IBM zSystems and LinuxONE Security

Anne Dames
IBM Distinguished Engineer, IBM zSystems
Cryptographic Technology Development

Security innovation driven through platform strategy

April 7th, 1964 – April 5th, 2022
4 Generations of Technology
12 Families of Innovation

IBM z14™

Crypto Express6s
CPACF

IBM z15™

Crypto Express7s
CPACF
Compression

IBM z16™

IBM Telum Processor

Crypto Express8s
CPACF
Compression
Memory Encryption

IBM zSystems & LinuxONE Security Leadership

Approach: Security integrated into all levels of the stack

Data Protection

Data Privacy
Confidential Computing

Cyber Resiliency
Continuous Compliance
Quantum Safe
Validated Boot for z/OS

Security innovation driven through platform strategy

April 7th, 1964 – April 5th, 2022
4 Generations of Technology
12 Families of Innovation

IBM z14™

Crypto Express6s
CPACF

IBM z15™

Crypto Express7s
CPACF
Compression

IBM z16™

IBM Telum Processor

Crypto Express8s
CPACF
Compression
Memory Encryption

IBM zSystems & LinuxONE Security Leadership

Approach: Security integrated into all levels of the stack

Data Protection

Data Privacy
Confidential Computing

Cyber Resiliency
Continuous Compliance
Quantum Safe
Validated Boot for z/OS

z16 Data Protection

encryption on-chip

+ z15 compression on-chip

+ z15 Fibre Channel Endpoint Security

+ z15 Secure Execution for Linux

+ z16 Memory Encryption

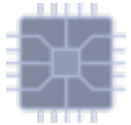
4

Protect z16 data in-flight, at-rest, and in-memory with capabilities integrated across hardware, OS, and middleware.

Focus on transparent adoption without application change and no Impact to SLAs.

Pervasive encryption with IBM Z and IBM® LinuxONE

Enabled through tight platform integration

Integrated Crypto Hardware		Hardware accelerated encryption on every core, CPACF performance improvements of 7x Crypto Express6S – PCIe Hardware Security Module (HSM) & Cryptographic Coprocessor
Data at Rest		Broadly protect Linux file systems and z/OS data sets using policy-controlled encryption that is transparent to applications and databases
Clustering		Protect z/OS Coupling Facility data end-to-end, using encryption that's transparent to applications
Network		Protect network traffic using standards-based encryption from end to end, including encryption readiness technology to ensure that z/OS systems meet approved encryption criteria
Secure Service Container		Secure deployment of software appliances including tamper protection during installation and runtime, restricted administrator access, and encryption of data and code in-flight and at-rest
Key Management		The IBM Enterprise Key Management Foundation (EKMF) provides real-time, centralized secure management of keys and certificates with a variety of cryptographic devices and key stores

Security innovation driven through platform strategy

April 7th, 1964 – April 5th, 2022
4 Generations of Technology
12 Families of Innovation

IBM z14™

Crypto Express6s
CPACF

IBM z15™

Crypto Express7s
CPACF
Compression

IBM z16™

IBM Telum Processor

Crypto Express8s
CPACF
Compression
Memory Encryption

IBM zSystems & LinuxONE Security Leadership

Approach: Security integrated into all levels of the stack

Data Protection

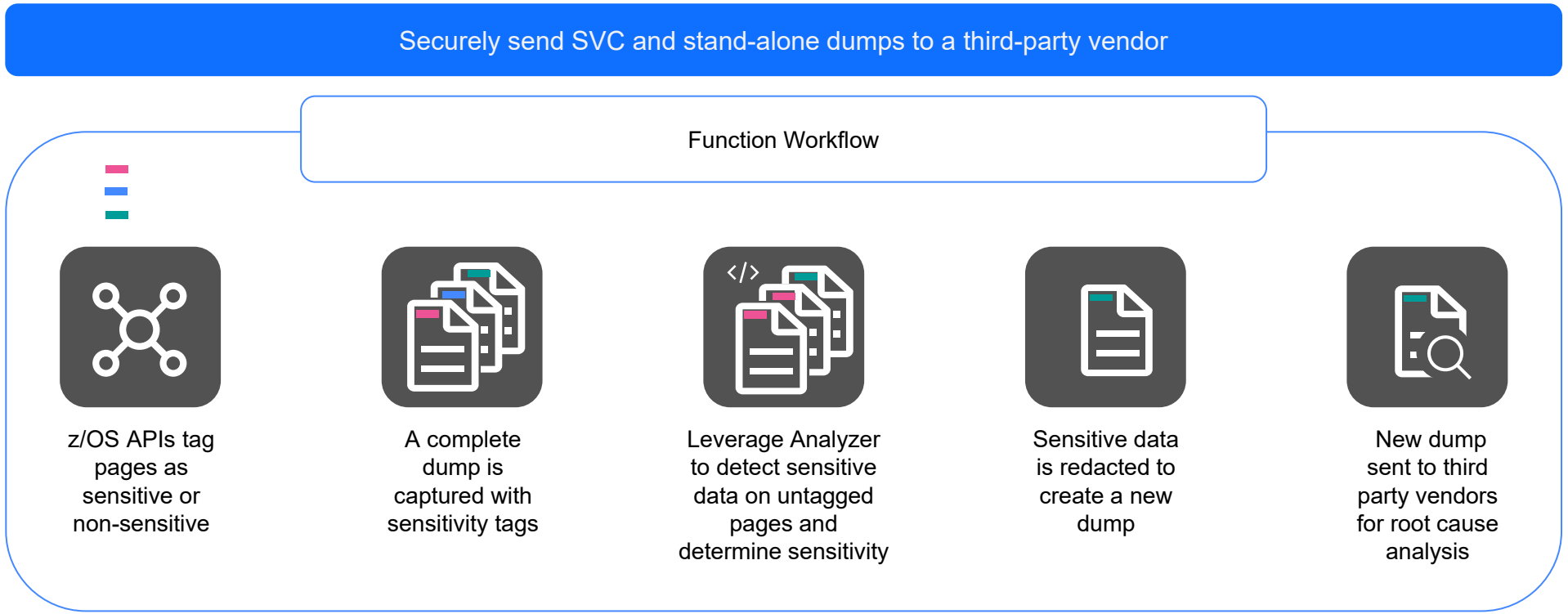
Data Privacy
Confidential Computing

Cyber Resiliency
Continuous Compliance
Quantum Safe
Validated Boot for z/OS

z/OS Data Privacy for Diagnostics

The only z/OS function that is designed to:

- Help clients **address compliance challenges** in the area of diagnostic data
- Help clients **more securely share** diagnostic data with third-parties
- Tag and redact sensitive diagnostic data **in minutes***



*Disclaimer: as measured in lab environment

Security innovation driven through platform strategy

April 7th, 1964 – April 5th, 2022
4 Generations of Technology
12 Families of Innovation

IBM z14™

Crypto Express6s
CPACF

IBM z15™

Crypto Express7s
CPACF
Compression

IBM z16™

IBM Telum Processor

Crypto Express8s
CPACF
Compression
Memory Encryption

IBM zSystems & LinuxONE Security Leadership

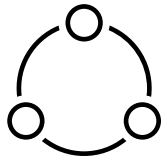
Approach: Security integrated into all levels of the stack

Data Protection

Data Privacy
Confidential Computing

Cyber Resiliency
Continuous Compliance
Quantum Safe
Validated Boot for z/OS

The audit process can be challenging



“The biggest challenge that we have …is gathering evidence for compliance” -CISO

Interpreting Requirements

Typically, requirements are written with distributed frameworks in mind. Leaving is up to the Line of Business Owners the responsibility of understanding new & changing regulations and how they map to their IT environments.

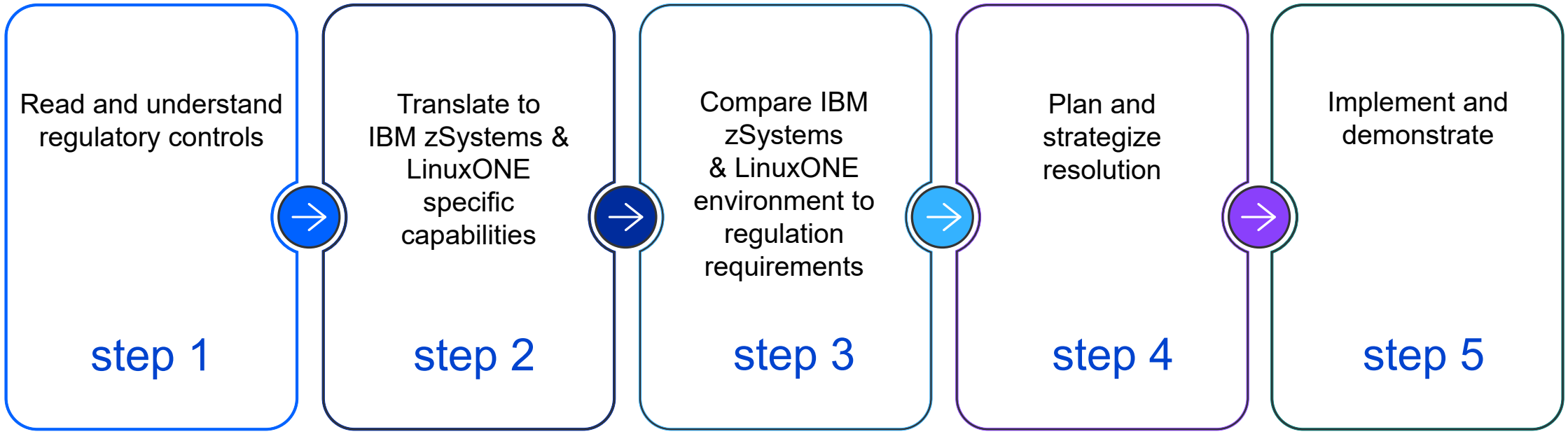
Evidence Collection

Manually extracting configuration data and storing it in spreadsheets or distributed databases comes with its many challenges. System changes, script management, missing data, and more.

Demonstrating Posture

When a CISO or an Auditor come to IBM Z teams asking for an update on compliance, producing a point in time report of posture often takes weeks or months. By the time the report is finalized, it is typically no longer accurate.

