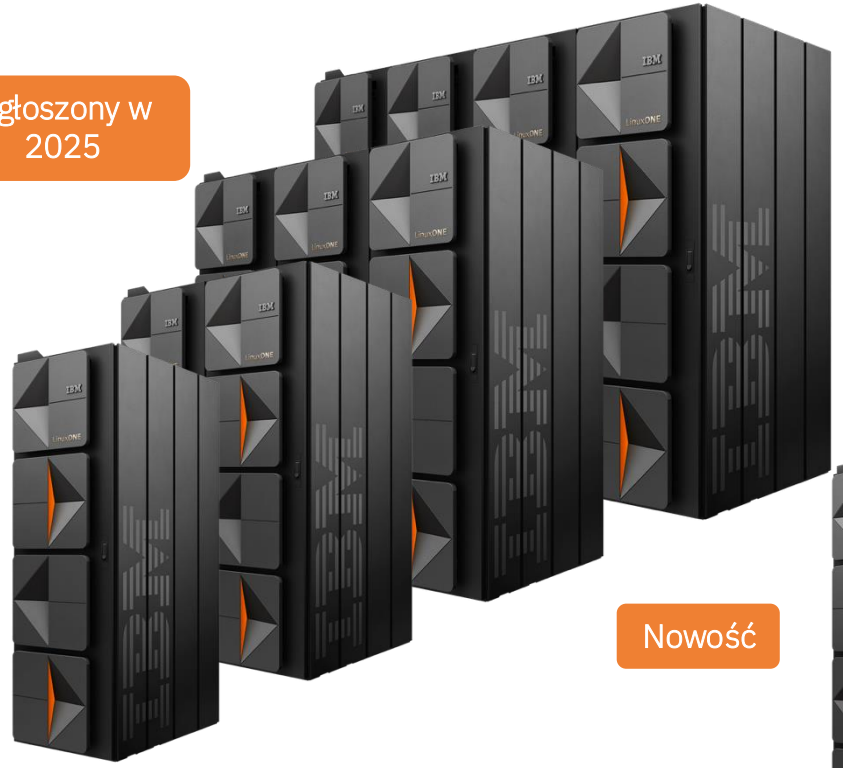
IBM One Vault

IBM Vault + Unified Key Orchestrator: klucze i sekrety pod pełną kontrolą w oparciu o najbezpieczniejszą platformę sprzętową

Common 2026 | Bartosz Dobrowolski | 20.10.2026

Portfolio IBM® LinuxONE 5

Ogłoszony w 2025



IBM LinuxONE Emperor 5

- Up to 208 cores
- Designed to support the growth in IT requirements for multi frame clients, with superior scalability & efficiency

Nowość



IBM LinuxONE Rockhopper 5 – Single Frame

- Up to 82 cores, ~20% increase
- Up to 18TB memory, ~12% increase

Nowość



IBM LinuxONE Rockhopper 5 – Rack Mount (Including Express at GA!)

- Components designed for colocation with other technologies. IBM-installed with expansion capability
- Enterprise grade Linux solution starting at $165,000

More performance and Capacity. Less Infrastructure. Secure and AI Ready.



HIGH PERFORMANCE

- **Commercial processor** at 4.8 GHz, up to 18TB memory
- **On-chip AI inferencing** — real-time fraud detection
- Requires up to 4x fewer cores versus running it on a compared x86 platform[2]

FLEXIBLE SCALABILITY

- Scale securely with enterprise-class resilience
- Consolidate distributed Linux environments at scale
- **Confidential Computing**, Enable Secure Data Rooms and customer-controlled encryption (KYOK/BYOK)

High Availability | Data Center Footprint savings | Lower power consumption

Workloads that thrive on LinuxONE

CLOUD FOUNDATION

- Virtualization Platform
- Container Platform

DATA SERVING

- Database Platform · Data Warehouse
- Event Streaming (Kafka · Confluent)
- Data Integration · Financial ISVs · EAM

