

Secret Management with IBM Cloud Hyper Protect Crypto Services

Sandeep Batta
IBM

November 2020
Session **4AZ**



Secret Management: What? Why? How?

What are Secrets?

Secrets are Digital Authentication Credentials used in Applications, Services, Privileged Accounts, etc

- IAM Credentials, SSH Keys
- API and other applications Keys / Credentials
- Authentication Tokens, Certificates
- Private Encryption Keys

Challenges

- Millions of secrets in an enterprise
- Secret Sprawl
 - Hardcoded application identities
 - Plain-text usernames / passwords / API-Keys embedded in scripts, configuration files, etc
 - Certificates & Encryption Keys stored in File Systems
- Difficult to track and handle security events

An Enterprise wide Secret Management strategy will enable moving from “Host-Based” identity to “Application-Based” identity to enhance security in a “Zero Trust” network environment with multiple clouds

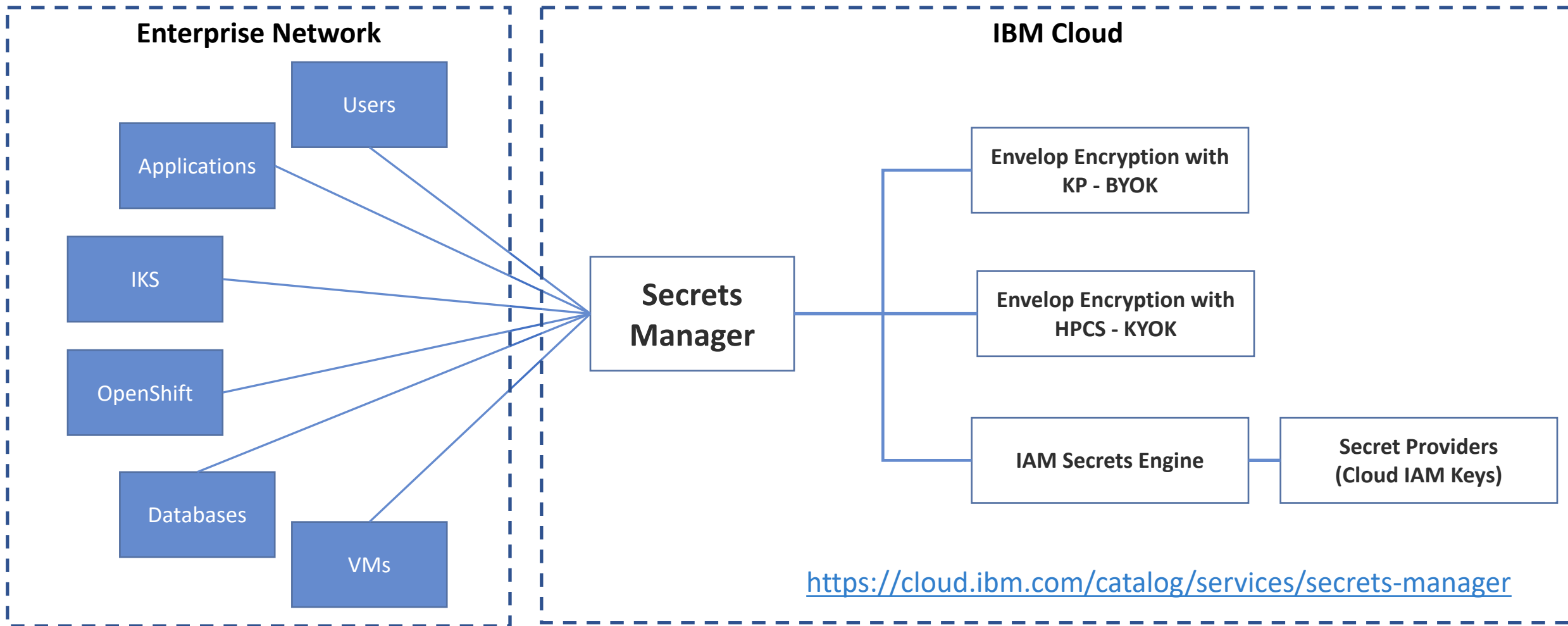
- Policy based “Secret” Rotation
- One-click Secret Disable anywhere in the enterprise in the event of a breach
- Auditing of security events – creation, use, deletion of secrets in the enterprise
- Will facilitate A2A (app-to-app) and A2D (app-to-database) communications and access
- Will help remove the need for hard-coded / default credentials
- Will help automate credential revocation OR create credentials that are only valid for a specific purpose / time frame