A Typical Audit Journey



IBM Z Security and Compliance Center

A modern application specifically designed for progressing towards a state of continuous compliance readiness with over 1000 pre-built goal validations and customizability.

Optimize Resources	Assess Compliance Posture	Identify Compliance Drift
Automates the collection and validation of facts against goals to help increase visibility into potential compliance oversights and reduce manual errors.	Interactive dashboard provides a view of current compliance posture for PCI-DSS and NIST SP800-53 regulations to help simplify audit preparations and improve continuous compliance operations.	Track compliance drift over time with dashboard style visualizations which display historical compliance scores, to help clients better understand their compliance posture

Reduce number of skilled resources needed for audit preparation functions by over 40%[1]

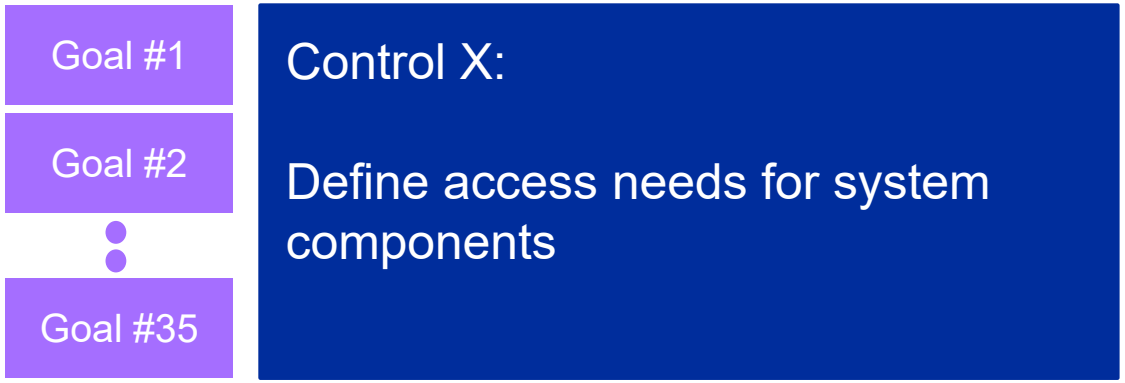
Reduce audit preparation time from one month to one week[2]

IBM Z Security and Compliance Center Terminology

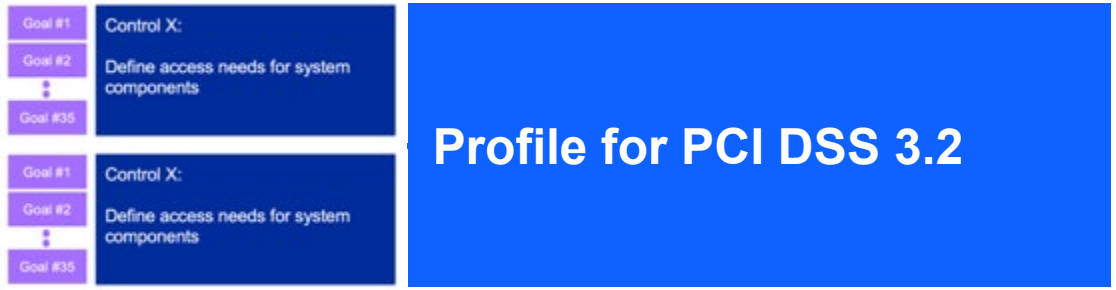
A goal is a specific technical check that can be run on data to produce a pass or fail

Goal #1 “Check whether only authorized users can access Db2 from CICS”

A control is a group of goals around a common theme which typically to a defined rule



A profile is a group of controls which will be match applicable regulatory frameworks



Payment Card Industry Data Security Standard (PCI-DSS) 3.2.1

Applicable to all entities that store, process, and/or transmit cardholder data.

Typical clients:

- Banking
- Financial
- Insurance
- Retail
- Mortgage

National Institute of Standards & Technology (NIST) SP 800-53

Applicable to all US federal government agencies and contractors; referenced by local governments and private industry regulations such as PCI-DSS.

Typical clients:

- Federal govt
- State / local govt

Center of Internet Security (CIS) Benchmarks

Applicable to organizations in all industries and geographies including government, business, industry and academic institutions.

Typical clients:

- Banking
- Financial
- Insurance
- Retail
- Mortgage
- Federal govt
- State / local govt

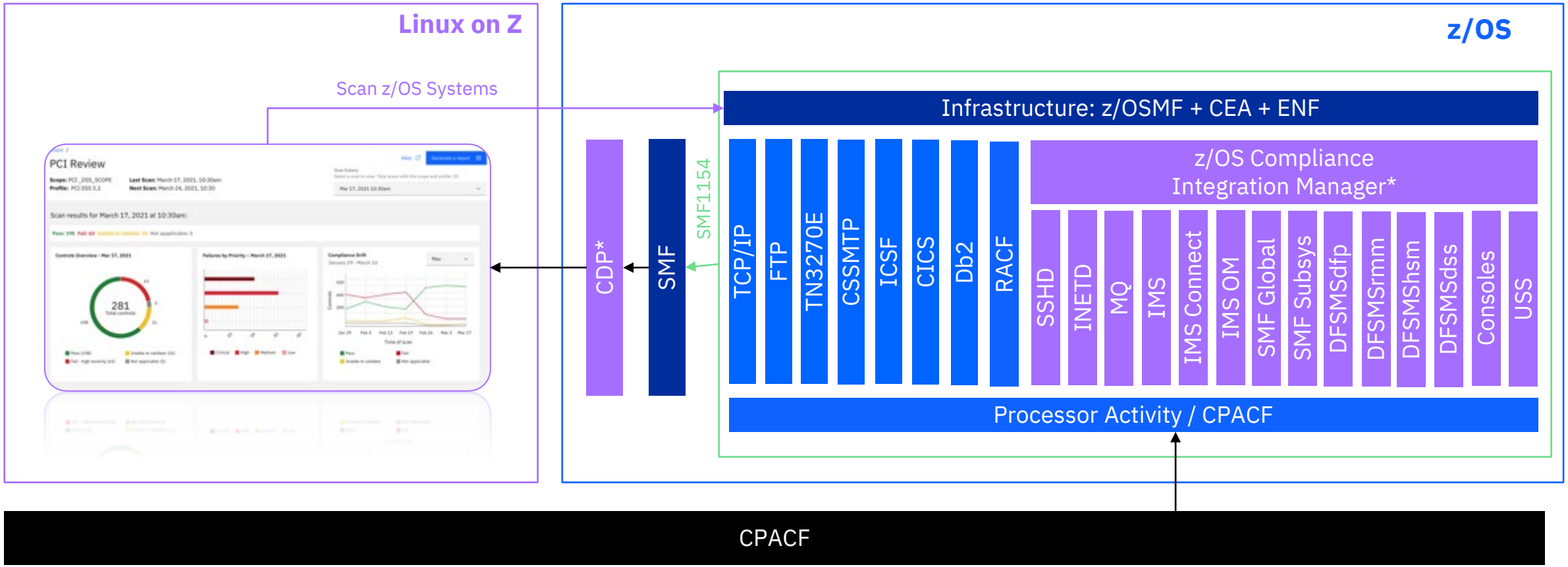
Solution Overview

z/OS Point of View

Update: *We plan to entitle zSCC customers to deploy the product on z15 or z16. And it can be used to gather evidence from all Z generations*

IBM Z Security & Compliance Center collectors connect to a resource, such as z/OS or Linux on Z, and scan for compliance data. For z/OS, the collector connects to a z/OSMF compliance REST API which triggers sysplex-wide compliance data collection using an ENF86 signal.

Participating z/OS components and products listen for the new ENF86 signal. When received, these components write compliance data to SMF 1154 records associated with a unique subtype. The SMF records are streamed to IBM Z Security & Compliance Center using the Common Data Provider. Then, the IBM Z Security & Compliance Center maps the compliance data to the appropriate regulatory controls associated with a profile for validation, display and reporting.



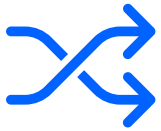
* The z/OS Compliance Integration Manager and CDP are delivered with the IBM Z Security & Compliance Center

Keeping Up With Compliance

In collaboration with IBM Security, IBM Research, IBM zSystems & LinuxONE

Interpret Regulations

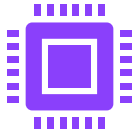
Determine which regulations are relevant for your organization



Map IBM zSystems capabilities to those regulations

Easily show how IBM zSystems & LinuxONE capabilities meet or exceed industry standards.

Implement Controls



Discover new IBM zSystems capabilities to meet compliance

Engage IBM experts to deploy new features and submit RFEs to request new capabilities

Utilize new capabilities throughout the IBM stack to meet compliance.

Collect & Validate Evidence

Identify which data is essential for auditors.

Regularly collect and validate compliance data

Optimize your audit process to reduce time and effort.

Security innovation driven through platform strategy

April 7th, 1964 – April 5th, 2022
4 Generations of Technology
12 Families of Innovation

IBM z14™

Crypto Express6s
CPACF

IBM z15™

Crypto Express7s
CPACF
Compression

IBM z16™

IBM Telum Processor

Crypto Express8s
CPACF
Compression
Memory Encryption

IBM zSystems & LinuxONE Security Leadership

Approach: Security integrated into all levels of the stack

Data Protection

Data Privacy
Confidential Computing

Cyber Resiliency
Continuous Compliance
Quantum Safe
Validated Boot for z/OS

Our modern digital world depends on *cryptography*

What is cryptography?
A tool we use when we have use cases that require data confidentiality, integrity, authentication, proof or authorship or non-repudiation.