SECURE COMPUTING

- Digital Assets
- Confidential Platform
- Enterprise Key Management

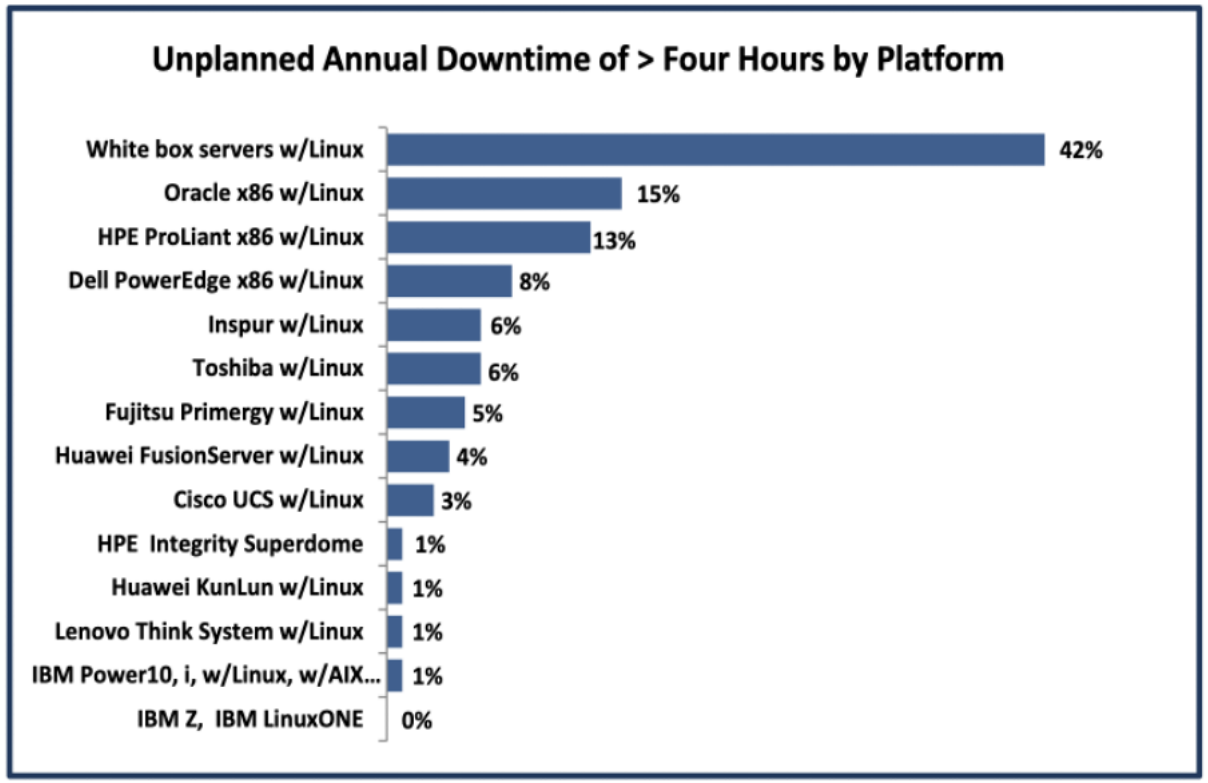
ACCELERATED COMPUTING

- Secured AI
- Scalable & Power-efficient AI

Post-Quantum Cryptography | FIPS 140-2 LEVEL 4 | EAL5+ CERTIFIED

© 2026 IBM Corporation / IBM LinuxONE Announcement overview

IBM LinuxOne delivers the highest availability



99.999999%
99.998801%
99.997100%
99.996849%
99.986529%
99.977168%
99.945205%
99.926940%
99.910958%

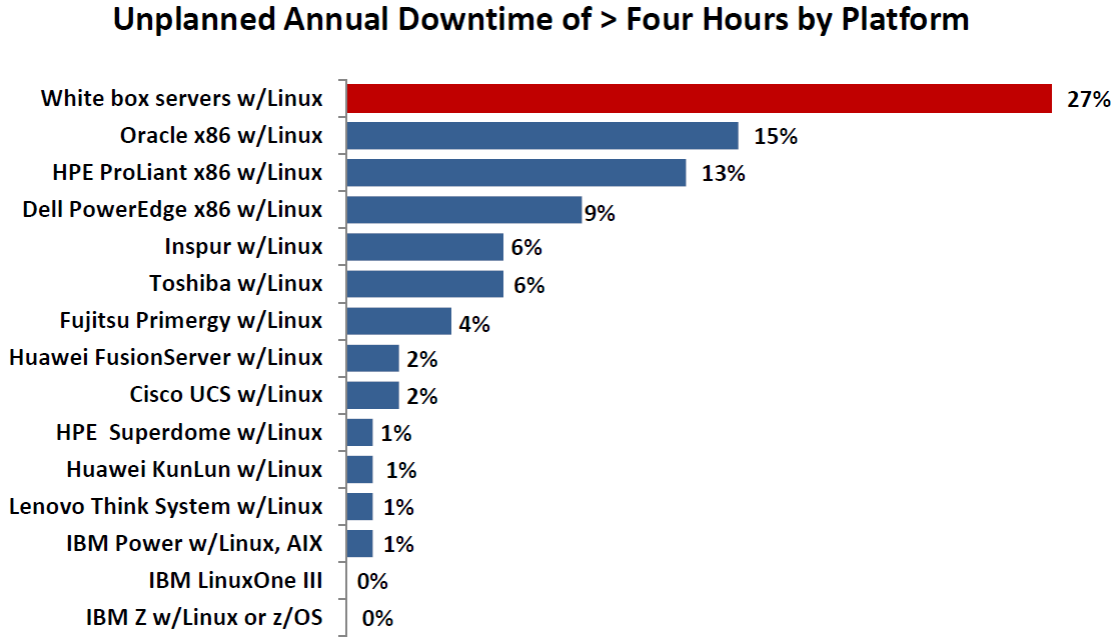
IBM LinuxOne exhibits true fault tolerance

The only platform with Eight 9's of availability (1). Far better than traditional x86 servers, and better than converged systems

For IBM Mainframe, the mean time between failures is measured in *decades*, not months

LinuxONE resilience

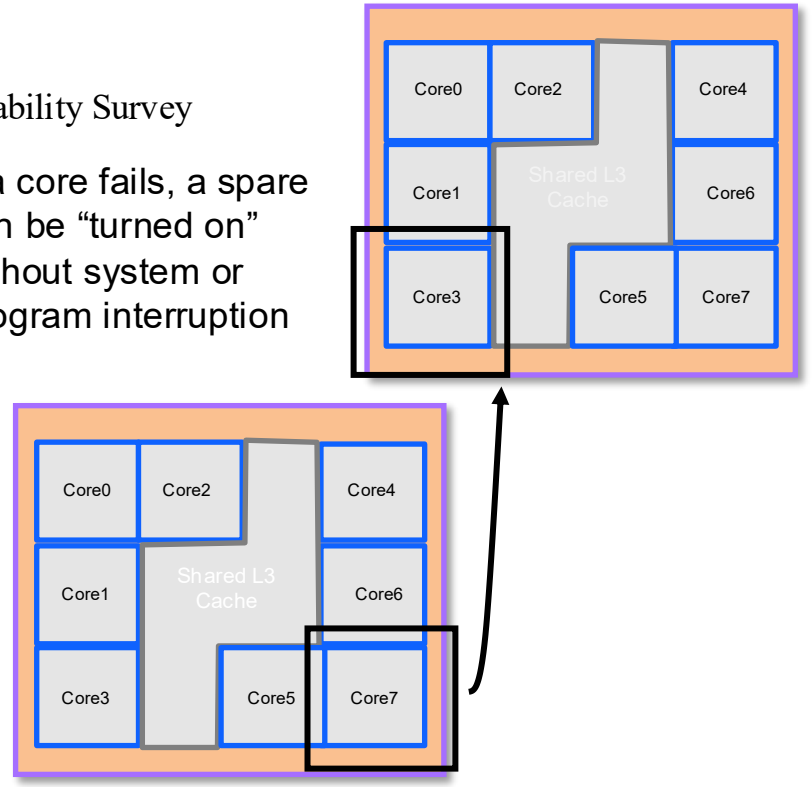
Most recent ITIC survey shows IBM Z/LinuxONE had **0%** unplanned system downtime due to inherent flaws in hardware



Source: ITIC 2021 Global Server Hardware, Server OS Reliability Survey

Capability	LinuxONE	x86
ECC on Memory Control Circuitry	Transparent While Running	Can recognize/repair soft errors while running; limited ability with hard errors
Oscillator Failure	Transparent While Running	Must bring server down to replace
Core Failure	Transparent While Running	Must bring server down to replace
Microcode Driver Updates	While Running	Some OS-level drivers can update while running, not firmware drivers; reboot often required
Drawer Additions, Replacement	While Running	Must bring server down
Memory Replacement	While Running	Must bring server down
Memory Bus Adaptor Replacement	While Running	Must bring server down
I/O Upgrades	While Running	Must bring server down to replace (limited ability to replace I/O in some servers)
Concurrent Driver Maintenance	While Running	Limited – some drivers replaceable while running
Redundant Service Element	2 per System	"Support processors" can act as poor man's SE, but no redundancy