Secret Management

Tools & Services

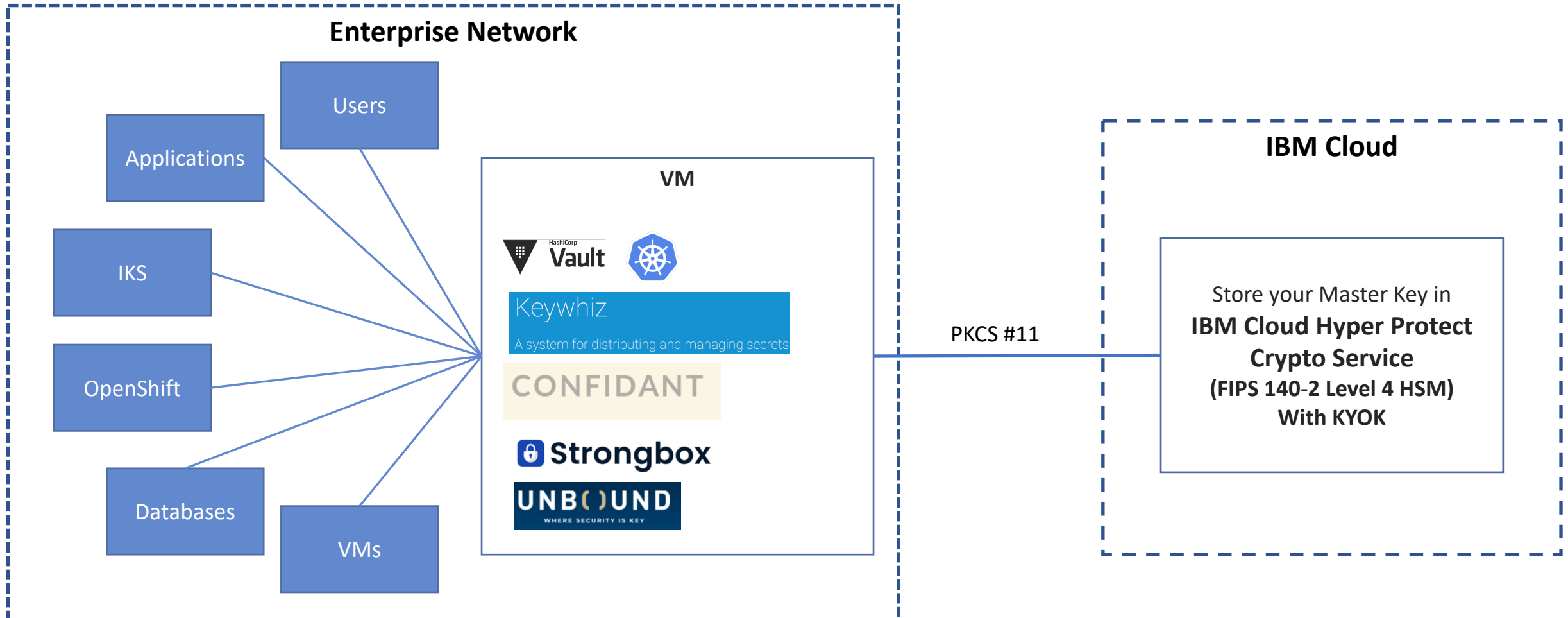
Secret Management: IBM Cloud Secrets Manager

- Create, lease, and centrally manage secrets that are used in IBM Cloud services or your custom-built applications.
- All your secrets will stay within the IBM Cloud Eco System
- Integrates with IAM – Identity and Access Management – allows creation of “secret groups”
- Enhances the security of secrets with IBM Key Protect (BYOK) or IBM Cloud Hyper Protect Services (KYOK)



Secret Management Tools / Applications

- Host **Secret Manager Tool** on a VM within the Enterprise Network Boundary
 - Secret Manager Tool will manage all the Secrets
 - Configure a Backend **HSM** (Hardware Security Model) for enhanced security



Secret Management: Source of Truth

Where does the buck stop?

- Vendor solutions can become the Single Point of Attack / Failure
- How do you inspire confidence?
- How will a KMS (Key Management System) Service help?

HSM – Hardware Security Module considerations?

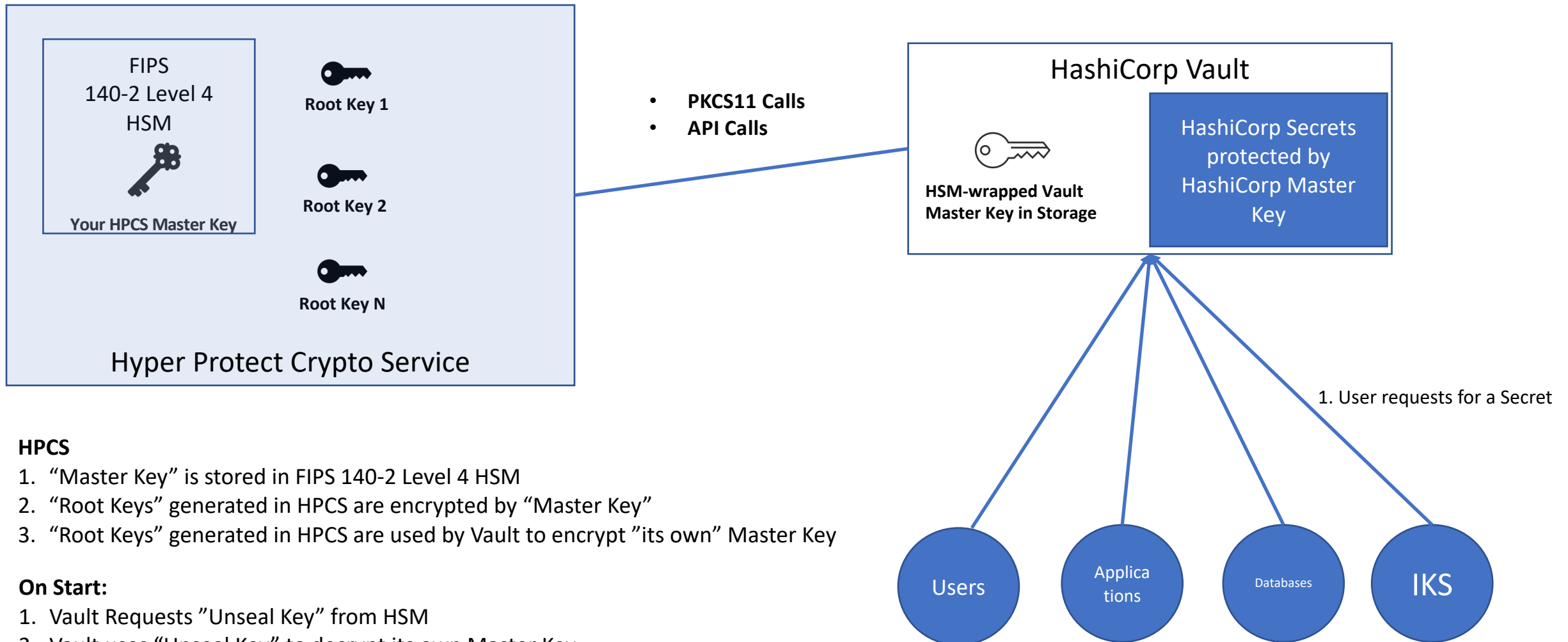
- Where will be **MY** master key?
 - Who will have access to **MY** master key?
 - What if **MY** master key is compromised?
- HSM
 - On-Prem – how do you keep up with new developments
 - Cloud-Based HSM – Pay as you go
- How secure is the HSM?
 - FIPS 140-2 Level 3
 - FIPS 140-2 Level 4 (Hyper Protect Crypto Service)



