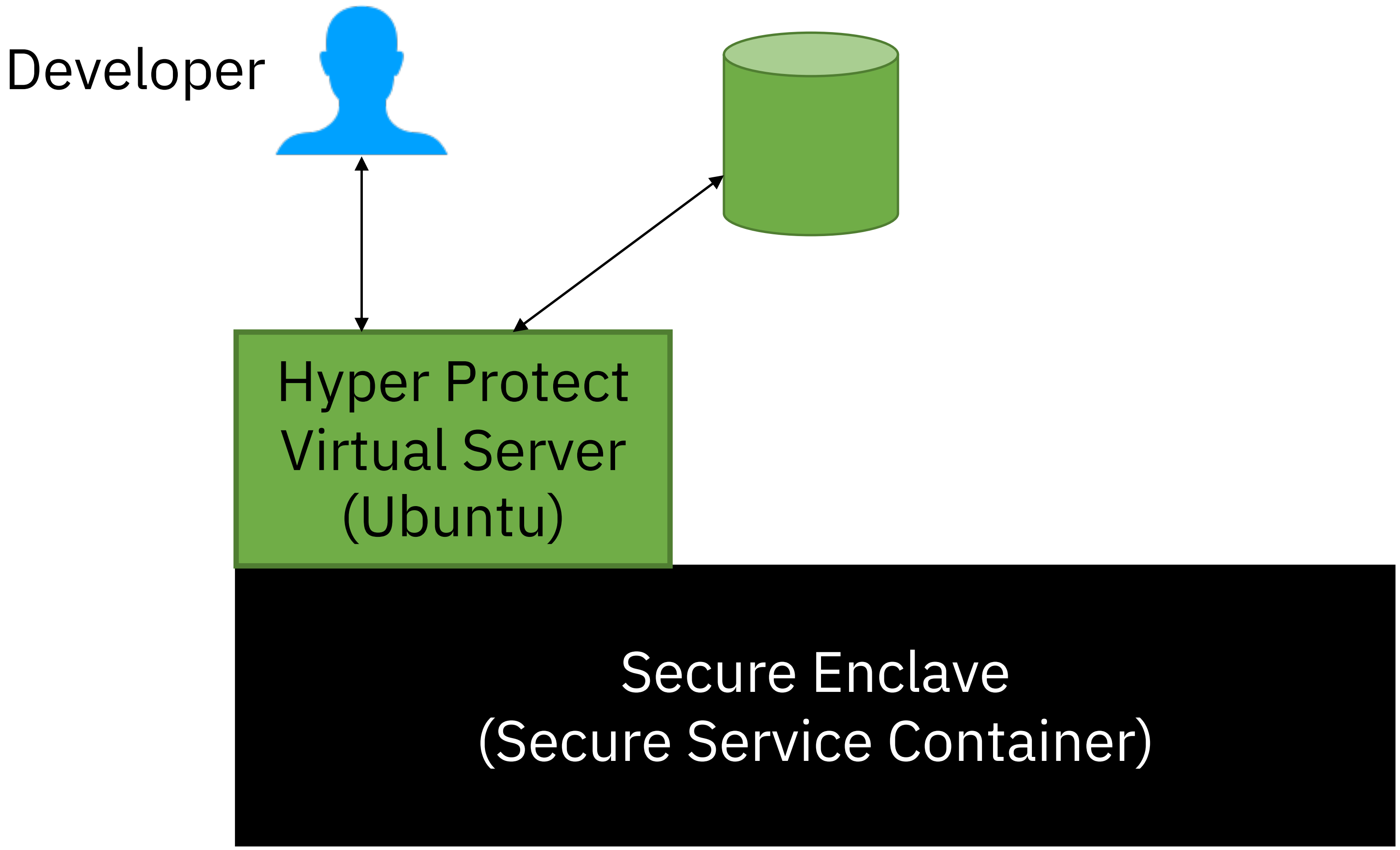
Session: 4AZ

IBM Cloud Hyper Protect Database as a Service



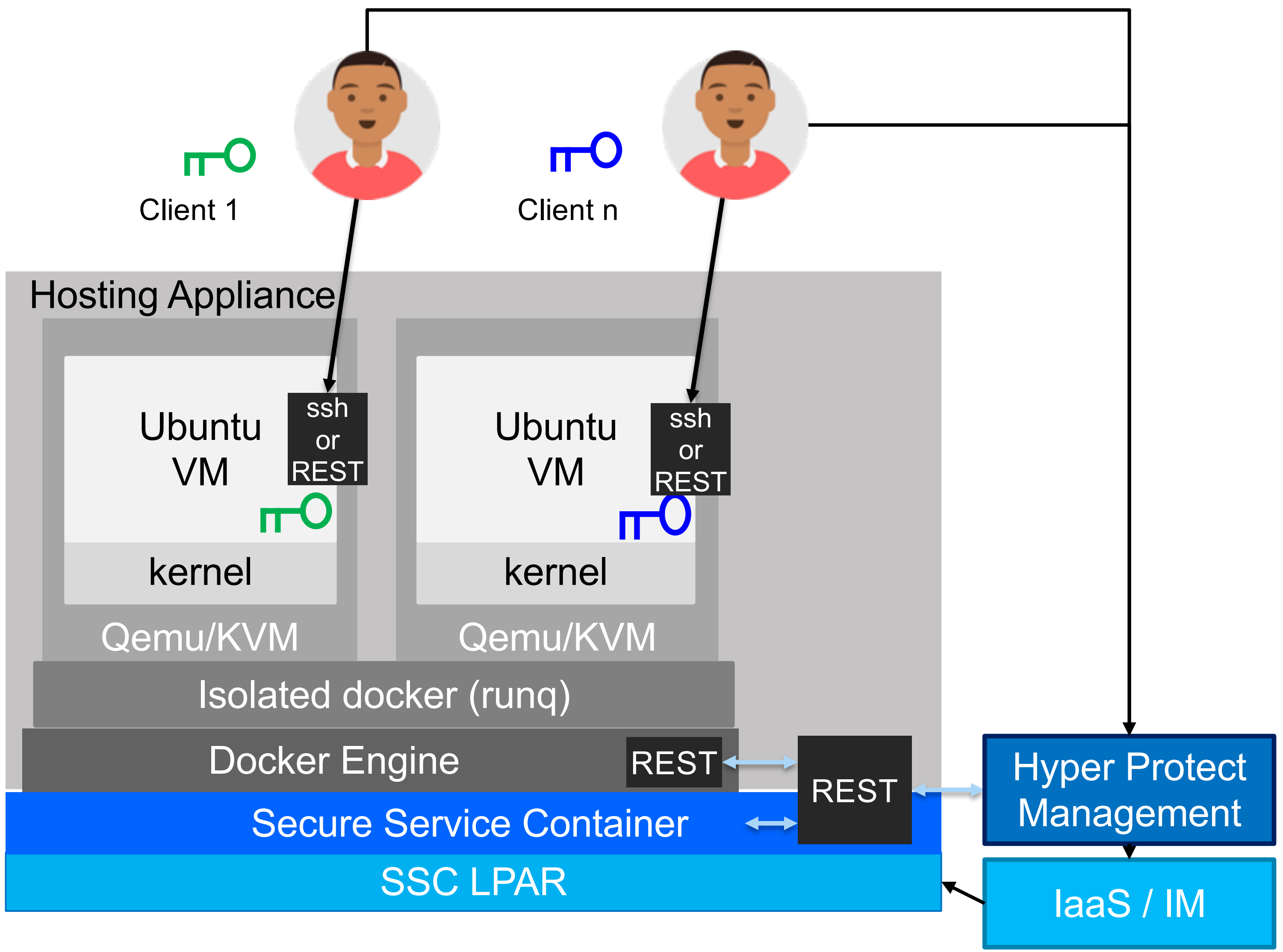
- Primary + 2 secondaries
- Fully managed
- Encryption key never leaves the enclave
- Encrypted logs & storage
- MongoDB EE
- PostgreSQL

IBM Hyper Protect Virtual Servers


Developer
Hyper Protect Virtual Server (Ubuntu)
Secure Enclave
(Secure Service Container)

- Access only via SSH with key
- Key inserted into server image, not accessible to SREs
- Ports closed by default