If a core fails, a spare can be "turned on" without system or program interruption



Inne przypadki użycia
LinuxOne

Port of Barcelona transforms operations

IBM LinuxONE and RedHat OpenShift improved

- Performance
- Customer service
- Disaster recovery
- Sustainability posture
- Security



Port de Barcelona

- 71M tons of goods
- 3.5M containers
- 3.9M passengers

Medical image on IBM LinuxONE analysis with contextual insights

Business Scenario

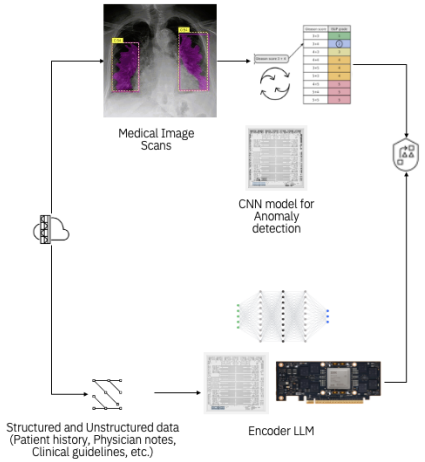
Healthcare professionals face increasing workloads due to the high volume of medical imaging scans (X-rays, MRIs, CT scans). Traditional AI models can detect anomalies, but they lack interpretability and context awareness. Moreover, generating structured reports from imaging findings remains time-consuming. Current x86/GPU servers also encounter scalability and provisioning issues. Data privacy and security are huge concerns as they handle extremely sensitive PII information

Business Impact:

- **Automate anomaly detection**
- **Reduce false positives and false negatives by adding patient history context to image analysis**
- **75% faster AI inferencing compared to x86/GPUs servers**
- **Workload consolidation and reduced datacenter footprint**

Achieved by deploying an encoder LLM model and a CNN AI model to deliver structured context aware reports on IBM LinuxONE complying with data privacy and PII compliance regulations

Example Solution



Integrated with client application:

Combined multi-model AI approach helps compare findings from multiple sources to flag inconsistencies and highlight high-risk cases for further medical review while adhering to sensitive data privacy and PII information regulation

Products

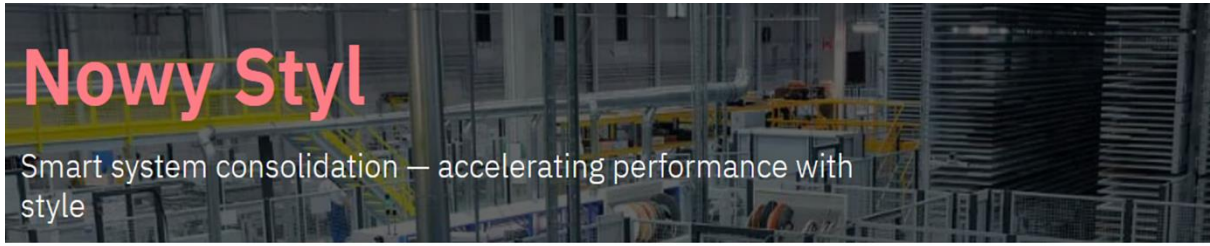
Machine Learning for IBM LinuxONE, IBM Operational Decision Manager

Components

OpenShift, Trustworthy AI - Explainability

Models

CNN, Vision Transformer BioBERT, Clinical BERT, T5



Nowy Styl

Smart system consolidation — accelerating performance with style

By deploying Oracle Database on LinuxONE, Nowy Styl increased system speed and security:

Increases key system processing speeds by ~450%

A shop material planning report that took 187 minutes to process is now completed in only 60 minutes — a 68% shorter time

A key process replication report that used to take 62 minutes to prepare is now completed in 16 minutes — a 74% shorter time

A key production scheduling planning report that used to require 111 minutes to prepare is now available in 24 minutes — a 78% shorter time

Provides more layers of security

through more powerful data encryption capabilities

Enables more growth for the future

without increasing the overall cost of software licenses or increasing footprint

Comprehensive security built into every layer



Security Services

- Expert Labs
- IBM Consulting®
- Crypto Competency Center

Enterprise Key Management

- Unified Key Orchestrator (UKO) for Containers

Enterprise Secrets Management

- IBM Vault

Digital Assets

- IBM Digital Assets Haven (i.e., Metaco Harmonize, Fireblocks)
- **Offline Signing Orchestrator

Quantum Risk Assessment

- IBM Quantum Safe Explorer

Confidential Computing

- IBM Confidential Computing Products

Distribution

- Redhat
- SUSE
- Canonical

Hypervisor

- z/VM®
- KVM

IBM LinuxONE

- FIPS Level 140-2 Hardware Security Modules
- Quantum Safe Secure Boot & Crypto APIs
- Dual HW Accelerated Cryptography
- **Secure Execution and Confidential Computing
- Hardware Protected Keys
- Common Criteria Isolation (LPAR)

** Requires KVM only z/VM not supported

© 2026 IBM Corporation / IBM LinuxONE Announcement overview

Dwa światy: klucze kryptograficzne vs sekrety

Klucze kryptograficzne (UKO)

- Klucze szyfrujące dane, master keys, klucze w HSM
- Rotacja według polityki
- Synchronizacja kluczy w różnych Key Stores
- Źródło entropi
- HSM as a Service

Sekrety i tożsamość (Vault)

- Hasła, tokeny API, certyfikaty, poświadczenia do baz
- Krótki cykl życia, dynamiczne poświadczenia
- Minimalne uprawnienia dla użytkowników



Encryption keys attacker-accessible: ~40% of those cases

(Keys stored in the same cloud/provider as the data)

Source: Thales Data Threat Report 2025

- **Primary cause of cryptographic failure:**
  - Poor key management
  - Excessive key access
  - No separation of duties

Source: Thales & ENISA reports



https://cpl.thalesgroup.com/sites/default/files/content/campaigns/data-threat-report/2026-thales-data-threat-report.pdf

© 2026 IBM Corporation

Encryption can help protect data but the safest door in the world becomes useless if the keys are lost, stolen, or otherwise compromised.