Secret Management

Use Cases

Secret Management with HSM Backend



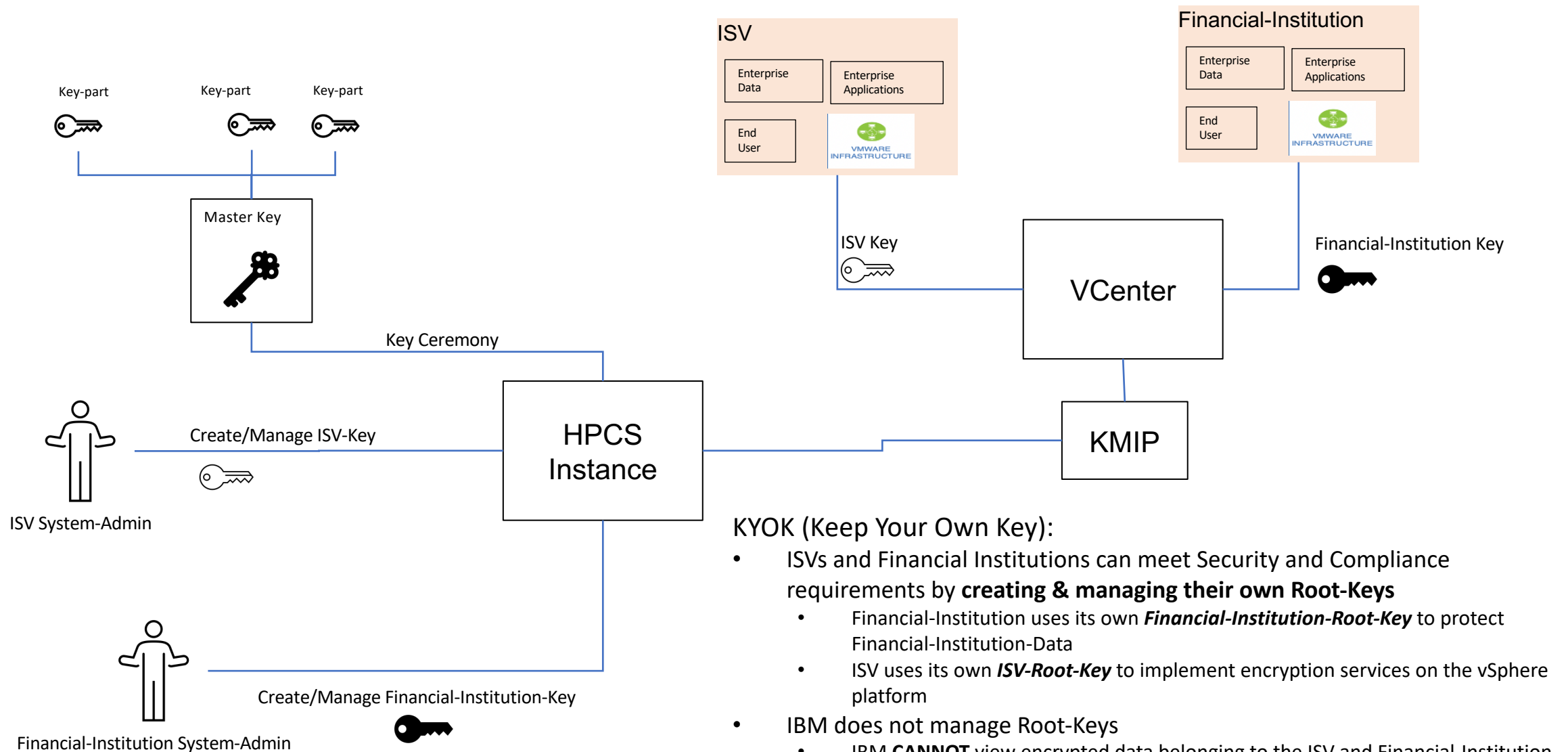
HPCS

1. "Master Key" is stored in FIPS 140-2 Level 4 HSM
2. "Root Keys" generated in HPCS are encrypted by "Master Key"
3. "Root Keys" generated in HPCS are used by Vault to encrypt "its own" Master Key

On Start:

1. Vault Requests "Unseal Key" from HSM
2. Vault uses "Unseal Key" to decrypt its own Master Key
3. Vault uses "its own decrypted Master Key" to decrypt its "Data Encryption Key"

