

*This
LinuxONE Security
Presentation was
Generated
by AI*

By Brian W. Hugenbruch, CISSP
bwhugen@us.ibm.com

**Sort of*

Who am I?

Brian Hugenbruch, CISSP

- 26 years in IBM and z/VM Development
- 20 years as a technical educator and public speaker
- Long-time platform security nerd
- “Sir Brian, Wielder of the Security Hammer”

What is this session?

Brian generated the following slides with AI

- [Last night](#), after he returned from dinner
- Beer may or may not have been involved

Other than a quick sanity check, Brian has neither validated the technical content, nor rehearsed this deck

What follows is an exercise in “scramble presenting” and “PowerPoint Karaoke”

Brian will present the slides **as generated**, and then will explain the methodology behind them

If you have questions, or see something incorrect, shout it out! Watch Brian pivot in real time! It'll be fun!

Note: **the PDF version of this deck** has **removed** the AI-generated content.

- While AI did a reasonable job, there were enough technical errors to make posting inadvisable
- To be clear, the prior slide is **not** the way to use AI / LLMs in any context
 - Human review always required
 - Iterate, don't "set and forget"
 - *The presentation as conducted was done as an exercise in silliness for the last session of the conference!*
- *As a result, 40 slides have been removed.*

Assessment

How this presentation was built: **watsonX Workshop**

IBM tooling for generation of presentation

- Based on prior IBM content (not Brian's, that he's aware of)
- Could have generated a shorter or longer presentation
- Uses standard IBM templates and approved graphics
- Tailorable based on audience
- Meant for “scramble presenting” – last-minute talks, rather than bespoke content

What is watsonx Workshop?

IBM watsonx Workshop is your AI-powered enablement partner, designed to help sales professionals learn faster, prepare smarter, and perform with confidence. Whether you're building pipeline, responding to RFPs, or mastering product knowledge, watsonx Workshop delivers a personalized, multilingual, interactive experience that adapts to your goals. Developed by IBM's global enablement team, watsonx Workshop is evolving rapidly through real user feedback.

At its core, watsonx Workshop empowers sellers with AI-driven agents that enhance learning, preparation, and execution, supporting every step of the sales journey.

This presentation

vs What Brian delivers at client briefings

5 IBM LinuxONE Emperor 5 Overview

6 Hardware-Rooted Security Foundation

7 PRISM Logical Partitioning Security

8 Why PRISM Isolation Matters

9 EAL5: Rigorous Assurance for PRISM

10 EAL5: Audit-Ready Security Evidence

11 Secure Boot & Measured Launch

12 Confidential Computing & Compliance

13 Hardware Vault: Defending the CPC

14 CPACF: Built-in Acceleration

15 CPACF: Accelerating Cryptography

16 CPACF: FIPS 140-2 Level 4 Validation

17 CryptExpress BS: Long-Term Key Protection

18 CryptExpress BS: Certifications and APIs

19 Cryptographic Roles: CPACF vs CryptExpress BS

20 Integrated Hardware Key Lifecycle

21 zVM Hypervisor Platform Overview

22 RBAC in zVM: Managed by Security Manager

23 RBAC: Enforcing Least Privilege in zVM

24 Network Security: VSWSwitch and VLAN Tagging

25 Strengthening Identity with IBM zMFA

26 Key Management

27 Vault: Secrets-as-a-Service

28 Centralized Key Distribution: URD

1 The Value of LinuxONE Security

2 Why is Linux on LinuxONE more secure?

3 IBM LinuxONE Value Proposition

4 Security & Resiliency

5 Mitigate growing risk and cost with an integrated and comprehensive cyber resiliency approach

6 Security Features: LinuxONE

7 Let's start with the hardware.

8 Let's start with the hardware.

9 If a core fails, a spare is "turned on" without system or program interruption

10 IBM LinuxONE 5 Crypto Hardware

11 What is CPACF?

12 CryptExpress BS Cleanup

13 The Problem

14 NSA - Commercial National Security Algorithm Suite 2.0

15 Hypervisors and Virtualization for IBM LinuxONE

16 Virtualization security requires some basics:

17 Virtualized Crypto Express devices for zVM virtual machines

18 This is your LinuxONE infrastructure on LockDown.

19 Linux Guest Security

20 Linux on LinuxONE is More Secure

21 Linux is More Secure on LinuxONE

22 Data Protection: LinuxONE Network Security

23 Data Protection: LinuxONE File System Encryption

24 LinuxONE Certification Stack

How this presentation was built: [watsonX Workshop](#)