© 2026 IBM Corporation

Encryption is easy but key management is difficult

Ponemon Institute: 2022 Global Encryption Trends Study

"The top 3 reasons that make key management painful:

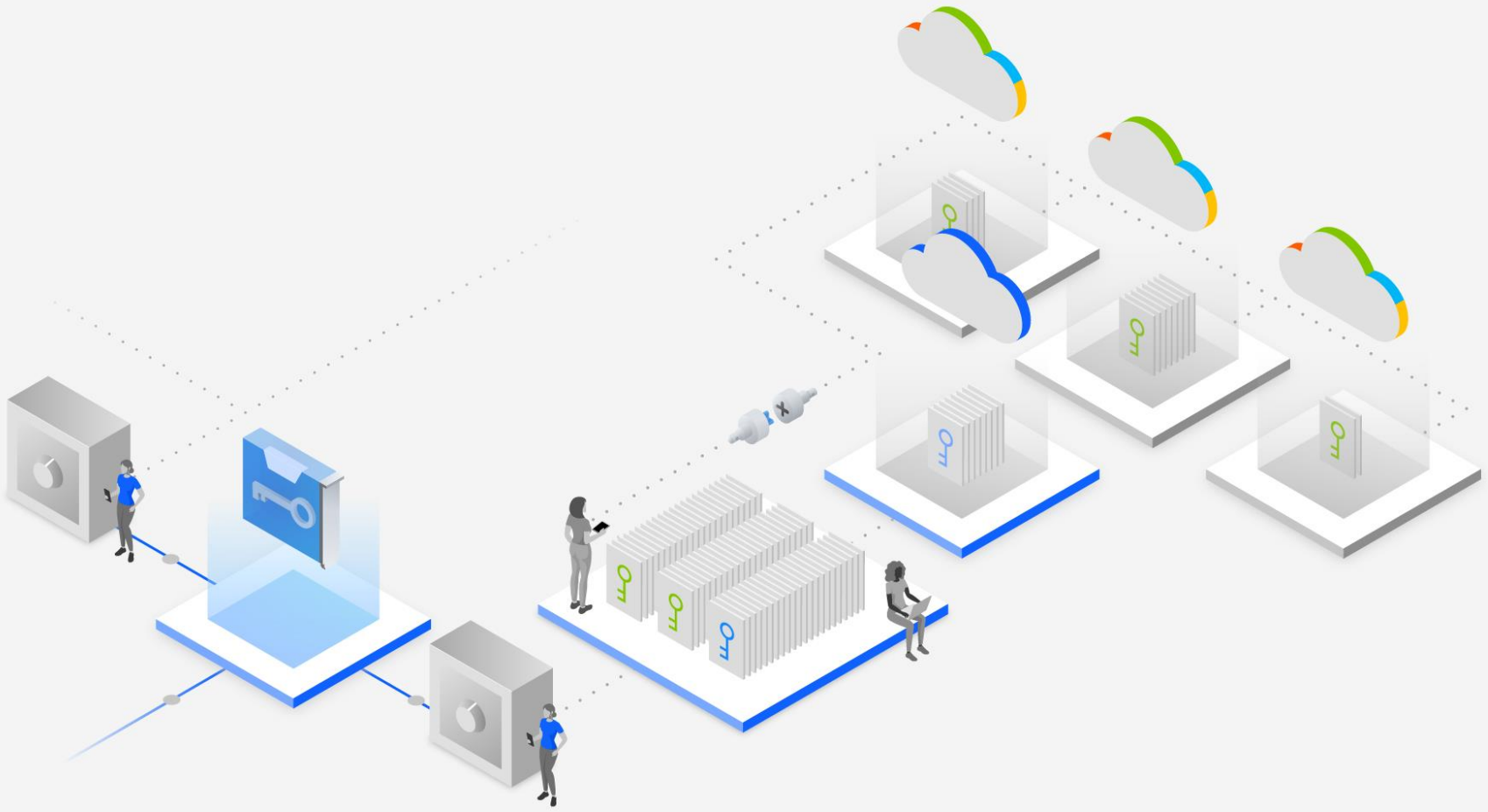
1. No clear ownership
2. Lack of skilled personnel
3. Key management tools are inadequate"

Ponemon Institute: 2022 Global Encryption Trends Study

© 2026 IBM Corporation

UKO for Containers streamlines Key Management on IBM Z and Hybrid Multicloud

Unified Key Orchestrator for Containers provides centralized key management across on-premises and cloud environments while addressing compliance and security needs.