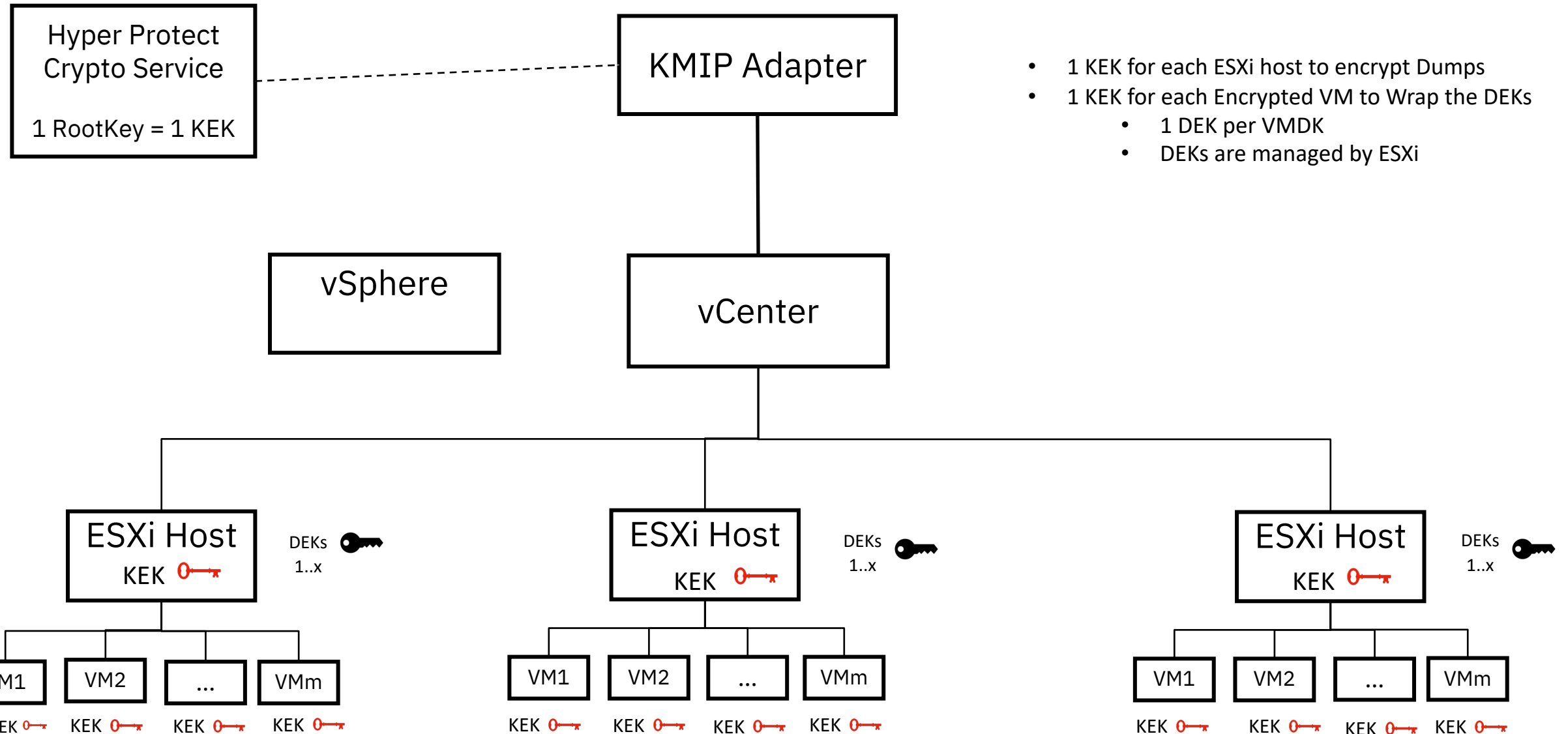
Secrets in a VMware Regulated Workload Environment



KYOK (Keep Your Own Key):

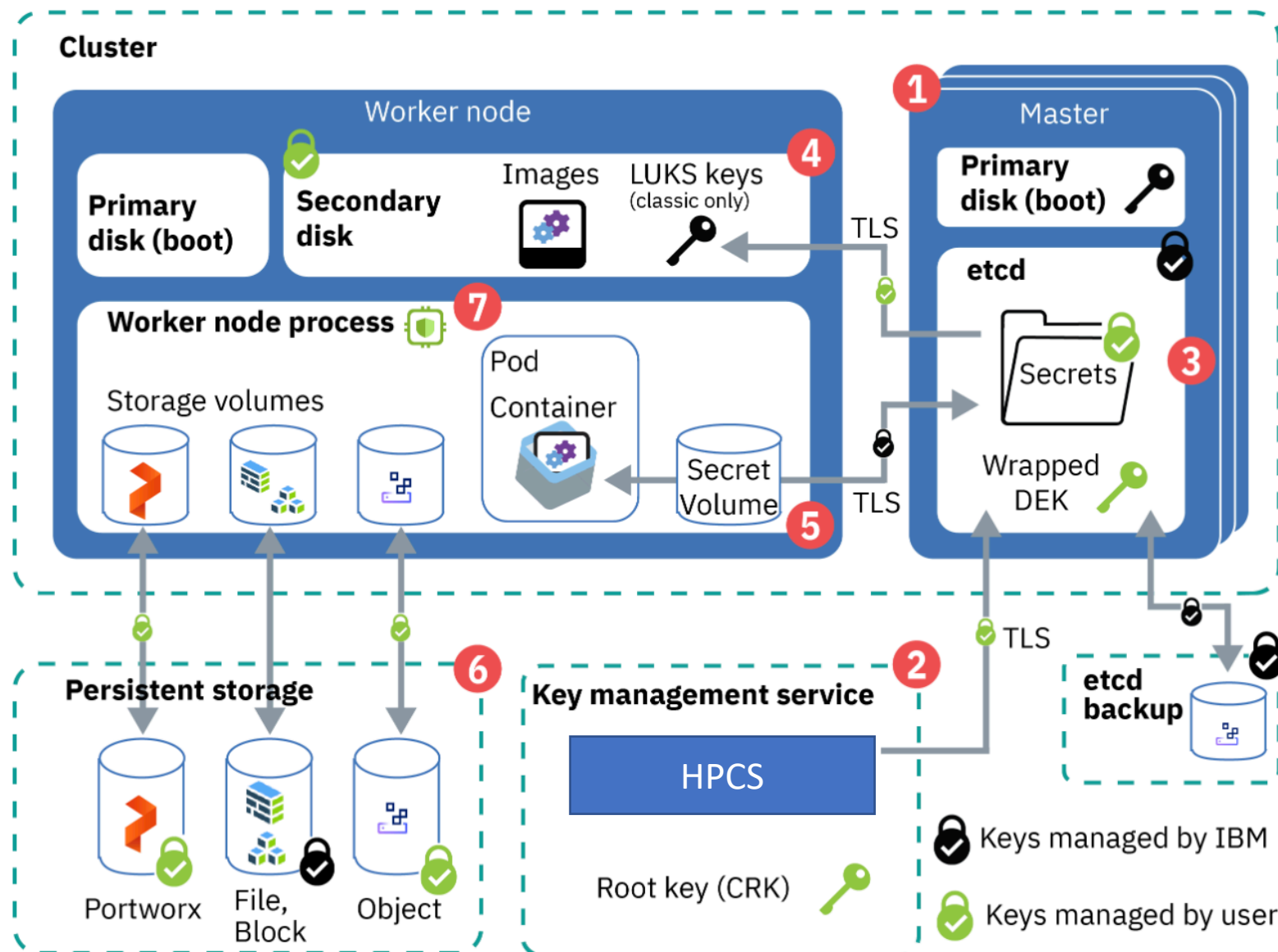
- ISVs and Financial Institutions can meet Security and Compliance requirements by **creating & managing their own Root-Keys**
 - Financial-Institution uses its own **Financial-Institution-Root-Key** to protect Financial-Institution-Data
 - ISV uses its own **ISV-Root-Key** to implement encryption services on the vSphere platform
- IBM does not manage Root-Keys
 - IBM **CANNOT** view encrypted data belonging to the ISV and Financial-Institution (Technical Assurance)
 - Similarly, ISVs cannot view encrypted data belonging to the Financial institution and vice-versa