IBM Cloud Hyper Protect Virtual Servers



Open Virtual Machine

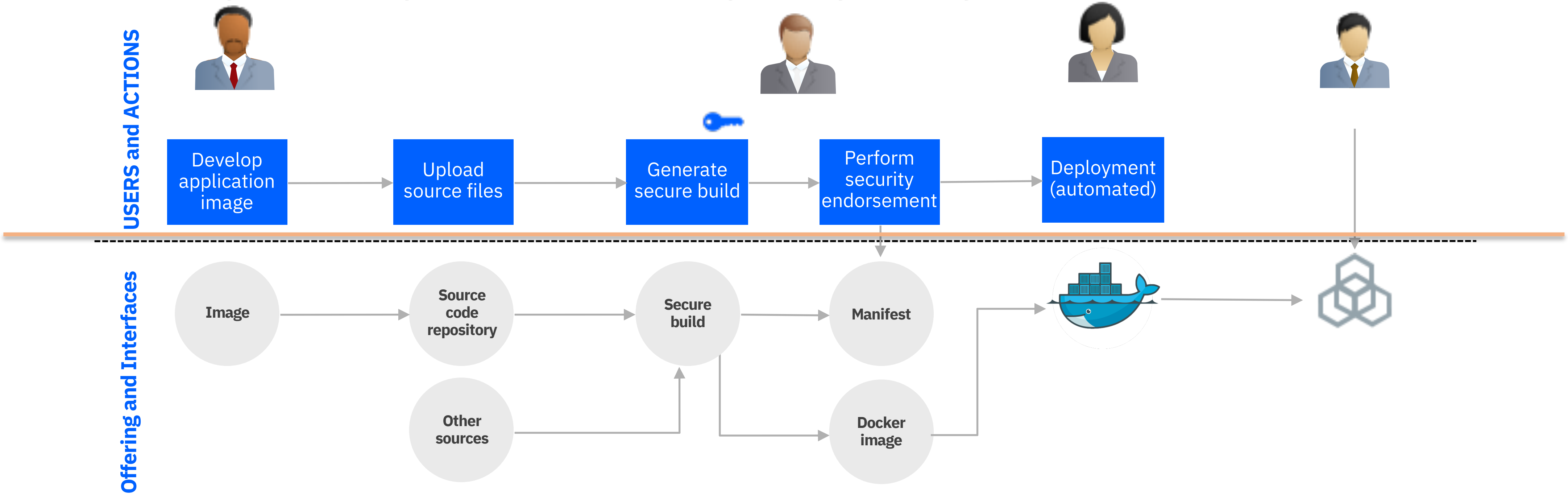
- Customer provides ssh public key at creation time
- Ubuntu (or other Linux OS) is deployed with enabled ssh in Virtual Server protected by ssh key
- **System/Appliance admin cannot get into VM**
- **Easy adoption -** can manage like regular Linux on Z VM

Locked-down Virtual Machine

- Customer/ISV builds the Virtual Server workload
- Workload deployed at build time – no need for ssh to install at runtime