Cryptography impacts everything

Cryptography touches every corner of the digital world

Internet Protocols

Domain Name Service(DNS), Hyper-text Transfer Protocol (HTTP), Telnet, SFTP

Critical Infrastructure

Code updates; Control systems- Oil pipelines, Electric grids; Car systems,…

Blockchain Applications

Coin wallets, Transactions, Authentication

Digital Signature Laws

EiDAS - PDF Advanced Electronic Signature – (PAdES), Advanced Electronic Signatures (AES), …

Financial Systems

Payment Systems: (EMV, SWIFT, Settlement Systems, FinTech, …)

Enterprise Applications

EMAIL – PGP, Identity Management PKI/LDAP/.., Virus scanning patterns, PKI Services

The Problem

Symmetric key and hashing algorithms:

Impacted by quantum computing – algorithm strengths are reduced

Example Mitigations:

Increase the key or digest sizes (i.e., AES-256, SHA2)

Public key algorithms:

Completely broken by large scale quantum computer

Example Mitigations:

New algorithms and schemes needed

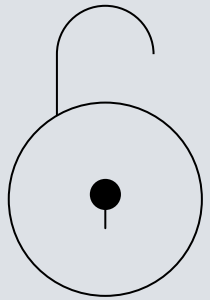
The Impact

- **Shor's algorithm** for factoring and discrete logarithms can completely break the RSA and Diffie-Hellman cryptosystems, and their elliptic-curve-based variants
  - To address an attack using **Shor's algorithm**, we need **new Math/Algorithms for classical computers**
- **Grover's algorithm** could be used to speed up an exhaustive search for symmetric keys or reverse engineer a cryptographic hash
  - To address an attack using **Grover's algorithm**, we need to **grow the key and message digest sizes**

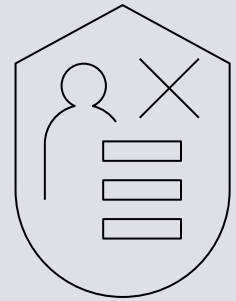
Algorithm*	**Purpose**	**Impact from quantum computer**
DES, TDES	Encryption	No longer secure
AES-256	Encryption	Secure
SHA-256, SHA-3	Hash Functions	Secure
RSA	Signatures, Key Establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Signatures, Key Exchange	No longer secure
DSA (Finite Field Cryptography)	Signatures, Key Exchange	No longer secure

What will a cyber criminal be able to do?

Manipulate updates and forge transactions through fraudulent authentication



Decrypt lost or harvested confidential historical data through cracking encryption keys



Manipulate legal history by forging digital signatures

Find or Derive your Keys

Adversaries can:

- Create fake identities for websites
- Create fake software downloads and software updates
- Launch extortion attacks by threatening to disclose harvested data
- Create indistinguishable fraudulent land records or lease documents

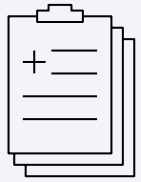
There are new attack vectors that did not exist before

Data is being stolen today with the intent of exposing it tomorrow

- Encrypted data lost during a data breach
- Data communications over TLS that has been harvested
- Snapshots of encrypted cloud data
- Media that is not encrypted with quantum-safe encryption methods and is improperly disposed or lost
- Encryption systems using blackened(wrapped) encryption keys that are public

Quantum-safe – So what? Why is the time to act now?

Data confidentiality



Healthcare data

- Guide 0068 – Clinical Trials (US) – 25 Years
- Health Records (Japan) – 100 Years
- Mental Health Records (UK) – 20 Years
- Radiation Records (D) – 100 Years

Finance data

- Tax Records 7-10 Years in most countries, Sarbanes Oxley
- Trade secrets, Mergers and Acquisitions up to 50 years
- Confidentiality agreements – (P) 50 Years
- Payroll records – (Rou) 50 Years

Government data

- Secure Intelligence Sharing
- Toxic Substances Control Act / Occupational Safety and Health Act – 30 years
- Military Data
- Dumpsite Record (I) – 30 Years

“There is a 1 in 7 chance that fundamental public-key crypto will be broken by quantum by 2026, and ***a 1 in 2 chance of the same by 2031***.”

Dr. Michele Mosca
Institute of Quantum Computing,
University of Waterloo

Quantum computers can, in principle, perform certain mathematical algorithms exponentially faster than a classical computer

Unstructured (random number) search

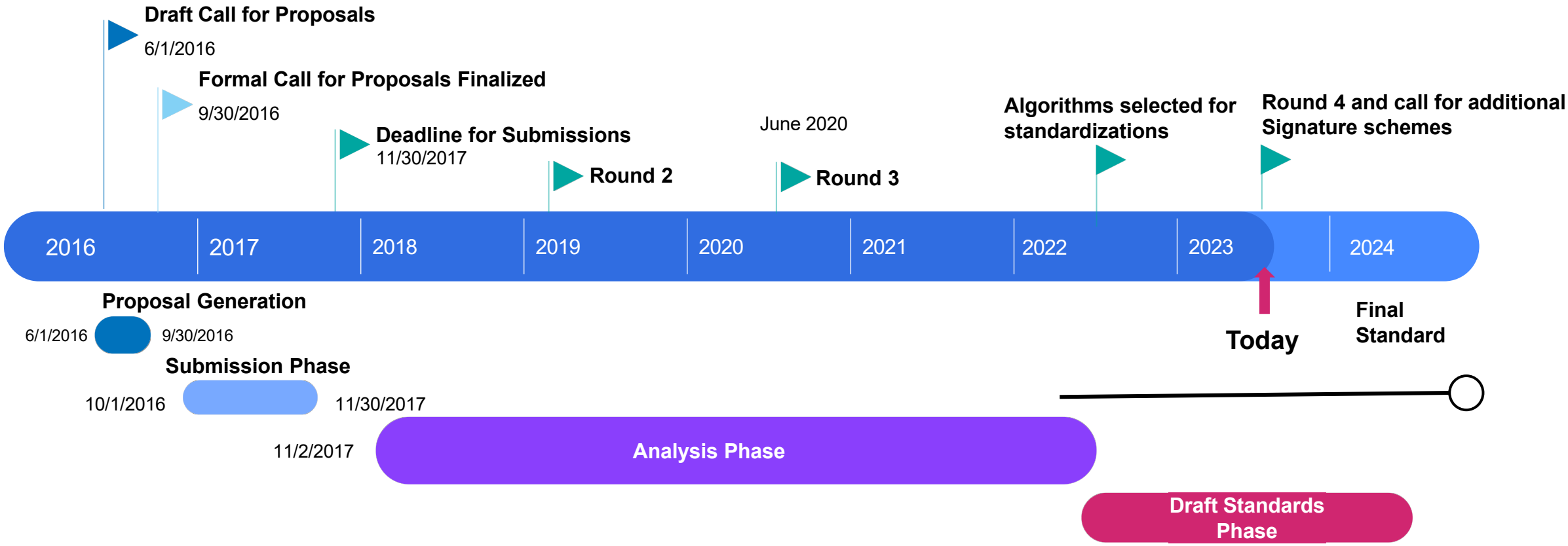
Grover’s algorithm could be used to speed up an exhaustive search for symmetric keys or reverse engineer a cryptographic hash.

Complex math operations

Shor's algorithm for factoring and discrete logarithms can completely break the RSA and Diffie-Hellman cryptosystems, and their elliptic-curve-based variants.

NIST standardization for quantum safe cryptography

Standardization Announcement July 5th!



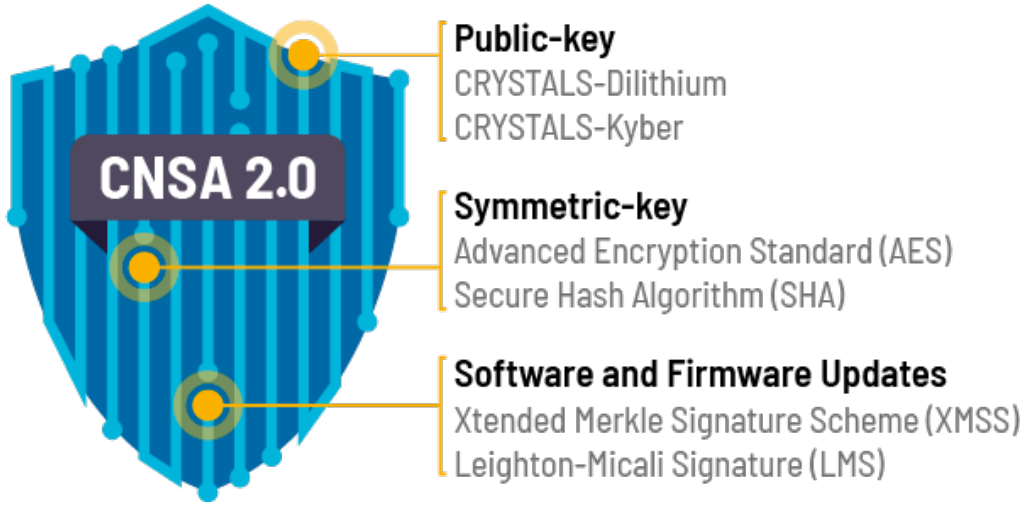
- National Institute of Standards and Technology(NIST) initiates process
- Industry communication protocols and other industry specific standards updates will follow based on the publication of the NIST standards
- This will drive client requirements – Compliance / Regulatory / Audit