Secrets (Keys) in a VMware environment

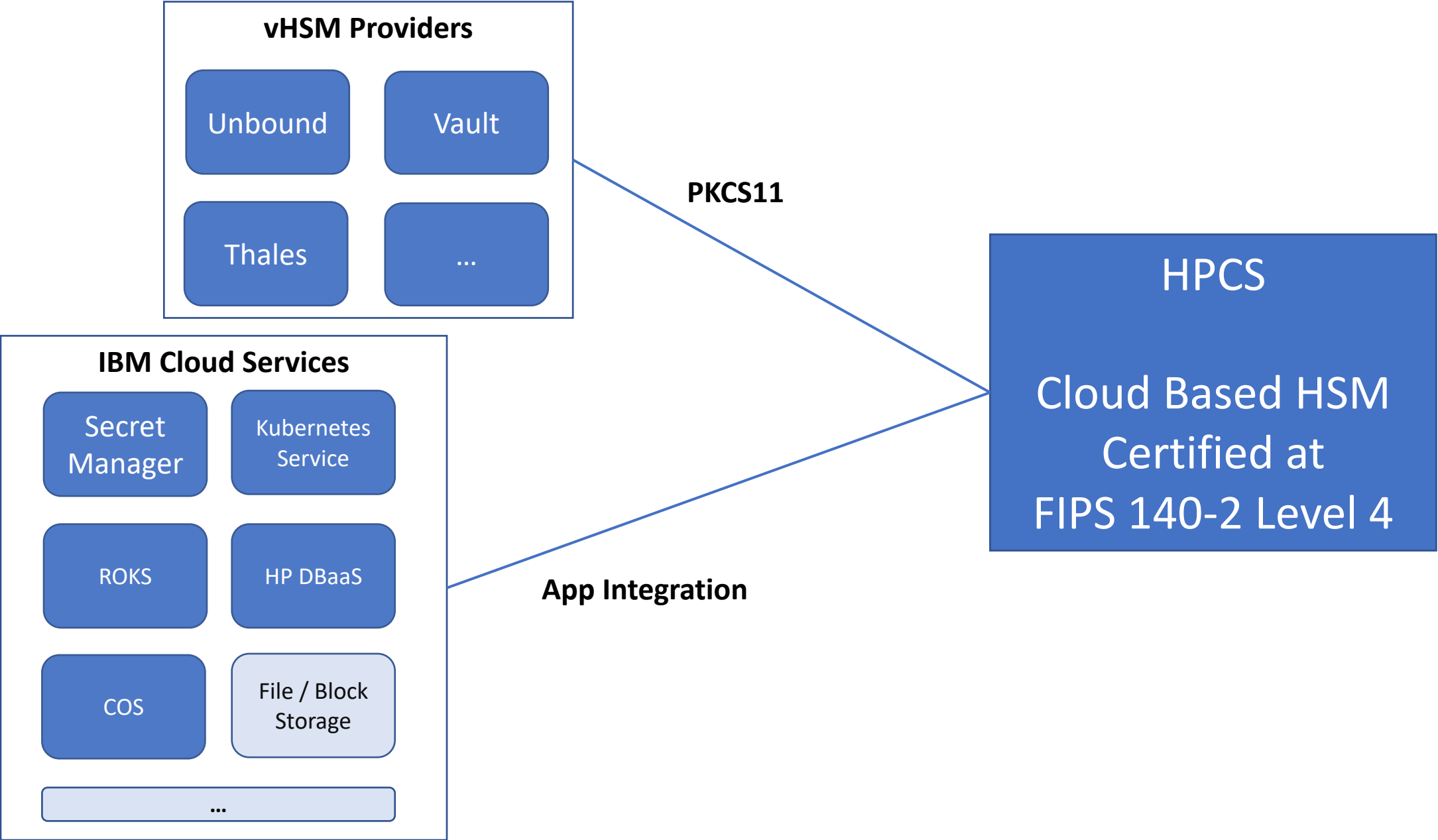


Secrets (Keys) in a Kubernetes environment

1. Master Control Plane come up on LUKS-encrypted drive by using IBM-managed Key
2. HPCS (KMS Provider) holds ALL the Root-Keys required for the K8S Environment
3. **etcd data** stores configuration data for your K8S resources. A wrapped DEK is used to encrypt **secrets** in the K8S cluster that store service-credentials and the LUKS key. Root-Key in HPCS is required to decrypt DEK.
4. **Worker node disks** encrypted by a LUKS key are stored as a Secret in **etcd**
5. Cluster Secrets are encrypted by HPCS Root-Key wrapped DEK
6. Persistent Storage Encryption
7. Data-in-use Encryption