PROMPT: The goal of this [40-minute presentation](#) presentation is to convey, from metal to cloud, all of the [security capabilities inherent in LinuxONE](#) -- especially when z/VM is part of the full stack. This technical overview [must be valuable for a highly technical audience](#), including z/VM systems programmers

[Focus the presentation](#) on:

- LinuxONE CPC security, with a detailed explanation of what EAL5 Common Criteria certification for PR/SM actually means
 - CPACF and CryptoExpress 8S
 - Hypervisor security, with a focus on z/VM RBAC, networking, isolation, and RACF for z/VM (as well as IBM Z MFA)
 - Vault, UKO, and Digital Assets Haven
 - Summarize end to end security for the platform
- Where possible, include LinuxONE images, stock photos, or z17 icons which will make the slides "pop."

How this presentation was built: [watsonX Workshop](#)

Elapsed time: 50 minutes

- 4 tries to come up with a reasonable prompt
- 5 minutes to generate the presentation
- 1 minute to remind myself not to correct the glaring errors
- 10 minutes to fix some issues (had to make slight modifications after combining the generated deck with the surrounding content – template mismatches)
- 30 minutes to build the surrounding metaphemera

- **Conclusion: took longer to explain how it was done, than to do it**

Could Brian have used more AI to refine? Yes:



This LinuxONE Presentation w...

This LinuxONE Presentation was Generated by AI - final.pptx The goal is an audience of system programmers for the mainframe, and I'd like to highlight technical capability, with the goal to inform. I would like better visual guidance and suggestions for slide improvements.

Copilot



Title:

Cryptography on LinuxONE: CPACF & CryptoExpress 8S

Content:

LinuxONE integrates two specialized cryptographic components—CPACF and CryptoExpress 8S—to deliver robust, hardware-rooted security for all workloads.

Visual Guidance:

- Use a layered architecture diagram showing both CPACF and CryptoExpress 8S.
- Add icons for hardware, keys, and compliance.

Could Brian have used AI to refine? Yes.

Here is Copilot summarizing what watsonx produced:

LinuxONE Emperor 5 delivers end-to-end security and cryptography, integrating hardware-rooted protection from the metal up to the cloud. The platform unifies virtualization, containers, and hybrid cloud, offering continuous availability, extreme scalability, and energy-efficient processing. Confidential computing ensures data is protected during processing, aligning with FIPS-140-2 Level 4 and global compliance standards. PR/SM logical partitioning creates isolated LPARs, enforced by EAL5 Common Criteria certification for rigorous assurance and audit-ready evidence. Secure Boot and Measured Launch guarantee only IBM-signed firmware runs, blocking unauthorized changes and supply-chain attacks. Cryptography is accelerated by CPACF, built into every processor chip, supporting AES, SHA, RSA, ECC, and quantum-resistant algorithms, with seamless OS integration and FIPS validation. CryptoExpress 8S provides enterprise-grade hardware security modules, offering tamper-resistant storage, dual-processor redundancy, and flexible API integration. Together, CPACF and CryptoExpress 8S enable secure key management, wrapping, and lifecycle automation via Vault, Unified Key Orchestrator, and Digital Assets Haven. z/VM hypervisor enforces granular security with RBAC, RACF, MFA, and network isolation through VSWITCH, VLAN tagging, and per-vNIC controls. Centralized identity and access management, defense-in-depth, and secure network stack ensure compliance and mitigate insider threats. The architecture supports secure asset storage, automated key rotation, and regulatory compliance for digital assets, blockchain keys, and AI models. Hyper Protect Container Runtime extends cryptographic assurance to containers, with policy-bound execution, secure enclaves, and zero-knowledge key release. LinuxONE's unified security model spans on-premises and cloud, delivering comprehensive data protection, operational trust, and measurable ROI for mission-critical workloads.

LINUXONE EMPEROR 5

End-to-End Security & Cryptography
From the Metal Up to the Cloud



CONFIDENTIAL COMPUTING

Data protected while in use



COMPLIANCE ASSURANCE

FIPS 140-2 Level 4
EAL5 Certified



HYBRID & CLOUD READY

Unified security on-prem and cloud



SUSTAINABLE BY DESIGN

Energy-efficient and cost-effective



HARDWARE-ROOTED SECURITY FOUNDATION

- Secure Service Processor (SSP) anchors trusted environments
- Keys never leave secure hardware boundaries
- Hardware-based key management ensures integrity and tamper resistance
- Foundation for cryptographic operations and compliance



PR/SM: LOGICAL PARTITIONING & ISOLATION

- PR/SM creates isolated LPARs with dedicated CPU, memory and I/O
- Hardware-enforced isolation prevents access between partitions
- Supports secure multi-tenant environments