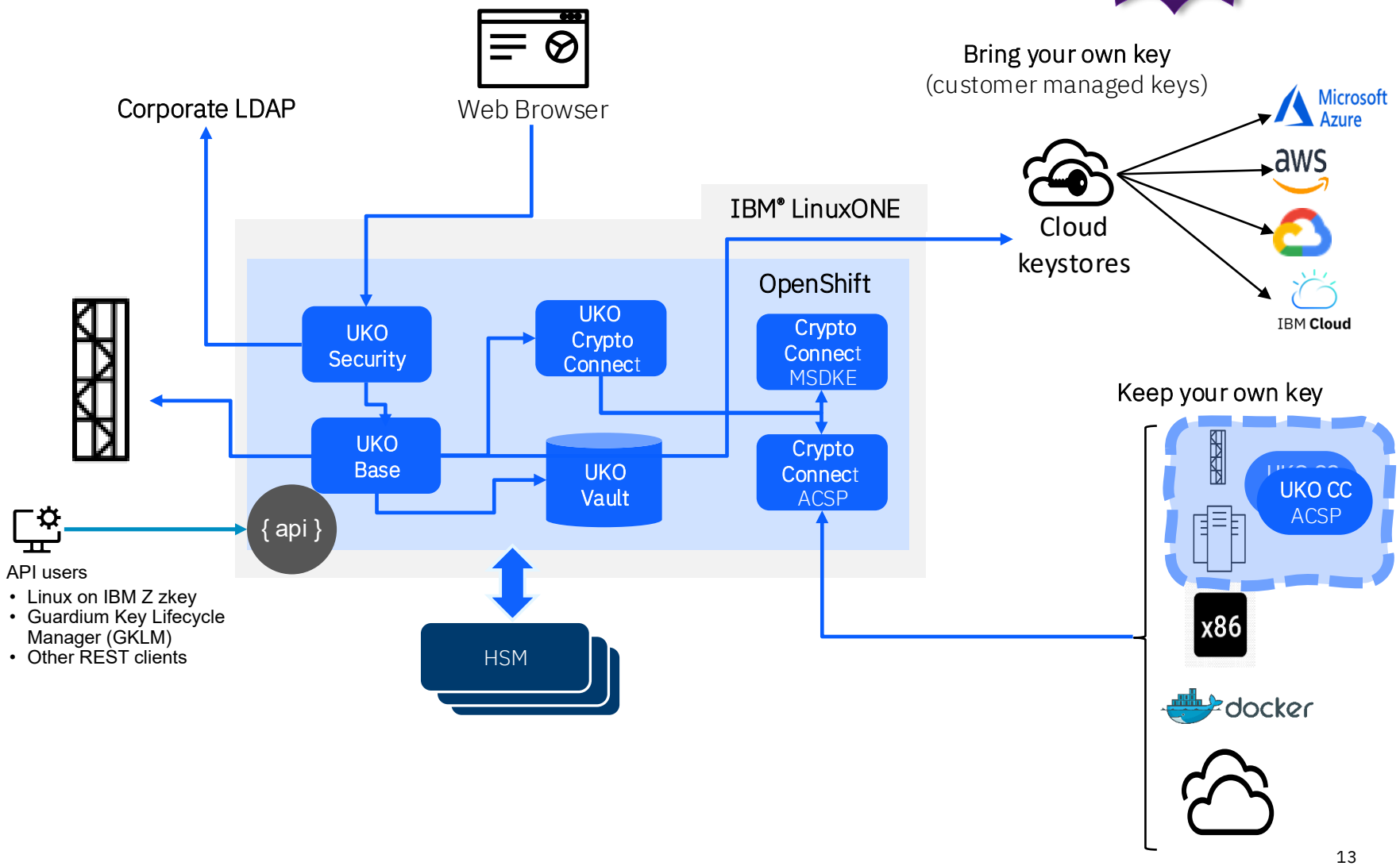
© 2026 IBM Corporation

UKO for Containers on IBM® LinuxONE and Linux on Z

Enterprise Crypto Consolidation with UKO

GA Dec 5th. v3.1.0.9

- Awarded UX supporting one-click distribution of keys into multiple endpoints or regions
- Restful API, Integration and Automation for Cloud and on-premise systems
- Audit & Key monitoring with one-click recovery
- Crypto consolidation with CC ASCP, access to cryptographic hardware over the network for cost effective use of HSMs and reduced administration effort
- Scalable and Resilient Crypto services to meet crypto SLAs, also during peaks



© 2026 IBM Corporation

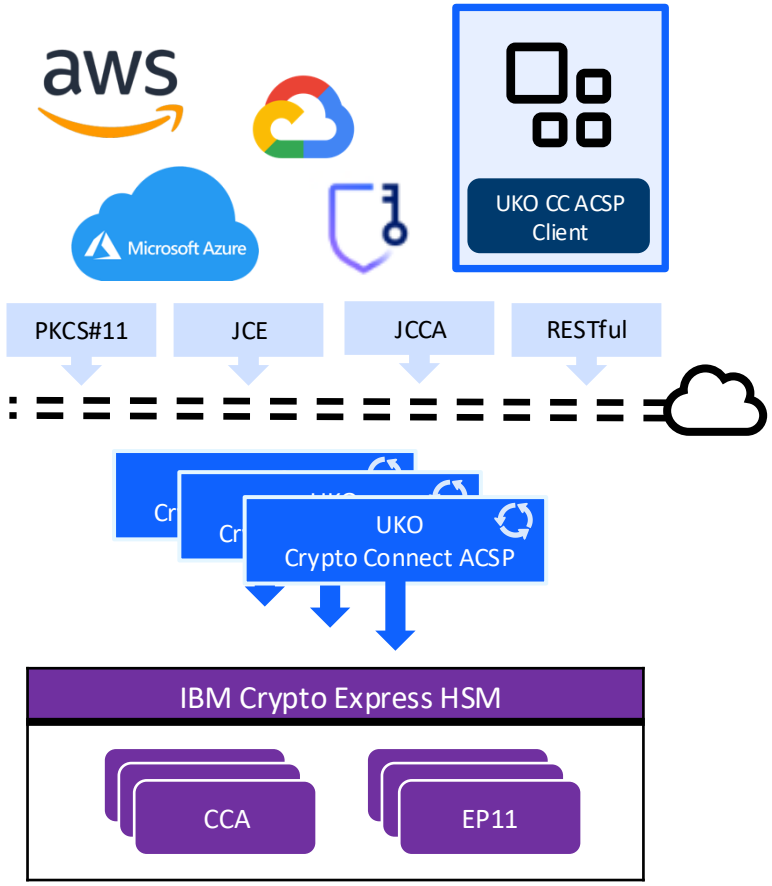
UKO Crypto Connect ACSP – Crypto as a Service

UKO CC ACSP, an evolution on the heritage and development of Advanced Crypto Service Provider (ACSP) services asset, is a remote crypto services solution enabling applications in distributed environments with access to cryptographic hardware over the network. CC ACSP provides flexible and consolidated HSM capabilities for the distributed and hybrid environments.

UKO CC ACSP provides by CC ACSP Client flexible API's and a choice of platform and operating system deployment options.

The CC ACSP Client will allow for load balancing a cluster of available CC ACSP servers. If a server fails or is taken out of service any cryptographic workload is automatically directed and distributed evenly to any remaining available servers. When outage has been resolved!
The client will automatically redistribute and balance to all servers again providing a scalable high availability crypto environment.