Use a Level-4 HSM to enhance security posture



Hyper Protect Crypto Service – Key Management

- Initialize YOUR FIPS 140-2 Level 4 HSM with **YOUR OWN** Master Key
 - Master Key is stored in the HSM
 - Master Key can have up to 3 parts
- Create Root-Keys and Standard Keys on the Portal
 - Create other key types using PKCS11
 - Keys are symmetric 256-bit, supported by AES-CBC algorithm
- Import your own Keys
- Access keys using
 - Key-Protect API
 - Programmatically using PKCS11
- Rotate Keys on a schedule
 - Set individual policies for each key
- Disable / Delete / Zeroize Master Key to immediately prevent access to ALL resources in case of an emergency
- 5000 Keys per Crypto Unit
 - 3 Crypto Units per HPCS instance
 - 1Million API Calls / month

Crypto units

Location [eu-de].[AZ3-CS3]. [00].[08]	HSM ID 707b9f1c-ecbd-4403-b9f9-50a0e1441
State ✓ INITIALIZED	Verification pattern bf011d9e5de538fe558a37824ca65f14 f1923558c723e8f7f66582a733e2ac1a

Location [eu-de].[AZ1-CS1]. [03].[07]	HSM ID e206c4f3-4c94-49c7-a086-de1e82e95
State ✓ INITIALIZED	Verification pattern bf011d9e5de538fe558a37824ca65f14 f1923558c723e8f7f66582a733e2ac1a

Locate



Region eu-de City Frankfurt

Connect

Key management endpoint URL	EP11 endpoint URL
Public https://api.eu-de.hs-crypto.cloud.ibm.com:9326	

Instance

Instance ID
ec3faac8-dbb8-4a91-80e4-802e69256ccf

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

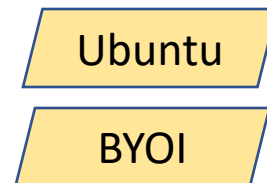
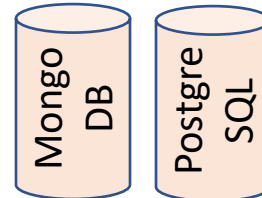
Hyper Protect Family of Services

Hyper Protect Crypto Services
HPCS

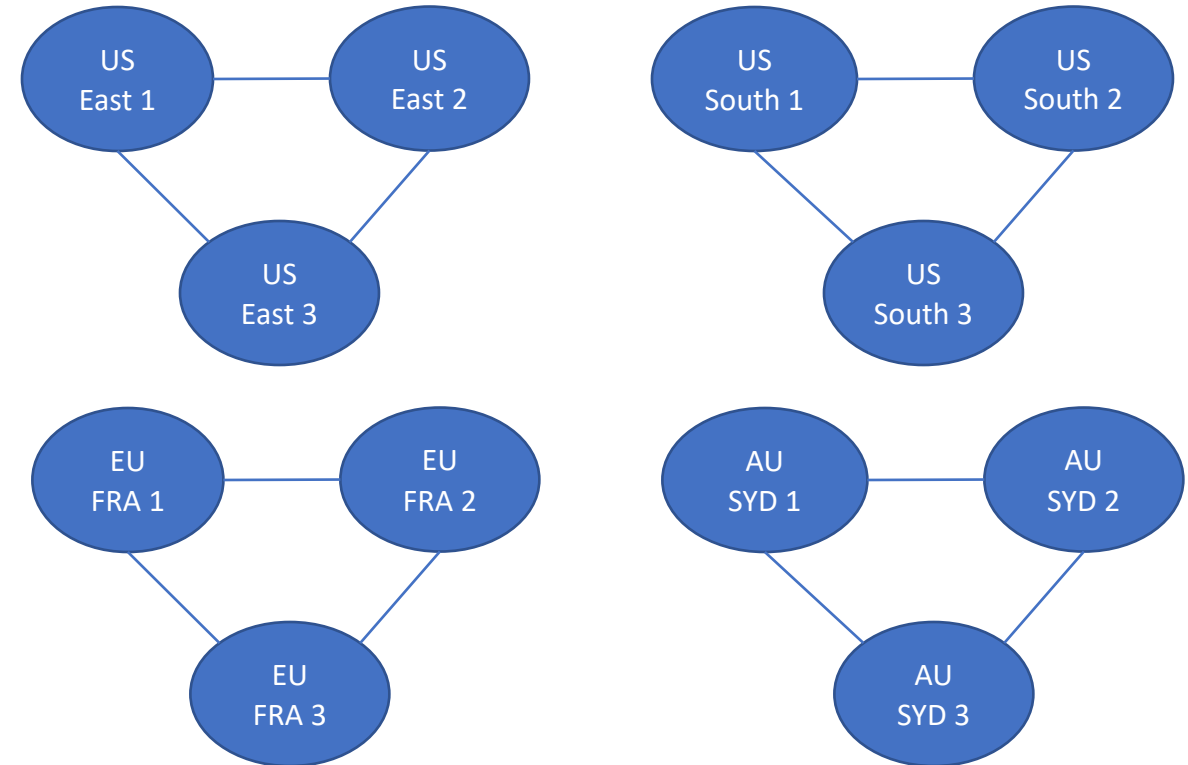
Hyper Protect DB as a Service
HPDBaaS

Hyper Protect Virtual Services
HPVS

Hyper Protect Kubernetes Service



Multi-Zone Regions (MZR)



SOC2
Type1

ISO
27000

IRAP

HIPAA
Ready

Thank you!

Sandeep Batta

Developer Advocate, IBM

sbatta@us.ibm.com

<https://www.linkedin.com/in/sandeep-batta/>

Useful Links

Hyper Protect Videos, Demos, Code-Patterns, Blogs ibm-hyper-protect.github.io

Try a Code-Pattern <https://developer.ibm.com/patterns/create-a-secured-microservices-and-deploy-it-to-a-consolidated-database/>

IBM Cloud Hyper Protect Services <https://www.ibm.com/cloud/hyper-protect-services>

How to BYOI? https://cloud.ibm.com/docs/hp-virtual-servers?topic=hp-virtual-servers-byoi#byoi_create

IBM Cloud architectures <https://www.ibm.com/cloud/architecture/architectures/>

Please submit your session feedback!

- Do it online at <http://conferences.gse.org.uk/2020/feedback/4AZ>
- This session is 4AZ



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 presentation correct?