EAL5 COMMON CRITERIA ASSURANCE

- PR/SM certified to EAL5 for rigorous assurance
- Extensive independent evaluation, source code review, penetration & vulnerability testing
- Provides audit-ready evidence for GDPR, NIST 800-53 and other regulations



SECURE BOOT & MEASURED LAUNCH

- Firmware digitally signed and verified
- Each boot stage measured and recorded in the Secure Service Processor
- Blocks unauthorized firmware and supply-chain attacks



CRYPTOGRAPHY ACCELERATION & PROTECTION

- CPACF: Built-in acceleration for AES, SHA, RSA, ECC, and quantum-resistant algorithms (FIPS 140-2 Level 4)
- CryptoExpress 8S: Enterprise HSM with tamper-resistant storage, dual processors, and flexible API support (PKCS#11, KMIP, IBM KMS)
- Together deliver high performance and strongest key protection



z/VM: SECURE VIRTUALIZATION LAYER

- Granular RBAC with RACF integration and MFA
- Network isolation with VSWITCH, VLAN tagging and per-vNIC controls
- Centralized identity & access management
- Defense-in-depth to mitigate insider threats and ensure compliance



KEY MANAGEMENT & ASSET PROTECTION

- Vault, Unified Key Orchestrator (UKO) and Digital Assets Haven secure keys and assets
- Automated key lifecycle, rotation and policy enforcement
- Protects digital assets: tokens, blockchain keys, AI models and more



CONTAINER SECURITY & CONFIDENTIAL COMPUTING

- Hyper Protect Container Runtime extends cryptographic assurance to containers
- Policy-bound execution with attestation and secure enclaves
- Zero-knowledge key release only when policy and runtime integrity are verified



LINUXONE SECURES AI, DATA AND CRITICAL WORKLOADS

UNMATCHED SECURITY. UNCOMPROMISING TRUST. BUILT FOR THE FUTURE.