CC ACSP provide options to define User Defined Function (UDF), a custom code which implements business specific functions and extends standard CCA/ICSF APIs running in CC ACSP Server and provide the base to implement Crypto Agility

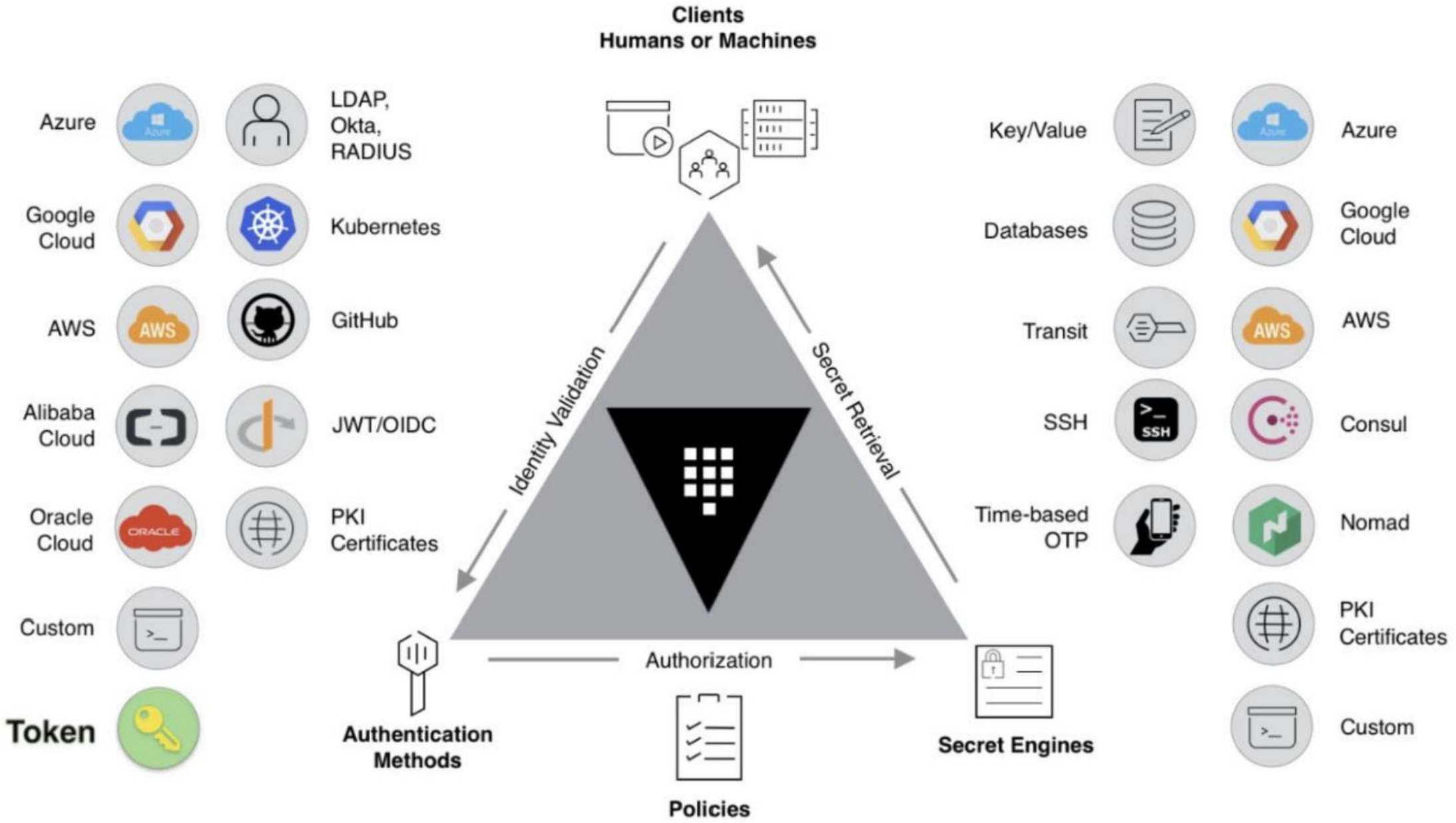


© 2026 IBM Corporation



HashiCorp
Vault

Vault components overview



Better Together

HashiCorp Vault Seal wrap with UKO Crypto Connect ACSP

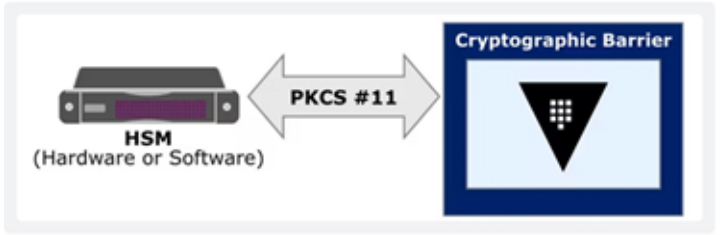
HashiCorp
an IBM Company

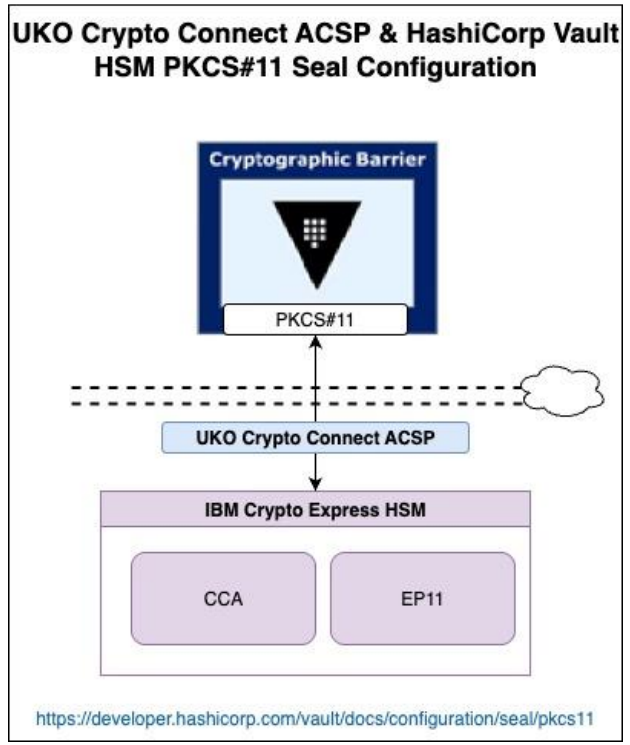
Seal wrap is a mechanism to wrap secret values with an extra layer of encryption. Examples of where seal wrapping is used:

- The LDAP, RADIUS, Okta, and AWS auth methods, for storing their configuration.
- PKI for storing the issuers and their keys,
- SSH for storing the CA's keys,
- KMIP for storing externally-provided keys and its CA keys.
- Transit engine for storing keys and their policy.

Vault's Seal Wrap feature has been evaluated by Leidos for compliance with FIPS 140-2 requirements. When used with a FIPS 140-2-compliant HSM, Vault will store Critical Security Parameters (CSPs) in a manner that is compliant with KeyStorage and KeyTransit requirements.