NSA - Commercial National Security Algorithm Suite 2.0

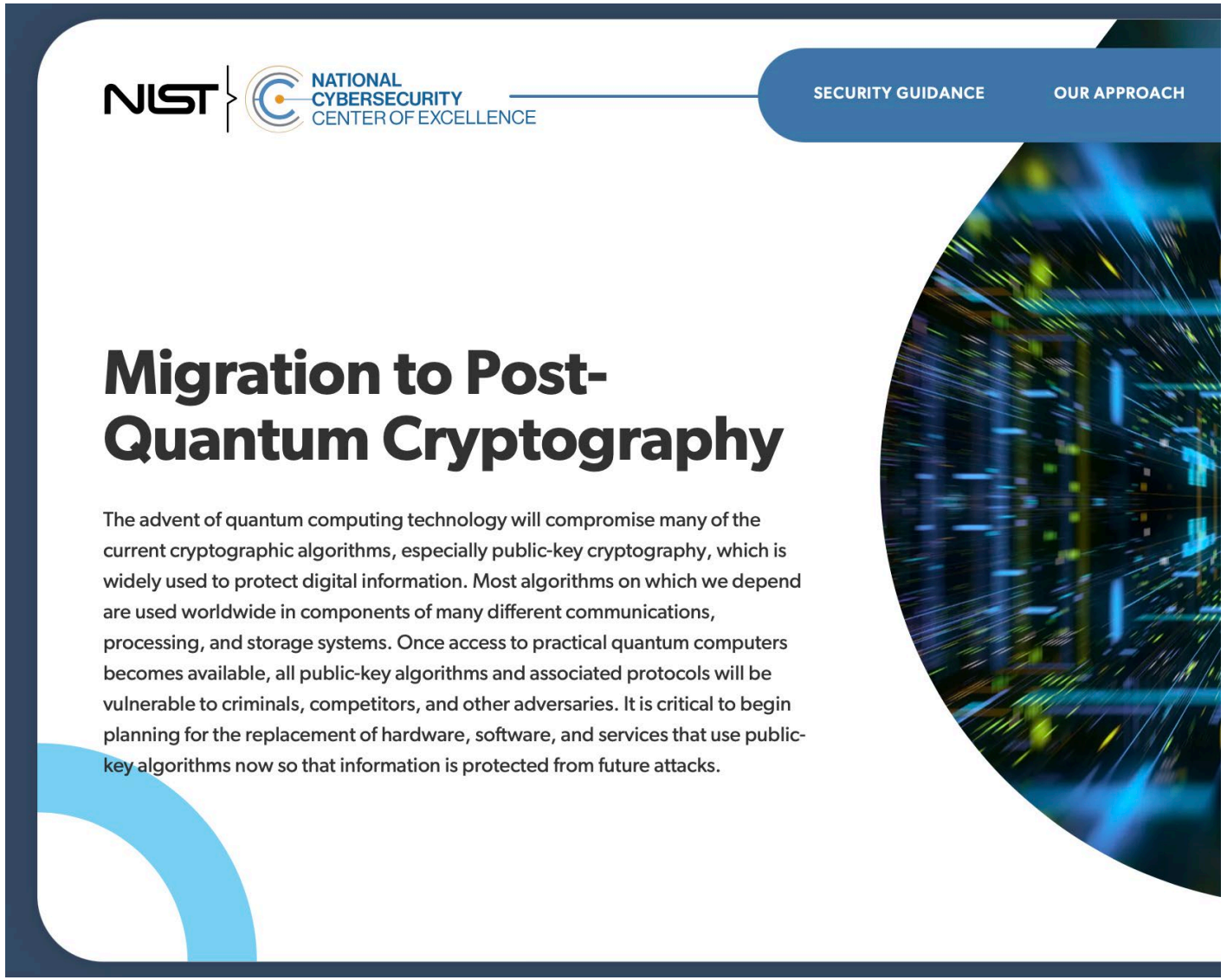
NSA anticipates the following timetable for implementing other CNSA 2.0 requirements for NSS:

- Software and firmware signing: begin transitioning immediately, support and prefer CNSA 2.0 by **2025**, and exclusively use CNSA 2.0 by **2030**.
- Web browsers/servers and cloud services: support and prefer CNSA 2.0 by **2025**, and exclusively1 use CNSA 2.0 by **2033**.
- Traditional networking equipment (e.g., virtual private networks, routers): support and prefer CNSA 2.0 by **2026**, and exclusively use CNSA 2.0 by **2030**.
- Operating systems: support and prefer CNSA 2.0 by **2027**, and exclusively use CNSA 2.0 by **2033**.
- Niche equipment (e.g., constrained devices, large public-key infrastructure systems): support and prefer CNSA 2.0 by 2030, and exclusively use CNSA 2.0 by **2033**.
- Custom applications and legacy equipment: update or replace by **2033**

NSA sets 2035 deadline for adoption of post-quantum cryptography across national security systems



IBM is an NCCoE Collaborator for this Project



Collaborating Vendors

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement to collaborate with NIST in a consortium to build this example solution.

- Amazon Web Services, Inc. (AWS)
- Cisco Systems, Inc.
- Crypto4A Technologies, Inc.
- CryptoNext Security
- Dell Technologies
- DigiCert
- Entrust
- IBM
- Information Security Corporation
- InfoSec Global
- ISARA Corporation
- JPMorgan Chase Bank, N.A.
- Microsoft
- PQShield
- Samsung SDS Co., Ltd.
- SandboxAQ
- Thales DIS CPL USA, Inc.
- Thales Trusted Cyber Technologies
- VMware, Inc.
- wolfSSL

IBM z16 industry-first[1] quantum-safe system

Quantum-safe technology and key management services were developed to help protect data and keys against a potential future quantum attack like harvest now, decrypt later

Quantum-safe System

Industry first quantum-safe system* protected by quantum-safe technologies through multiple layers of firmware
Helps protect IBM z16 firmware from quantum attacks through a built-in dual signature scheme with no changes required

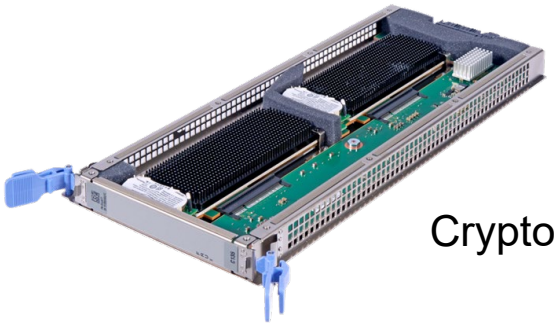
*Please See Disclaimer on next page.

Create Crypto Inventory

Discover where and what crypto is used in applications to aid in developing a crypto inventory for migration and modernization planning New crypto discovery features in IBM Application Discovery and Delivery Intelligence (ADDI) to analyze source code and discover crypto usage in applications. Using ADDI can improve productivity up to 30%.

Protect Sensitive Data

New Crypto Express card with quantum-safe APIs to modernize existing and build new applications leveraging quantum-safe cryptography along with classical cryptography



Crypto Express 8s

DISCLAIMER

DISCLAIMER: IBM z16 with the Crypto Express 8S card provides hardware enabled quantum-safe APIs. The quantum-safe public key technology used in IBM z16 has been selected by NIST to become part of its post-quantum cryptographic standard. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms Quantum-safe cryptography refers to efforts to identify algorithms that are resistant to attacks by both classical and quantum computers, to keep information assets secure even after a large-scale quantum computer has been built. Source: https://www.etsi.org/technologies/quantum-safe-cryptography." These algorithms are used to help ensure the integrity of a number of the firmware and boot processes. IBM z16 is the Industry-first system protected by quantum-safe technology across multiple layers of firmware. According to Peter Rutten, Research Vice-President IDC, "z16 is the industry's first quantum-safe computing platform."

z16 capabilities

Infrastructure hardening

Hardening of crypto related components (HSM, TKE, etc.) with quantum-safe protections

- HSM internal changes to support Quantum Safe protection of HSM firmware using Dual Signing (Quantum safe & Classical algorithms)
- Operating system updates to support the new Crypto Express Card HSM (CEX8S)
- TKE internal changes to use Quantum-Safe Cryptography (QSC) for:
  - Authenticating the CEX8S
  - Verifying replies from the CEX8S
  - Protecting key parts in flight for CCA

System hardening that leverages quantum-safe technologies

- Pervasive Encryption internal key handling support using Quantum Safe protections with Hybrid Key Exchange mechanism using CRYSTALS-Kyber & ECDH and Dual Signing Scheme using CRYSTALS-Dilithium & ECC
  - Benefits:
    - LoZ – Protected key dm-crypt
    - Data Set Encryption
    - Coupling Facility Encryption
    - z/VM – Encrypted Paging
  - RACF QS Encrypted VSAM Database Support
  - Also leverages Pervasive Encryption

z16 capabilities

Application development

- Crypto Express 8S(CEX8S)
- Quantum-safe key management APIs and lifecycle management support (QS key generation, import, export, etc.)
- Quantum-safe algorithm APIs (Digital Signature Generation, Key Encapsulation, Encryption*, Ciphertext Translation*)
- Fully available hybrid key exchange mechanism usable from the CCA API, with all operations performed in the CEX8S

Leverage quantum-safe technology in your applications

- EKMF Key Management support for Dilithium and Kyber keys in support of new QS Algorithm APIs
- z/VM – Guest support for Quantum Safe APIs on virtualized Crypto Express features (Linux, z/OS, VSE)
- Use cases:
  - Quantum-safe Key Generation
  - Quantum-safe Data Protection
  - Quantum-safe Dual Digital Signatures
  - Quantum-safe Hybrid Key Exchange Schemes

IBM z16 quantum-safe APIs will enable clients to begin using quantum-safe cryptography along with classical cryptography as they begin modernizing existing applications and building new applications.

*APIs existed in prior machine generations but are useful in the quantum-safe context.

Your Journey to Quantum Safe Starts with z16

Crypto Inventory

- Identify how your data is encrypted
- Create your cryptography inventory (containing certificates, encryption protocols, algorithms, key lengths, etc.)
- Manage your cryptography inventory and the lifecycle of certificates, encryption keys, etc.