- **Full SSC security value proposition** - Management done with Remote APIs&UI to the Virtual Server : lock-down access possible as done by Blockchain Enterprise and Hyper Protect services

IBM Hyper Protect Virtual Server (on-premises)

Trusted CI/CD Stages: Bring your Own Image, Sign, Register, Approve and Deploy



Workload Lifecycle Phases

- Code Development
- Workload Build
- Pre-Production
- Production

Threat Vectors pose Potential Risks

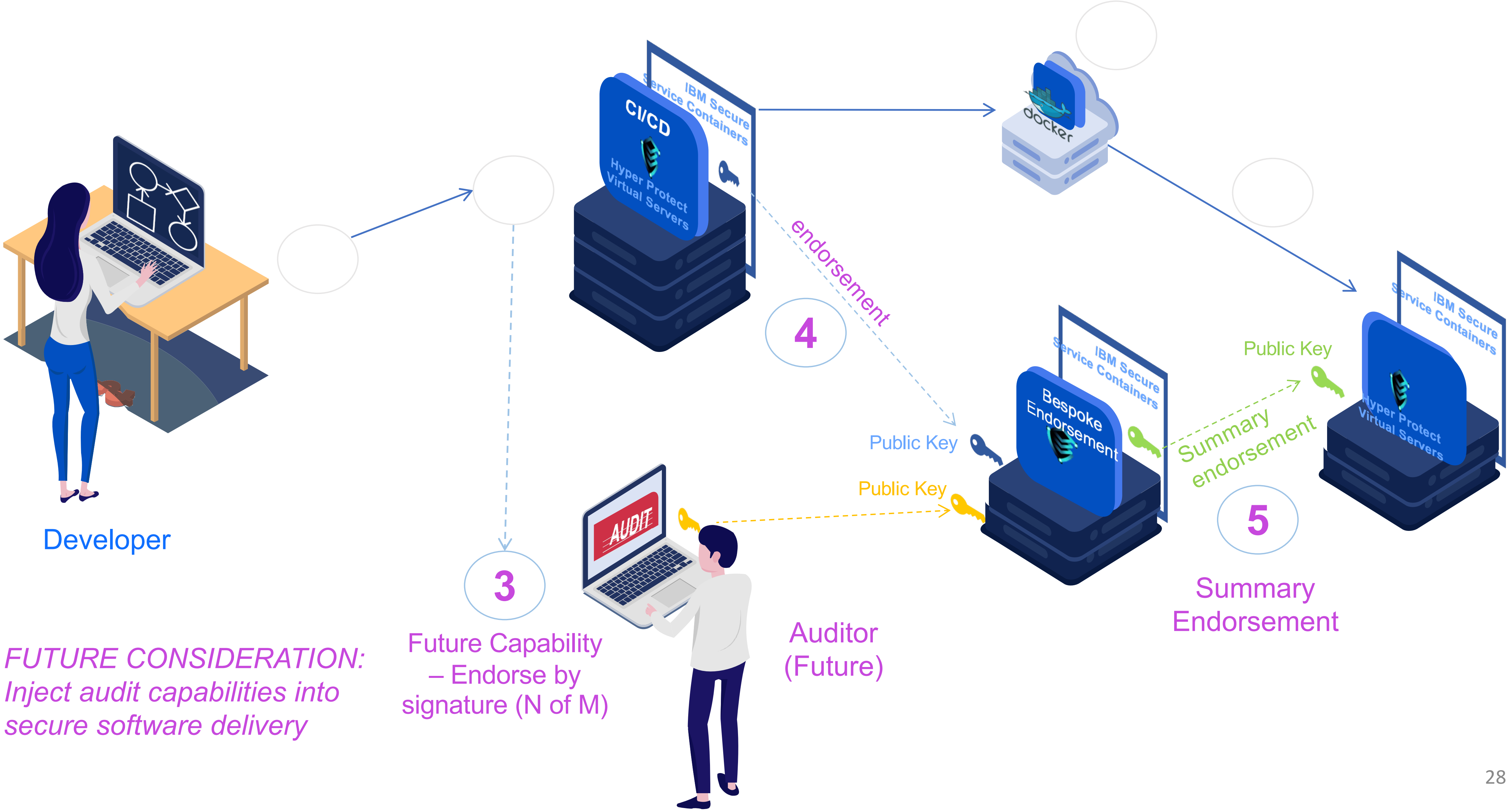
- Alter workload
- Alter build environment
- Modify workload deployment conditions
- Secrets visible to admin