SECURITY



PERFORMANCE



LOWER TCO

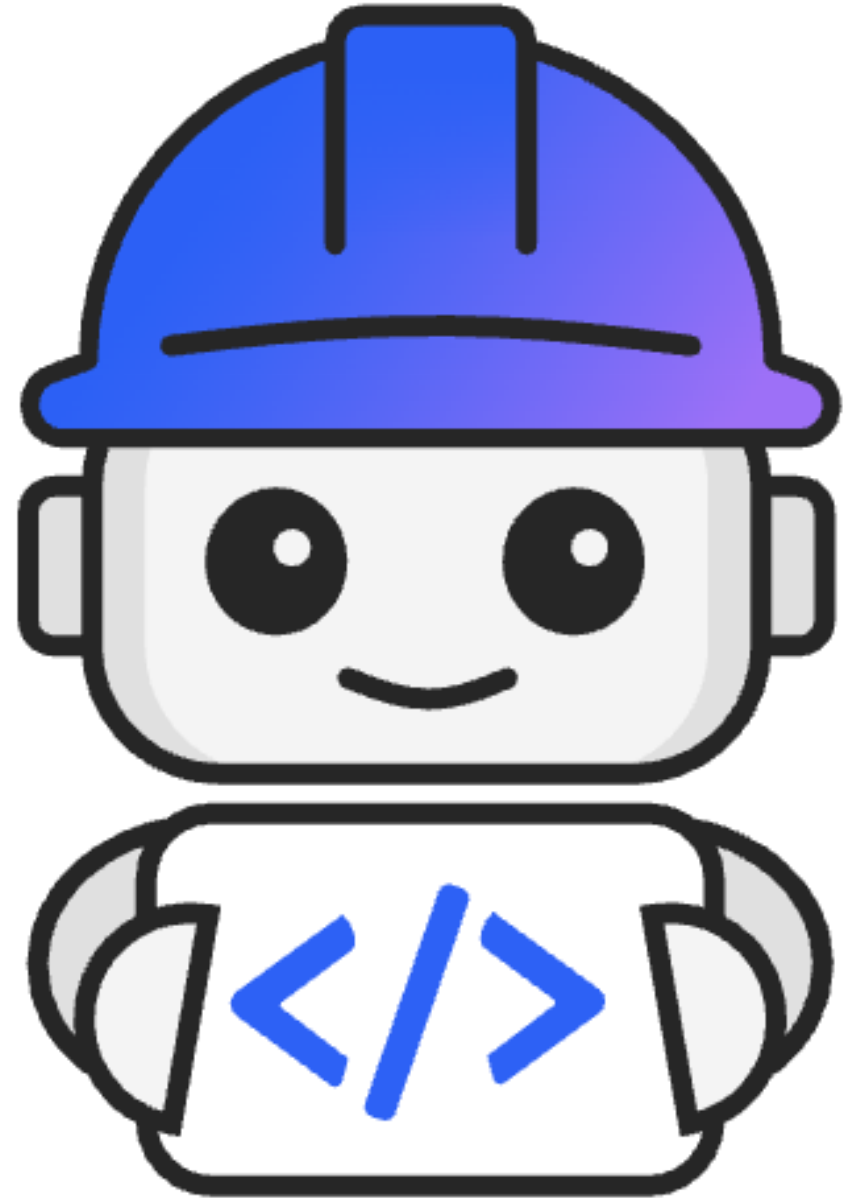


BUSINESS VALUE

- Shows an IBM z16

What about Bob? (1/2)

Prompt: Hi Bob. I'm going to copy/paste some text summarizing LinuxONE security features at a high level. Please produce a crisp but detailed breakdown of the content, expanding upon important technical features while identifying any errors. Do you have any questions before we begin?



What about Bob? (2/2)

LinuxONE Emperor 5 Security Analysis

Hardware-Level Security

CPACF (Central Processor Assist for Cryptographic Functions)

- Integrated into every processor core (not just "chip")
- Hardware-accelerated: AES, SHA-2/SHA-3, RSA, ECC (P-256, P-384, P-521)
- Quantum-resistant algorithms: Dilithium (ML-DSA), Kyber (ML-KEM)
- FIPS 140-3 validated (not just 140-2)
- Zero-latency cryptographic operations via CP Assist instructions

CryptoExpress 8S HSM

- FIPS 140-2 Level 4 certified (highest commercial grade)
- Tamper-responsive (not just resistant): active zeroization on physical intrusion
- Dual crypto processors for redundancy and performance
- EP11, PKCS#11, CCA API support
- Secure key storage with master key hierarchy

Firmware & Boot Security

Secure Boot

- IBM-signed firmware enforcement via hardware root of trust
- Cryptographic chain of trust from POWER-on Self Test through hypervisor
- Prevents unauthorized firmware/bootloader modifications

Measured Launch

- TPM-equivalent attestation via Trusted Boot
- Cryptographic measurements stored in secure registers
- Remote attestation capability for compliance verification

Errors & Clarifications

Error 1: "FIPS-140-2 Level 4" for platform

- **Correction:** Platform achieves FIPS 140-2 Level 4 via CryptoExpress 8S HSM. CPACF is FIPS 140-3 Level 1 (algorithm validation, not module certification).

Error 2: "EAL5 Common Criteria certification"

- **Correction:** PR/SM holds EAL5+ certification. z/VM is EAL4+ certified. Distinction matters for audit requirements.

Ambiguity 1: "Quantum-resistant algorithms"

- **Clarification:** CPACF supports NIST PQC finalists (Dilithium, Kyber) as of firmware SE770. Not all quantum-resistant algorithms are hardware-accelerated.

Ambiguity 2: "Digital Assets Haven"

- **Clarification:** This appears to reference IBM Hyper Protect Digital Assets, a blockchain key custody solution. Not a standalone z/VM component.

Missing Context

Not Mentioned

- Pervasive Encryption: Dataset-level encryption with minimal performance overhead
- Crypto Express Network: Secure communication between HSMs across LPARs
- ICSF (Integrated Cryptographic Service Facility): z/OS crypto management layer
- Secure Service Container: Tamper-resistant appliance model for sensitive workloads

Summary (hand-crafted)

- The past year has shown some fantastic evolutions in AI usage
- The presentation space can benefit from AI
 - Faster drafting
 - Image creation
 - Validation and some degree of fact checking
 - *Especially nice for when Brian is writing this presentation the night before*
- **Humans still required**
 - Always validate the content
 - Always iterate and improve – use the tools properly!
 - Won't replace a bespoke story – bullet points don't form a personal connection

Brian W. Hugenbruch 
IBM z/VM Security and Cryptography Product Owner


IBM webpage:


<https://www.vm.ibm.com/devpages/hugenbru/>

Technical Blog: <https://bwhugen.github.io/>

Social Media:

 <https://www.linkedin.com/in/bwhugen/>

 @the_lettersea

 @apictureofaman@infosec.exchange



IBM Z
Federated
Advocate
Super Hero

Federated Advocate Program
Mastery



Trustworthy 
AI and
AI Ethics

IBM Office of Privacy and
Responsible Technology
Foundational



AI+ Content 
Creator with
watsonx
Workshop

Technology Sales
Foundational