Crypto Agility

- Define and implement processes to update / replace cryptography with well-defined lead-times
- Take all dimensions of crypto agility into account
- Test your crypto agility

Quantum-Safe Algorithms

- Implement quantum-safe cryptography
- Consider key management for quantum safe cryptographic keys
- Understand the performance impact of quantum-safe crypto on the business

z16 tooling to aid crypto inventory

IBM Application Discovery and Delivery Intelligence (ADDI) with Crypto Discovery

- Discover where and what crypto is used in applications
- Aid in migration and modernization planning
- Capture valuable metadata and dependencies

Dynamic Crypto Usage Tracking

- Provides workload correlated crypto usage data for ICSF callers
- New workload correlated crypto usage data for CPACF callers

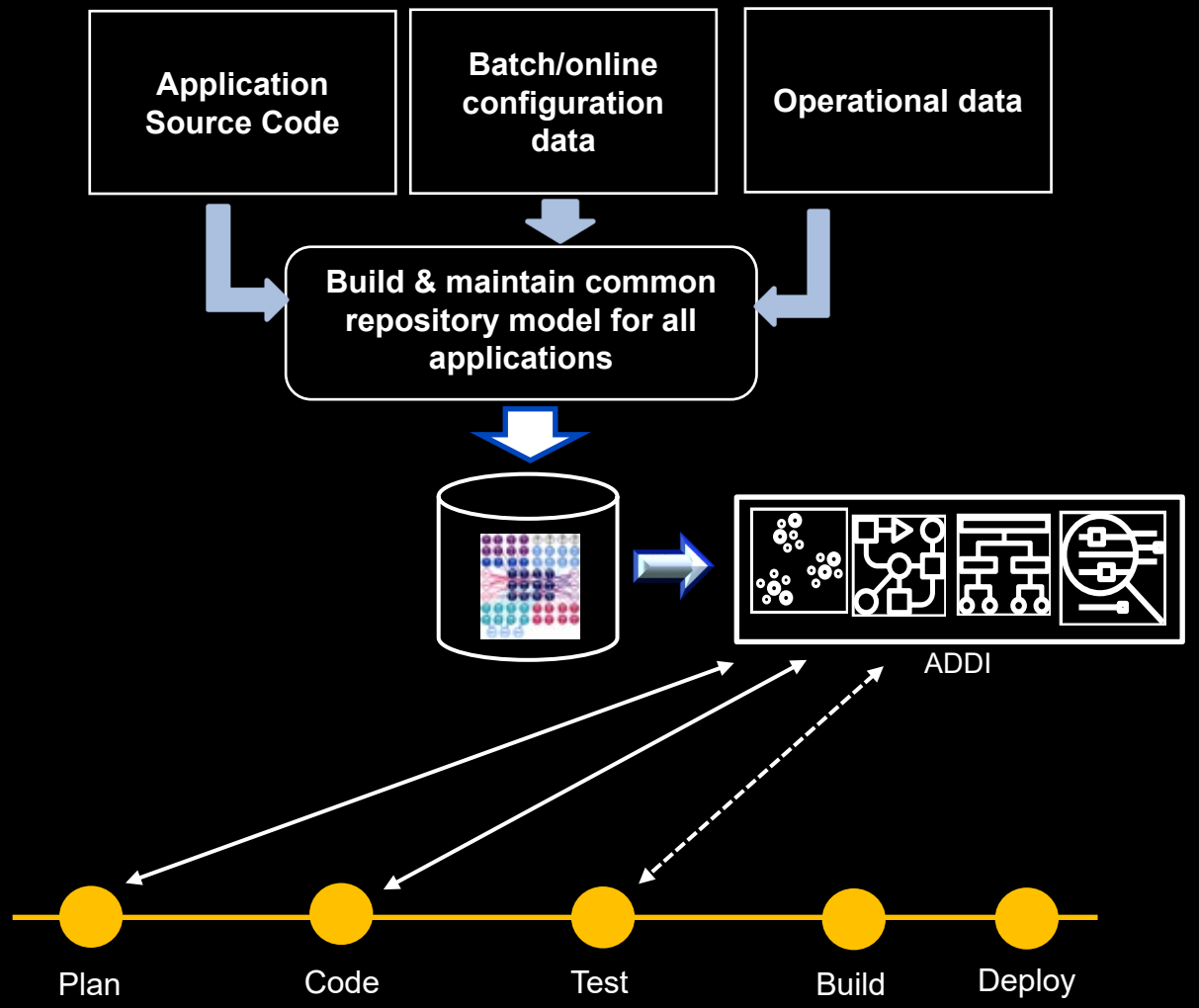
Crypto Analytics Tool

- Provides a cryptographic view with up-to-date monitoring of crypto keys and functions

z/OS Encryption Readiness Technology (zERT)

- Answers the question “Which traffic do I have and how is it protected?” – Identifies Security protocols, Crypto algorithms, Key lengths, etc.

Enable crypto discovery with IBM ADDI



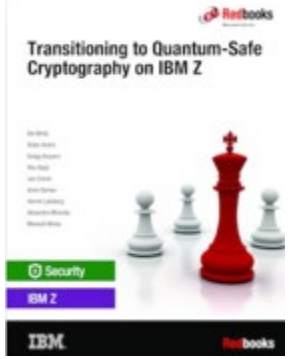
ADDI: Application Discovery and Delivery Intelligence
ICSF: Integrated Cryptographic Service Facility
CI/CD: Continuous Integration / Continuous Delivery
UI: User Interface

Industry migration guidance

IBM Redbook

Transitioning to Quantum-safe Crypto on IBM Z

https://www.redbooks.ibm.com/redpieces/abstracts/sg248525.html



National Cyber Security Centre

Preparing for Quantum-Safe Cryptography

https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

National Cybersecurity Center of Excellence (NCCoE)

Migration to post-quantum cryptography

https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography

Cloud Security Alliance

Practical preparations for the post-quantum world – Tasks every organization should be performing now to prepare

https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

Electronic and Telecommunication Standards Institute (ETSI)

Migration strategies and recommendations to Quantum Safe schemes

https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

Use cases we are not quite ready to tackle ready to tackle…

Communications and Network Security

Communication and Network Protocols and related tech - TLS, SSH, VPN, Certificates, SFTP have not yet been updated by the IETF community.

- NIST PQC standardization process is underway
- Interoperability is a must
- New certificate formats and key serialization methods must be standardized
- Open quantum safe provides testing options
- PQC Activity in IETF Community - https://trac.ietf.org/trac/sec/wiki/PQCAgility

Distributed Ledger Technologies

Including blockchain, Ethereum, etc.

- Technologies use hashing and public key technology
- Signatures created by current PQC candidate algorithms not suitable for some of these use cases. They are too large
- NIST initiating a 4th round for signature algorithms
- The distributed ledger community looking at alternatives

Core Banking

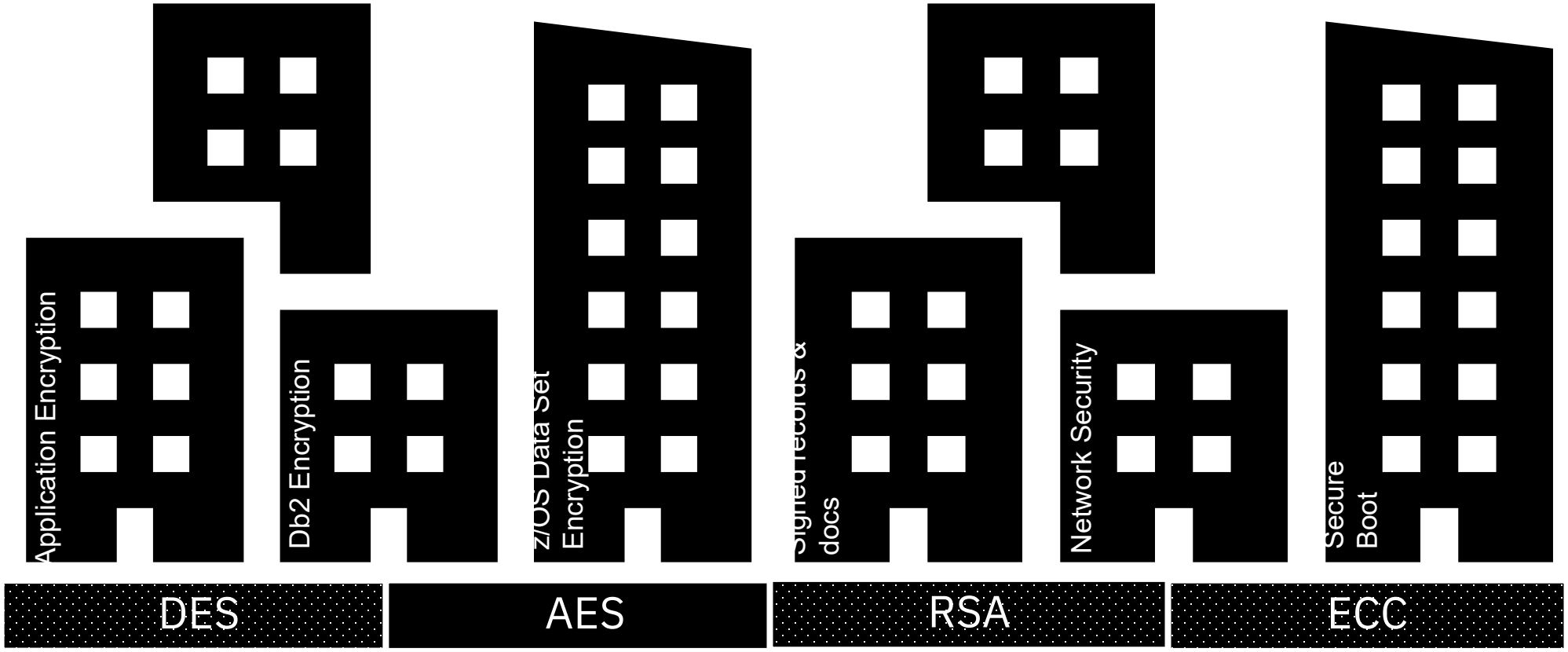
- Heavily using TDES for PIN processing
- PIN block standards already support AES*, industry adoption is slow
- Standards will take time to evolve
- Interoperability outside the institution with partners must be maintained
- Many stakeholders involved (Issuers, acquirers, card brands, networks, chip card vendors, ATM vendors, etc.)