How Hyper Protect Virtual Servers COMBATS risks:

- **Sign** application via secure build flow
- **Encrypt** and **register** application configuration info
- **Check image provenance** via workload **manifest**
- **Decrypt** application **registration file** – only possible via Secure Service Container (trusted execution environment)
- **Manage** infrastructure **via only RESTful interfaces**

IBM Hyper Protect Virtual Servers – A Trusted CI/CD

Secure Build Process

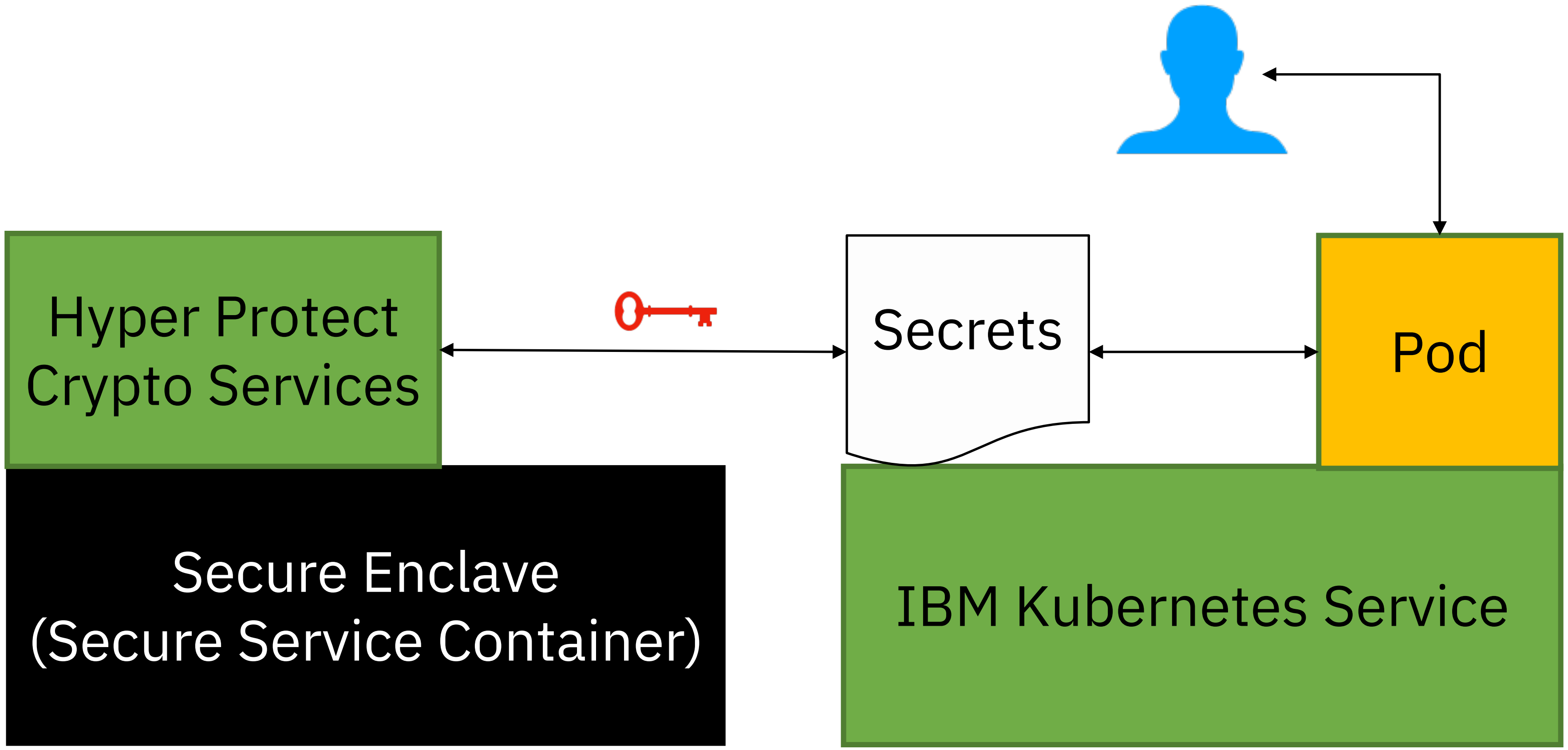


Future Capability – Endorse by signature (N of M)

FUTURE CONSIDERATION: Inject audit capabilities into secure software delivery

How IBM Hyper Protect is being used

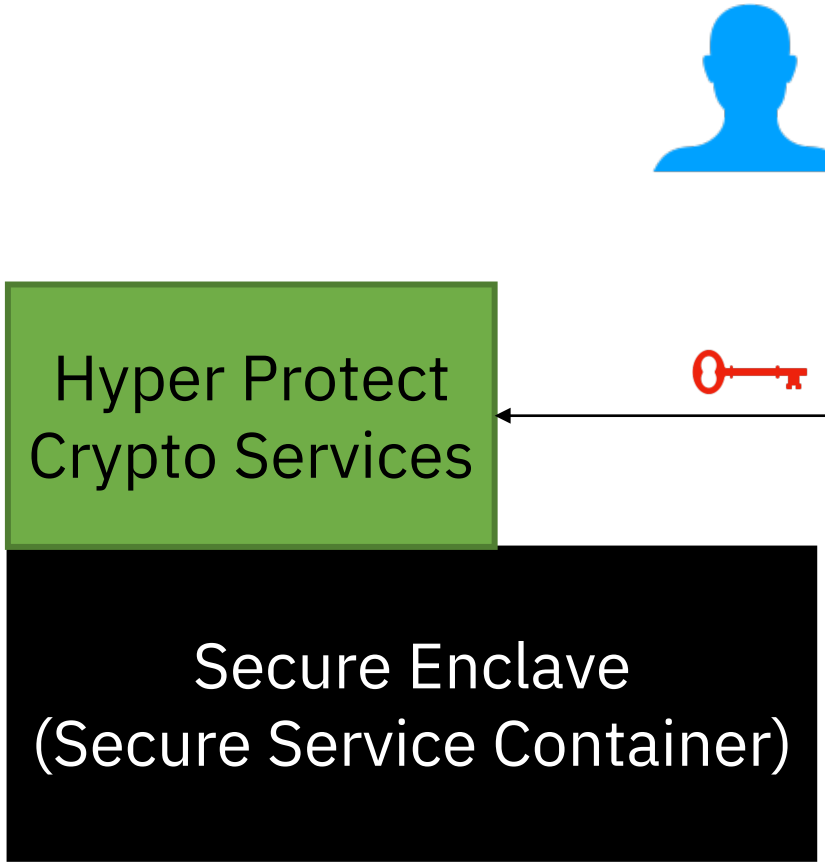
IBM Cloud Hyper Protect Crypto Services + IBM Kubernetes Service Secrets



Hyper Protect Crypto Services
Secure Enclave (Secure Service Container)
Secrets
Pod
IBM Kubernetes Service