Requires a Vault Enterprise Plus license





© 2026 IBM Corporation

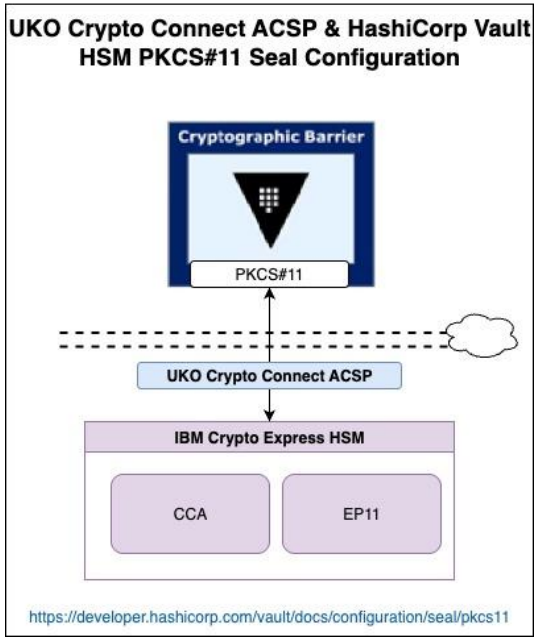
UKO Crypto Connect ACSP & HashiCorp Vault

with CCA or EP11 IBM Crypto Express HSM

HashiCorp
an IBM Company

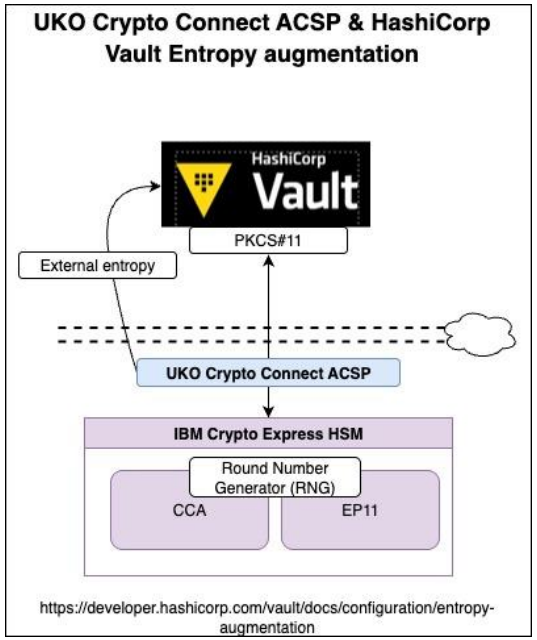
PKCS#11 Seal with UKO Crypto Connect ACSP

Vault HSM PKCS#11 Seal Configuration (HashiCorp Vault Enterprise license) configured with UKO CC ACSP PKCS#11 library providing standard PKCS#11 using IBM Crypto Express HSM through UKO CC ACSP



Vault Entropy augmentation with UKO Crypto Connect ACSP

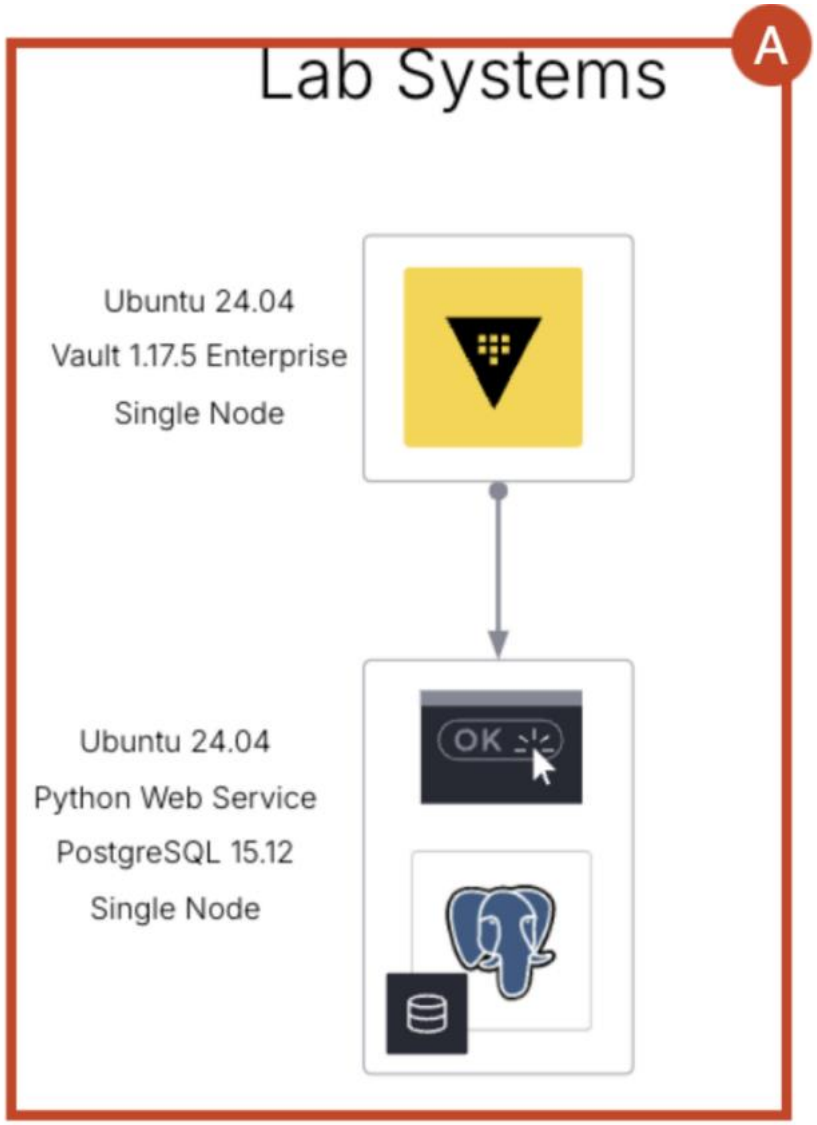
Vault Entropy Augmentation (HashiCorp Vault Enterprise license) from external cryptographic module configured with UKO CC ACSP PKCS#11 library provides standard PKCS#11 using IBM Crypto Express HSM