*Note: The Crypto Express supports ISO format 4 PIN blocks which have AES protection

Crypto Skyline

Built on cryptographic primitives for classical computers

Entering the quantum era



- Symmetric keys
- Random numbers
- Up to 168-bit keys

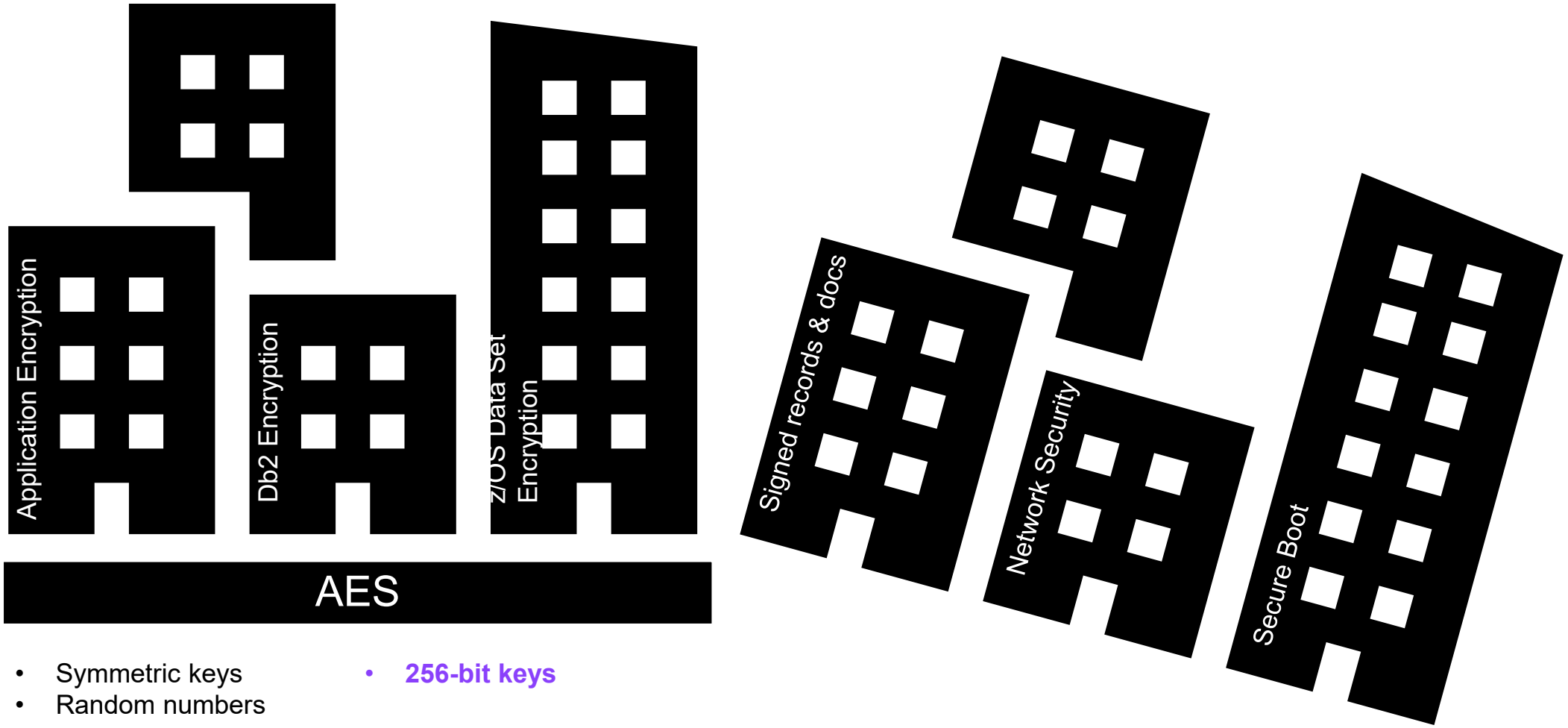
- Symmetric keys
- Random numbers
- Up to 256-bit keys

- Asymmetric key pairs
- Complex math
- 4096-bit keys require more time to generate

- Asymmetric key pairs
- Complex math
- Strongest keys require minimal time to generate

Crypto Skyline

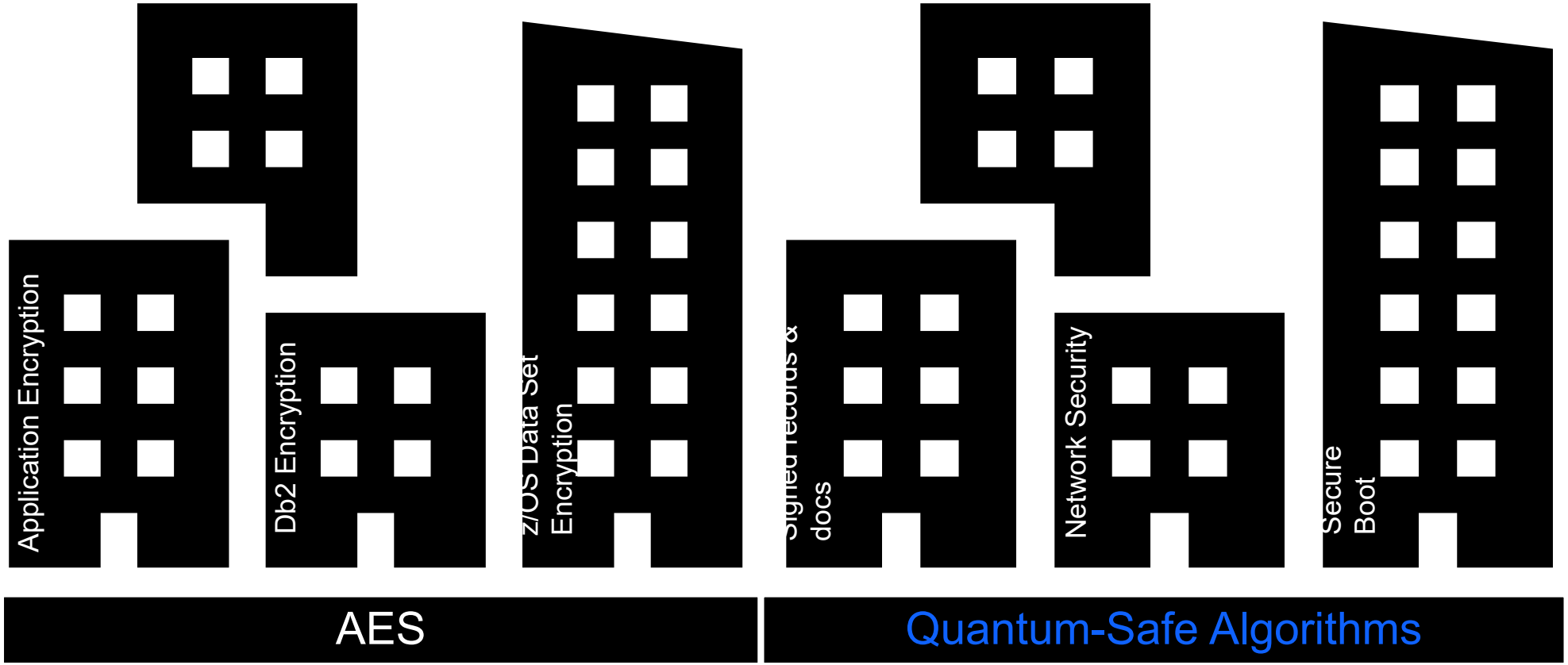
In the quantum era would be in jeopardy



- Symmetric keys
- Random numbers
- **256-bit keys**

Crypto Skyline #goals

Built on cryptographic primitives for classical computers AND quantum computers



- Symmetric keys
- Random numbers
- **256-bit keys**
- Asymmetric key pairs
- Lattice-based cryptography
- CRYSTALS-Dilithium
- CRYSTALS-Kyber

"The threat that quantum computers pose to our modern cryptographic systems is well-known. Even though large-scale quantum computers are not yet here, it is critical to take action well before their arrival. Organizations need to be planning now, for the upcoming transition to new quantum-resistant cryptographic algorithms. Failure to do so may mean that your information will not be protected from these future attacks."

—
Dustin Moody
Mathematician, Post-Quantum Cryptography Project Leader
National Institute of Standards and Technology (NIST)

Mitigation is not dependent on standardization. Actions can be taken today.

- *Data can be protected with strong algorithms like AES today.*
  - *The standardization process affects public key crypto not symmetric key crypto.*
- *Dual Signature Schemes / Hybrid Key Agreement can be used today w/agility in mind.*
  - *Ex. NIST SP 800-56C; https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs*

Summary

Classical Cryptographic Algorithms are widely used to protect data and communications in computer systems and networks.

An adversary with access to a sufficiently strong quantum computer can break the classical algorithms we have used for many years.

Most vulnerable are Asymmetric Algorithms and Protocols.

Risks include theft of digital assets, forged documents, transactions, signatures, code and the like. Secure communications are also in jeopardy.

Researchers and standards bodies are moving to address the threats.

They are identifying new quantum-safe algorithms that can be used to protect classical and quantum computer workloads and data from the attacks that can be launched from quantum computers.

Organizations are providing migration guidance.

IBM is playing a prominent role.

Security innovation driven through platform strategy

April 7th, 1964 – April 5th, 2022
4 Generations of Technology
12 Families of Innovation