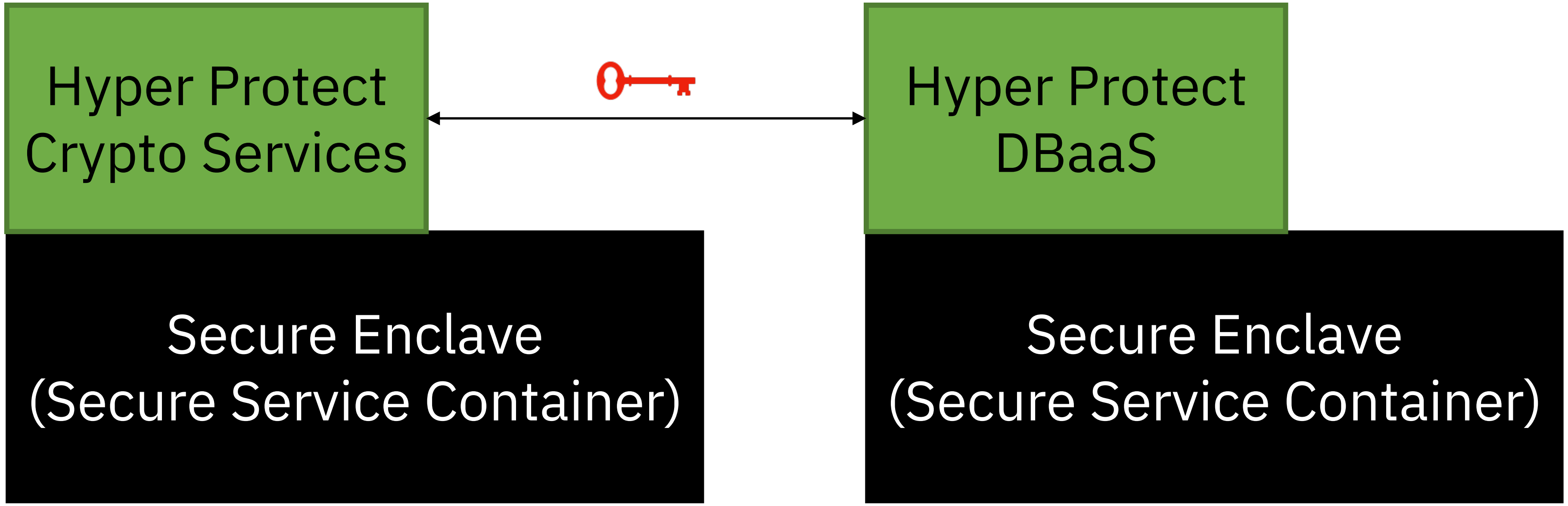
- Kubernetes can provide secrets to pods: OAuth tokens, passwords, etc.
- Pods can read secrets when stood up
- Transparent encryption of secrets

IBM Cloud Hyper Protect Crypto Services + IBM Cloud Object Storage



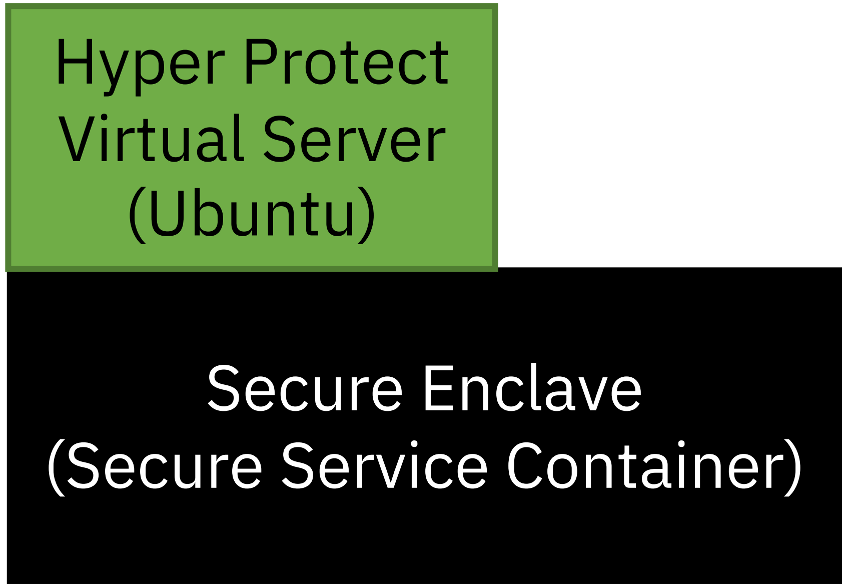
- Connect the services to encrypt objects put into a bucket
- Backup and recovery
- Data archiving
- Binary blob storage

IBM Cloud Hyper Protect Crypto Services + IBM Cloud Hyper Protect DBaaS (KYOK)