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

1 2 3 4 5 6 7 8 9

3. Did this presentation 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

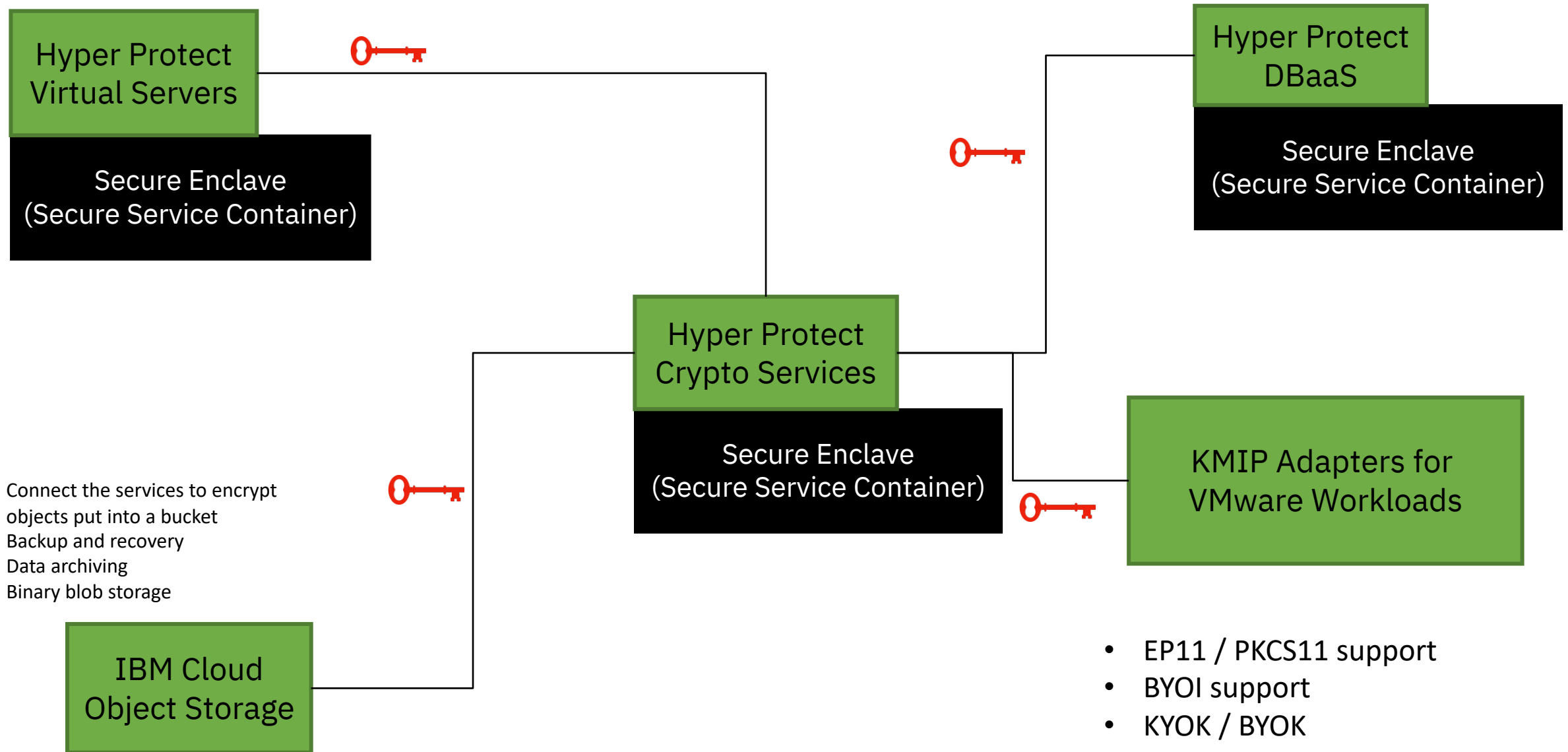
GSE UK Conference 2020 Charity

- 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>

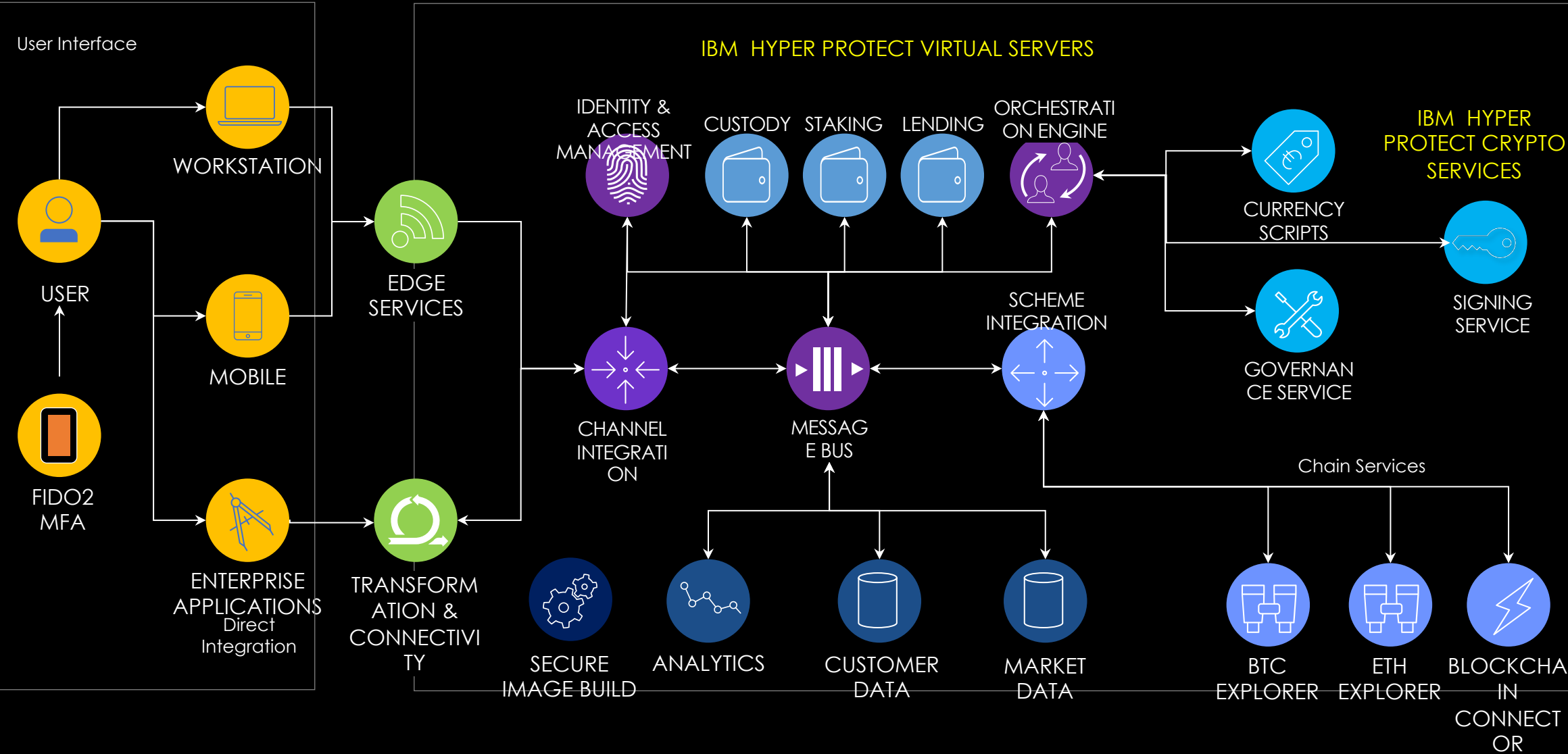


IBM Cloud Hyper Protect Crypto Services Integration



- EP11 / PKCS11 support
- BYOI support
- KYOK / BYOK
- Use tamper-resistant hardware

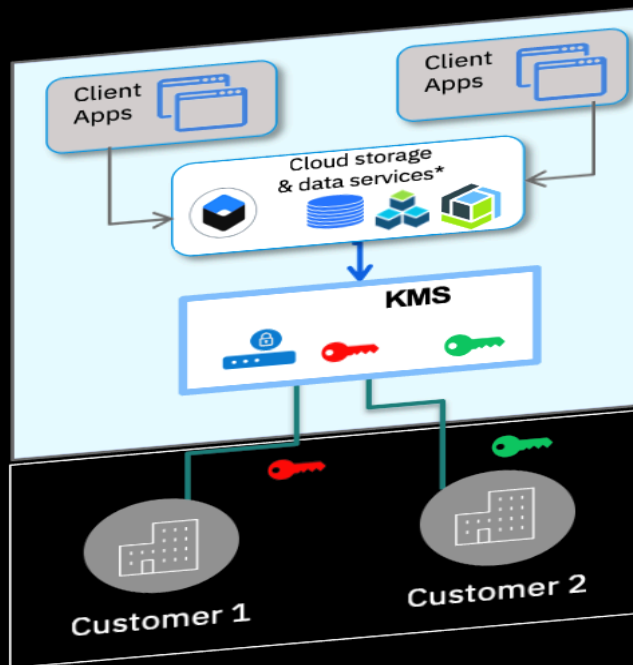
IBM Cloud Hyper Protect Services + Digital Assets Platform (Custody)



IBM Cloud Hyper Protect Crypto Services (HPCS): KYOK vs. BYOK

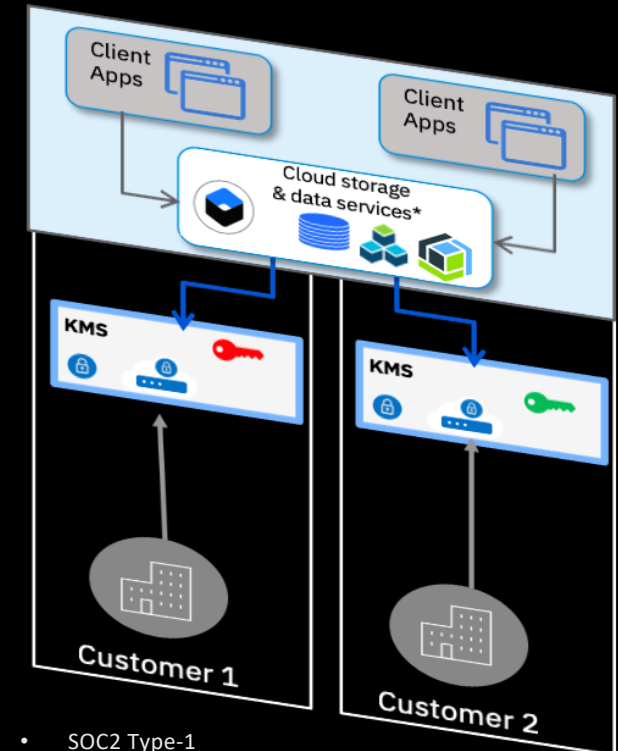
- Keep Your Own Key (KYOK) provides **technical assurance** that a Cloud Services Provider **cannot** access the encryption keys, with industry's highest level security

Industry's Bring Your Own Keys (BYOK)



Industry BYOK	Cloud key management capabilities	IBM's KYOK
✓	Customer key lifecycle management	✓
✓	As a service. Integrated with Cloud services	✓
✓	Client can bring their keys from <u>onprem</u> HSM	✓
✓	Operational assurance - provider will not access keys	✓
	Technical assurance - IBM can not access the keys	✓
	Single tenant, dedicated KMS	✓
	Client has exclusive control of HSM's master key	✓
	Highest level security – FIPS 140-2 Level 4 HSM	✓
	Client manages master key, with smart card	✓
	Client can perform key exchange ceremony	✓

IBM's Keep Your Own Keys (KYOK)



- SOC2 Type-1
- GDPR
- ISO 27K
- IRAP Protected
- HIPAA Ready