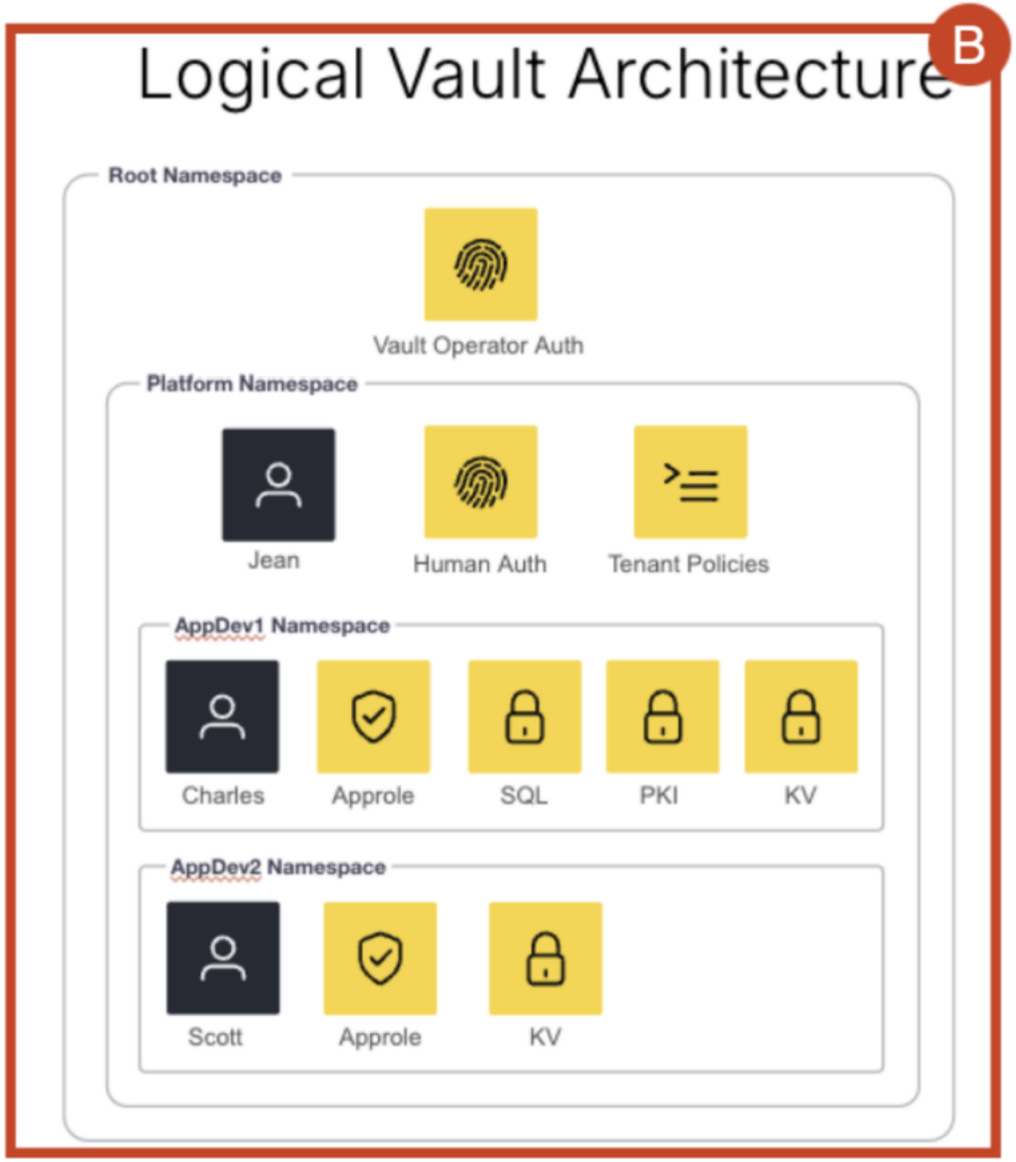


Use case supported by
- UKO for Containers
- UKO for z/OS

© 2026 IBM Corporation

Demo environment Architecture





IBM ONE Vault – Your Quantum Safe Enterprise Secrets & Key Management Hub

1 **Protect your Secrets**
Use your on-prem IBM crypto card and Confidential Computing to protect Secrets across the datacenter with IBM Vault and UKO Crypto Connect ACSP

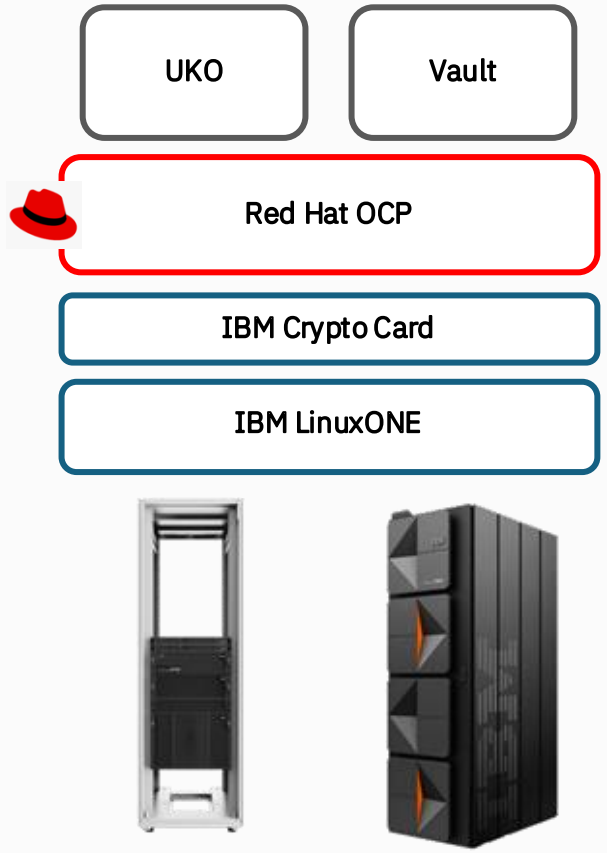
2 **Centralized Key Management for Applications**
Vault API based Key management facilities in conjunction with Encryption as a Service, Storage (KMIP) management, Transparent Data Encryption (TDE) for Databases & Middleware, DevSecOps

3 **Enterprise Key Mgmt for Hybrid Cloud**
Key management across Public Cloud and on-prem x86, IBM LinuxONE, Z, IBM Power, with root of trust in your on-prem HSM

4 **Network HSM for the Datacenter**
Encrypt data on x86 or IBM Power systems, leveraging your on-prem IBM crypto card over the network with Vault & UKO Crypto Connect ACSP

5 **Post-Quantum Cryptography for data protection and key management**
Protect Secrets, Keys, Digital Signatures with NIST-standardized ML-KEM and ML-DSA PQC algorithms.

6 **Storage Keys for data at-rest encryption**
Vault manages storage keys through KMIP protocol, across storage platforms



Leverage one or all the above use cases from a single solution with ONE Vault

Bartosz Dobrowolski | bartosz.dobrowolski@ibm.com