Hyper Protect Crypto Services
Hyper Protect DBaaS
Secure Enclave (Secure Service Container)
Secure Enclave (Secure Service Container)

- KYOK: store the key in the HSM
- Use tamper-resistant hardware

Hyper Protect Virtual Servers



Hyper Protect Virtual Server (Ubuntu)

Secure Enclave (Secure Service Container)

- Secure CICD server: use it to build and/or run your applications
- Offsite build: docker doesn’t cross-compile
- Only production-ready cloud s390x Linux platform
- Quickly spin up dev/test systems with reduced overhead of cost and time

IBM **Cloud**

BANK OF AMERICA

World's first Financial Services-ready public cloud

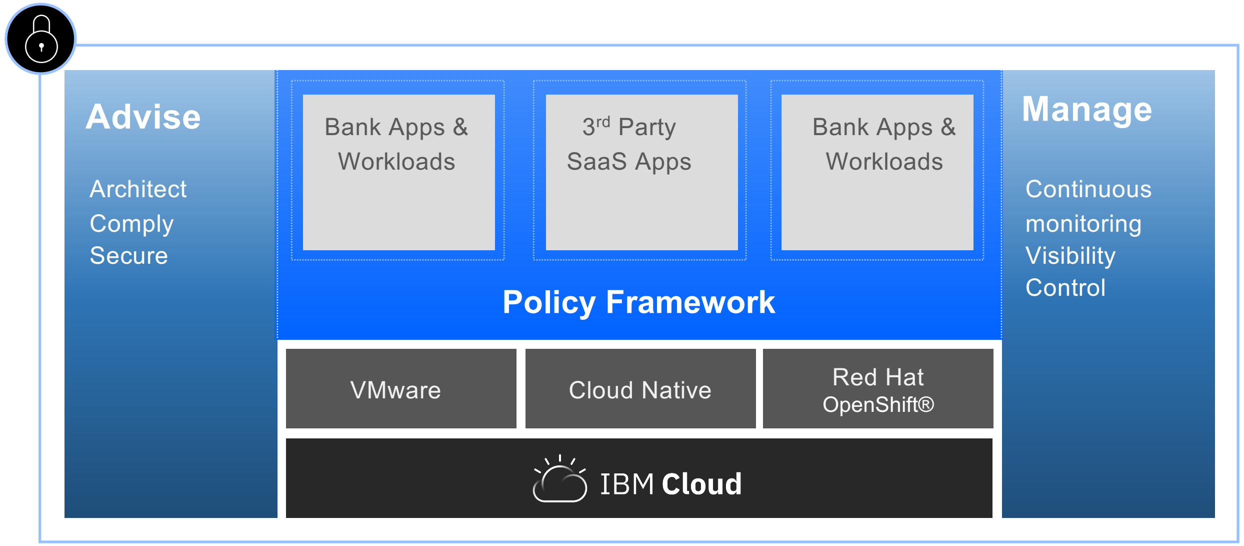
In collaboration with Bank of America, IBM Cloud is making public cloud **Financial Services-ready** by delivering the benefits and flexibility of a public cloud in a secure environment, enabling financial institutions, ISVs and SaaS solutions to host apps and workloads in the cloud with confidence and trust.

Robust Financial Services policy framework

Extensive infrastructure services – VMware, cloud-native, RedHat OpenShift as-a-service

Secure and enterprise grade, built on IBM's public cloud

Promontory risk analysis and security regulation consulting and expertise on-demand.



Financial Services-Ready Public Cloud

IBM Cloud today offers unique technologies for trusted computing:

- Monitoring and security to the microchip level
- Highest level of encryption certification
- Robust isolation options and data protection
- Data immutability with Hyper Protect Services
- Risk analysis, security consulting, and IBM Promontory industry expertise.

IBM Hyper Protect + Apple CareKit

Enables iOS developers to hyper protect consumers' personal health information.

The IBM Hyper Protect iOS SDK for CareKit is available in the CareKit open-source community, simplifying integration with the IBM Cloud Hyper Protect Services.

https://developer.ibm.com/blogs/using-ibm-cloud-hyper-protect-services-with-apple-carekit/

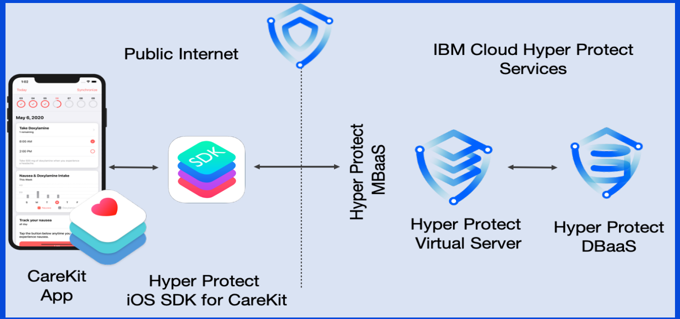
BENEFITS

- Complete data confidentiality
- Simplifies developer experience
- Works with new and existing CareKit applications
- Accelerates time to market for healthcare apps

WHY

End-to-end security:

Consumers want assurances their information is protected.