IBM z14™

Crypto Express6s
CPACF

IBM z15™

Crypto Express7s
CPACF
Compression

IBM z16™

IBM Telum Processor

Crypto Express8s
CPACF
Compression
Memory Encryption

IBM zSystems & LinuxONE Security Leadership

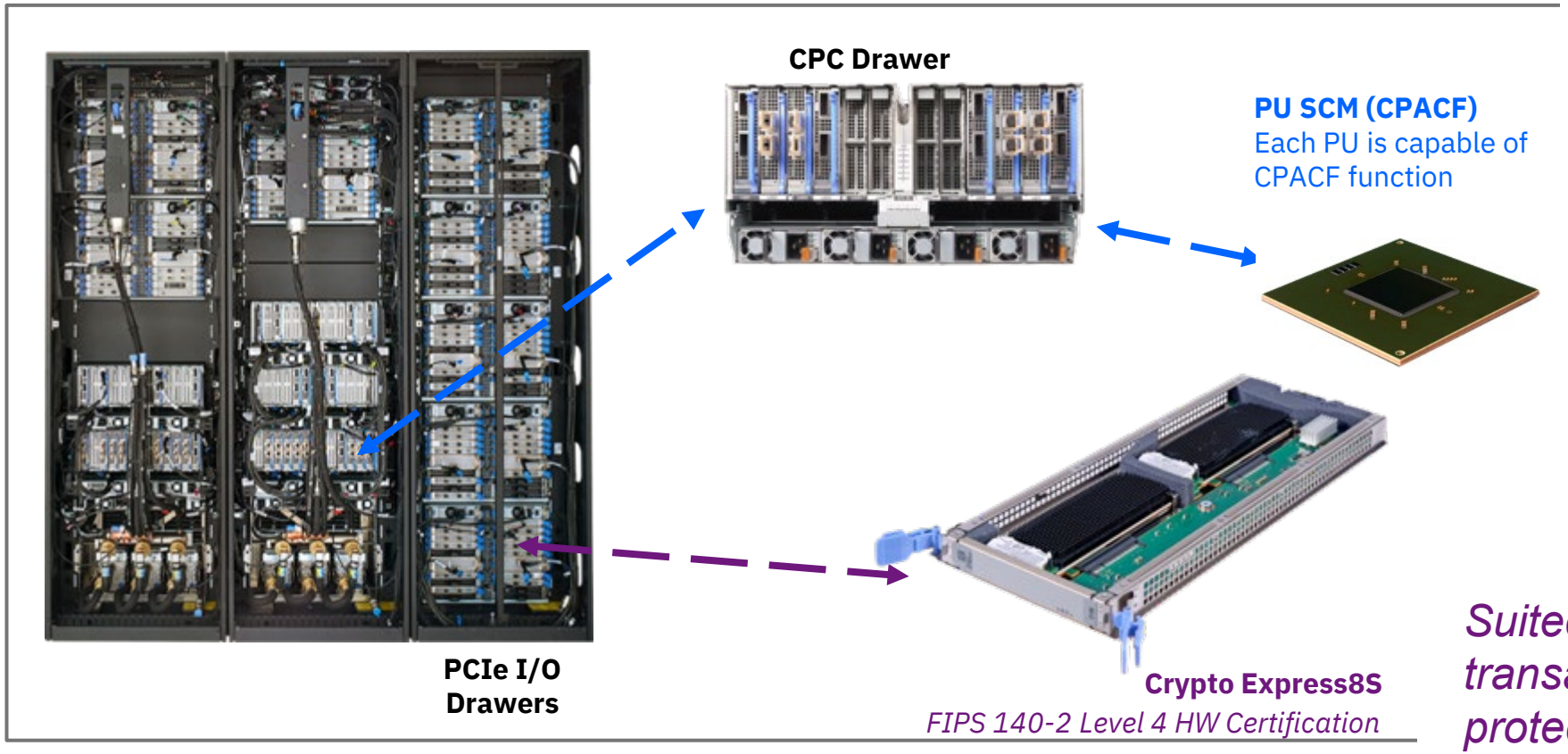
Approach: Security integrated into all levels of the stack

Data Protection

Data Privacy
Confidential Computing

Cyber Resiliency
Continuous Compliance
Quantum Safe
Validated Boot for z/OS

IBM Z and LinuxONE Crypto Hardware

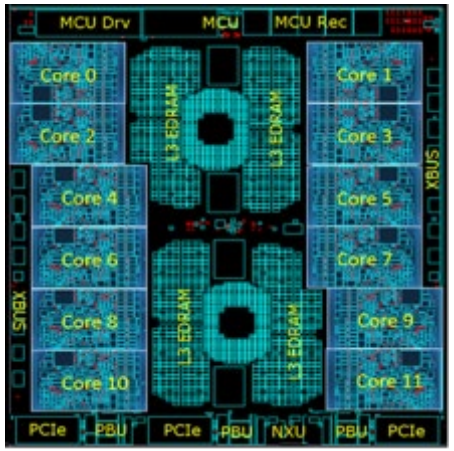


Used for high speed bulk encryption

Up to 14GB/s

Suited for high value transactions, key protection

CPACF
On-Chip Crypto Acceleration



Central Processor Assist for Cryptographic Functions (CPACF) On each processor core

The following algorithms are supported by CPACF:

- AES
- DES/TDES
- SHA-1, SHA-2, SHA-3
- EdDSA (Ed448, Ed25519)
- ECDSA (P-256, P-384, P-521)
- ECDH (P-256, P-384, P521, X25519, X448)

New for z16 – Crypto Counters – Included in SMF30 records

Accelerate your encryption

Hardware accelerated encryption on every microprocessor core

Protected Keys - Key values are never exposed to the OS, hypervisor, or application

Suited for high speed bulk symmetric encryption

Why on-chip encryption?

More performance = lower latency and less CPU overhead for encryption operations

No-charge feature enabled on all LinuxONE systems

z16 Crypto Express8S
Hardware Security Module (HSM)

Built for the future of cyber resiliency

Over 300+ APIs with new algorithms such as:
ed448, ec25519, SHA3, SHA3 XOF modes, FPE

IBM z16 with the Crypto Express8S can help you protect today's data from "harvest now, decrypt later" quantum attacks.

Built using the 4770-001 Hardware Security Module, it has been designed to meet the needs of the most regulated industries.

- Module and its PKCS11 Firmware have been FIPS 140-2 Level 4 tested and currently part of the Modules in process list in the NIST website:
  https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List

Firmware and secure boot load process are secured using FIPS validated plus quantum-safe algorithms

Acceleration for Quantum Safe Crypto

Security innovation driven through platform strategy

April 7th, 1964 – April 5th, 2022
4 Generations of Technology
12 Families of Innovation

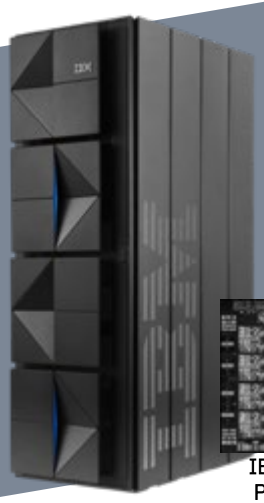
IBM z14™

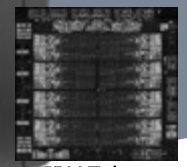
Crypto Express6s
CPACF

IBM z15™

Crypto Express7s
CPACF
Compression

IBM z16™





IBM Telum Processor

Crypto Express8s
CPACF
Compression
Memory Encryption

IBM zSystems & LinuxONE Security Leadership

Approach: Security integrated into all levels of the stack

Data Protection

Data Privacy
Confidential Computing

Cyber Resiliency
Continuous Compliance
Quantum Safe
Validated Boot for z/OS

Validated Boot

What is Validated Boot?

- Use digital signatures to provide an IPL-time check that IPL data (ie. executables residing on an IPL volume) is intact, un-tampered-with, and originates from a trusted source
- Enable detection of unauthorized changes to software executables

What value does it provide?

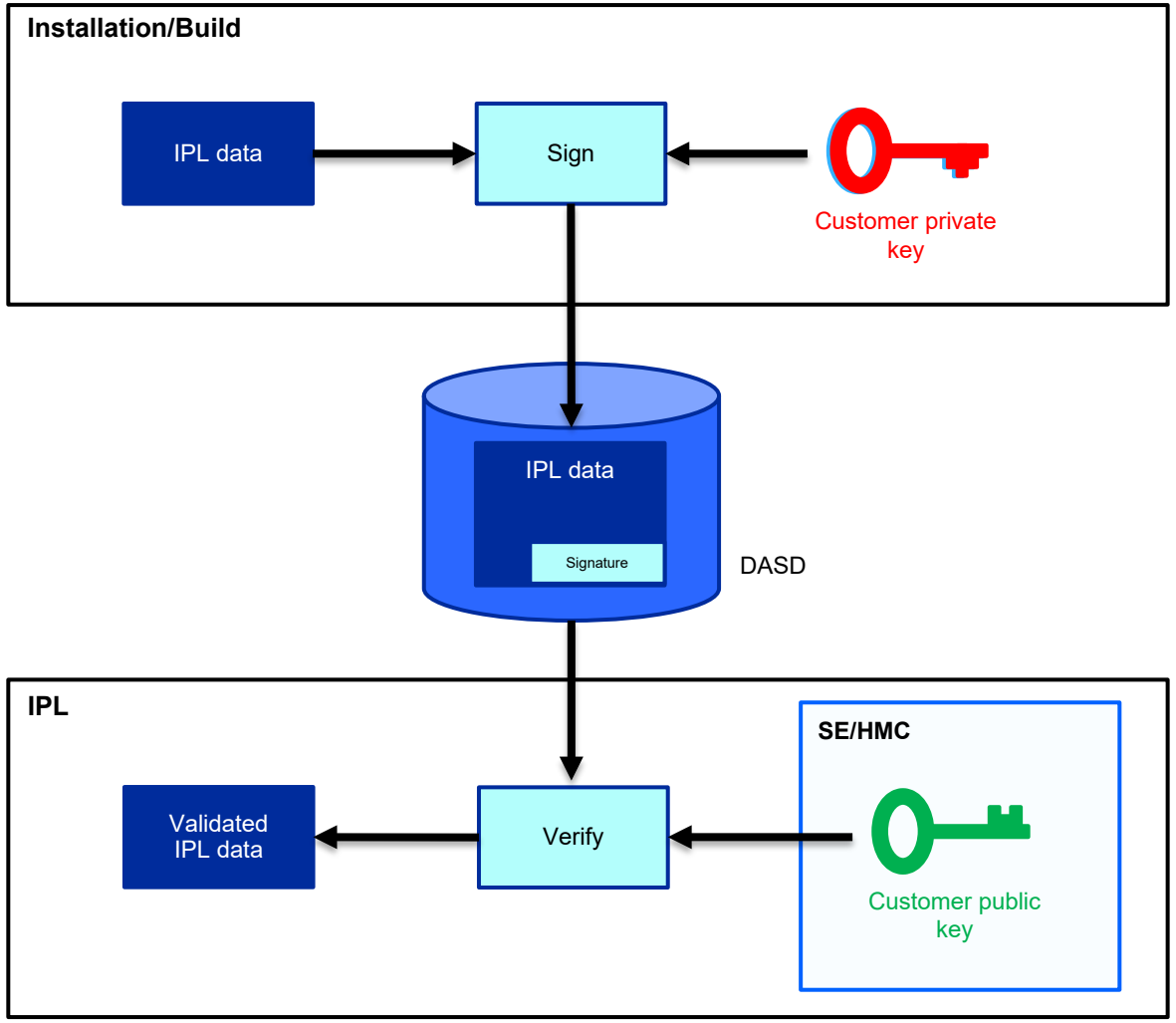
- Ability to meet regulatory compliance required for certain secure software deployment scenarios - designed to meet ***NIAP OS Protection Profile 4.2.1*** Certification
- Early detection of *accidental* IPL data changes can reduce impact of outages
- Detection of *malicious* IPL data changes can stop certain types of attacks