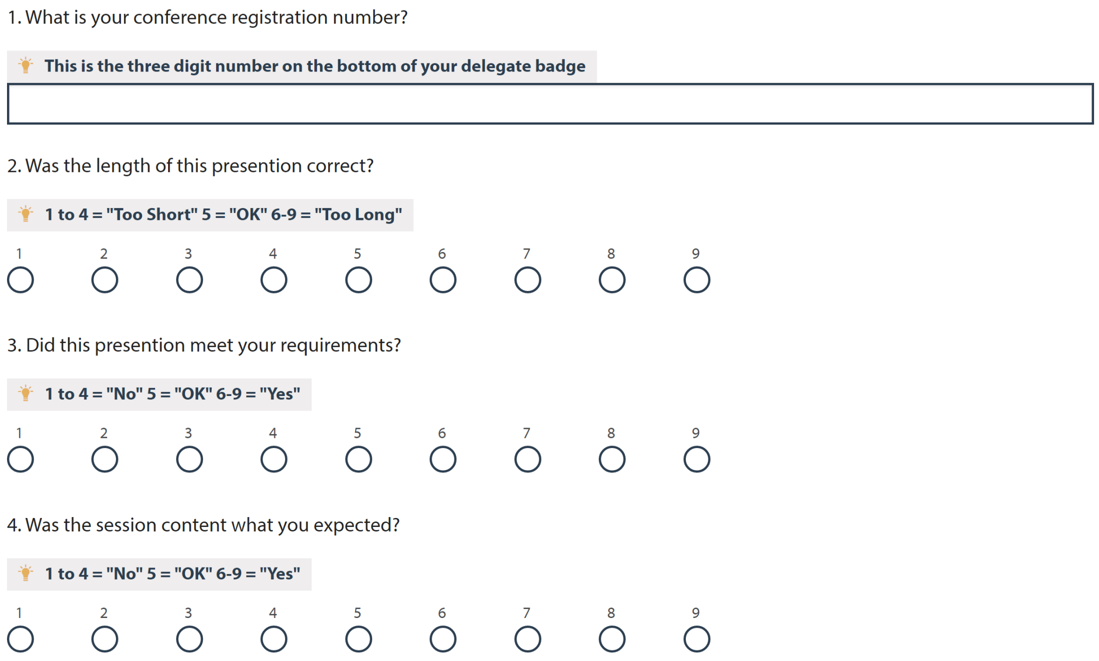

Public Internet
IBM Cloud Hyper Protect Services
Hyper Protect MBaaS
Hyper Protect Virtual Server
Hyper Protect DBaaS
SDK
CareKit App
Hyper Protect iOS SDK for CareKit

Integrating IBM Hyper Protect SDK for iOS with Apple CareKit, simplifies the ability for developers to ensure end-to-end security from the Apple device to the IBM Cloud.

- Paul Giani, Vice President & Global Leader - Apple Partnership, IBM

Please submit your session feedback!

- Do it online at http://conferences.gse.org.uk/2020/feedback/1as
- This session is 1AS



1. What is your conference registration number?

This is the three digit number on the bottom of your delegate badge

2. Was the length of this presention correct?

1 to 4 = "Too Short" 5 = "OK" 6-9 = "Too Long"

1	2	3	4	5	6	7	8	9
○	○	○	○	○	○	○	○	○

3. Did this presention meet your requirements?

1 to 4 = "No" 5 = "OK" 6-9 = "Yes"

1	2	3	4	5	6	7	8	9
○	○	○	○	○	○	○	○	○

4. Was the session content what you expected?

1 to 4 = "No" 5 = "OK" 6-9 = "Yes"

1	2	3	4	5	6	7	8	9
○	○	○	○	○	○	○	○	○

GSE UK Conference 2020 Charity

- The GSE UK Region team hope that you find this presentation and others that follow useful and help to expand your knowledge of z Systems.
- Please consider showing your appreciation by kindly donating a small sum to our charity this year, NHS Charities Together. Follow the link below or scan the QR Code:

http://uk.virginmoneygiving.com/GuideShareEuropeUKRegion

GSE GUIDE SHARE EUROPE UK REGION

NHS CHARITIES TOGETHER