Note:

– "Validated Boot" = "Secure Boot" = "Boot Integrity Validation"

– "Boot" = "IPL" **(NOT IML)**

– Note that Validated Boot is NOT the same thing as "Secure Execution"



Technology Outlook for IBM Z

Drive innovation to remain the most securable, most reliable, most scalable transaction processing and data serving platform

2017 → 2030

IBM z14

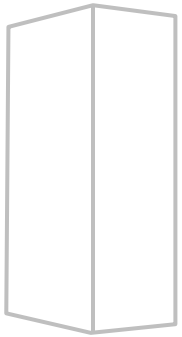
- 14nm
- Accelerated Encryption
- Virtual Flash Memory
- High-Speed Synch I/O
- Secure Service Containers

IBM z15

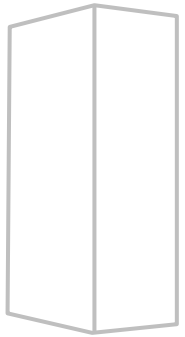
- 14nm
- Accelerated Compression
- Accelerated Sort
- Secure Execution
- System Recovery Boost

IBM z16

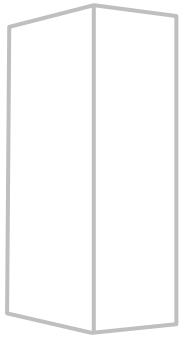
- 7nm
- Accelerated AI
- Quantum Safe System
- Secure Boot
- Memory Encryption
- Flexible Capacity for Cyber Resiliency



IBM zNext



IBM zNext +1



IBM zNext +2

5nm → 2nm

Continuous Compliance

Foundation AI

AI for Security

Accelerated I/O

Enhanced Workload Isolation

Fully Homomorphic Encryption

Quantum Integration


IBM

Important Links

IBM Z SCC Webpage: https://www.ibm.com/products/z-security-and-compliance-center

Solution Brief : https://www.ibm.com/downloads/cas/8NJA2R9P

IBM Z SCC Documentation (Guide): https://www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm

IBM Z SCC Docs: https://www.ibm.com/docs/en/zscc/1.1.0

CIS Benchmarks: https://www.cisecurity.org/benchmark/ibm_z

IBM Z and LinuxONE Services
Quick Reference Guide

Quantum-Safe Assessment for IBM Z

Overview

The today digital trust relies on encryption. Therefore, it is important to ensure at first that encryption is secured and match with standards.

While quantum computing aims to solve complex problems even the world's most powerful supercomputers cannot solve, future fault-tolerant quantum computers could pose potential risks, such as the ability to quickly break encryption algorithms and access sensitive data.

Therefore, it is important from an inventory to build a quantum safe harbor in order to be ready when the time will come.

Without quantum-safe cryptography and security, almost everything that ever has been – or will be – sent over a network is vulnerable to attack.

Based on a technical study, SMEs will explore encryption quality to further improve the IBM Z encryption as today and tomorrow needs mandate.

IBM Lab Services

Target Audience

IBM Z customer interested in learning more about their IBM Z encryption quality regarding compliance and today standard.

The assessment is designed for client willing to know from an inventory their exposition to the Quantum Computing threats and how to build a quantum safe strategy for their IBM Z.

Why Use This Service?

Leverage the knowledge of proven experts who work with IBM Z Security and encryption projects.

Partner / assist you with the latest IBM Z encryption technologies adoption including the latest Post Quantum Cryptography features.

Benefits

Gain understanding of encryption areas that may represent potential exposures according to today ant tomorrow threats.

To be advised on how to fix, update and to remediate according to findings.

Service Provided

A data collection to take place in order to evaluate encryption quality and vulnerabilities:

- Cryptosystems
- Security protocols
- Products, Logical, Services

Interviews to go beyond technical facts, and to assess the encryption strategy:

- Governance, encryption guidelines
- Encryption control, monitoring

(Optional) IBM Application Discovery and Delivery Intelligence (ADDI) with Crypto Discover can be deployed -- *trial is possible.*

Engagement Schedule and Duration

Standard technical study is generally delivered with-in 2 weeks after validation of the data collection quality.

An extra week is required if ADDI with Crypto must be deployed for the first time.

Final workshop generally last ½ day.

Deliverables

Summary report with findings and recommendations.

Discovery of where and what crypto is used by applications

Recommended next steps to strengthen IBM Z encryption capabilities to match with today and tomorrow objectives.

Scenarios and roadmap to build step by step an IBM Z quantum safe harbor.

Contacts

To get more information and schedule a workshop contact Lab Services:

ibmsls@us.ibm.com

Lab Services Principal Consultants

Guillaume Hoareau

Guillaume_hoareau@fr.ibm.com

What makes the IBM compliance solution better?

Customizable Compliance Frameworks

Profiles built specifically for regulatory requirements like PCI DSS. Take advantage of profiles out of the box or customize to meet your needs with custom profiles & validation threshold changes. Configurable frequencies for scans. Allowing the management of various audit and regulatory frameworks

Keep Data on Platform

Keeping data on IBM Z, is a key requirements for many existing customers. This keeps data safe and secure with all the RASS benefits that exist on IBM Z today.

Identify compliance misconfigurations in near real time

Discover sysplexes where compliant relevant data can be stored, automatically. With the option of selecting all or some of the underlying systems.

PCI DSS Coverage

Different compliance products accommodate different regulatory controls. Some don't offer PCI DSS which is highly sought after.

Native Evidence Writing

Middleware components are creating records directly from their configurations through signed SMF data. Limiting the opportunity for tampering or discrepancies.

Help with changing regulations

Remove some of the burden of interpreting new and changing regulations as IBM has worked with SMEs and Auditors to make regulatory interpretations relevant to IBM Z and repeatable

Compliance on IBM Z and LinuxONE

Dashboard

Assess

Scans

Configure

Scopes

Profiles

Goals

Settings

PCI Review

PCI _DSS_SCOPE | PCI _DSS 3.2.1 | Validation

Details

Mar 16, 2022 1:10 PM

Feb 16, 202 1:10 AM

Jan 16, 202 1:10 AM

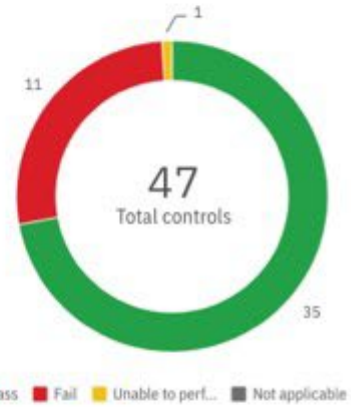
Dec 16, 202 1:10 AM

March 16, 2022 1:10 PM

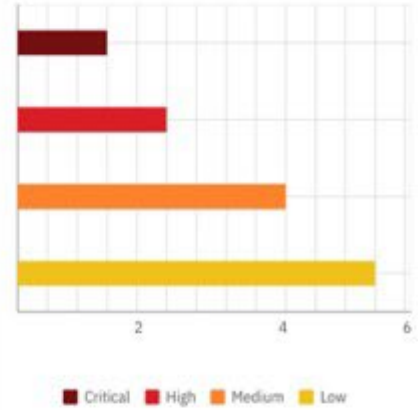
35 11 1 0

Download report

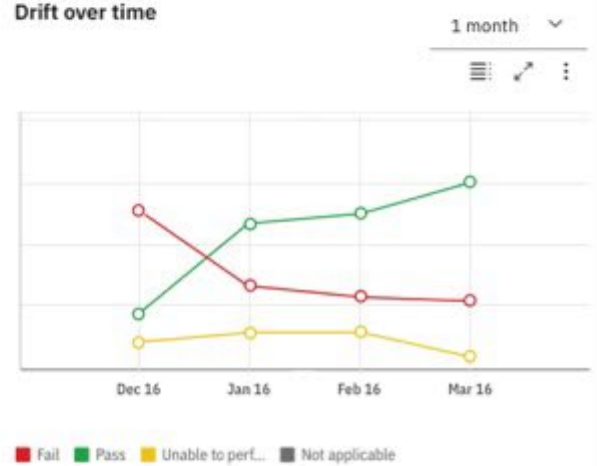
Controls



Failures



Drift over time



Control view | Resource view

Status Filter... | Severity Filter... | Search

Status	ID	Control	Severity	Resource details
⊘	1.1	Ensure the Appropriate Version/Patches for Oracle Software Is Installed	Critical	0 1 0 0
⊘	2.1.1	Ensure 'extproc' Is Not Present in listener config	Medium	0 1 0 0
!	2.1.2	Ensure 'ADMIN_RESTRICTIONS' is set to 'ON'	-	0 0 1 0
✓	2.2.1	Ensure 'AUDIT_SYS_OPERATIONS' Is Set to 'TRUE'	-	1 0 0 0

IBM Quantum Safe: Use Cases and Examples

Core Area of Cryptographic	Example Use Case	Example Use Case Details	Example Technology
Data Encryption	Database Encryption (data at rest)	Symmetric encryption algorithms (e.g., AES) are used to encrypt the database (tablespace, row, or column)	DB2 Native Encryption
	Symmetric Key Management	Symmetric encryption algorithms (e.g., AES) are used to encrypt the data encryption keys use in applications or databases	Enterprise Key Management Facility
	Disk Encryption (data at rest)	Symmetric encryption algorithms (e.g., AES) are used to encrypt the full disk	IBM DS8000
	Data in-transit Encryption (TLS)	A combination of asymmetric encryption (e.g., RSA) and symmetric encryption to encrypt communication (e.g., web traffic)	TLS
Digital Signature	E-mail Signing	An asymmetric encryption algorithm (e.g., RSA) is used to sign email in order to ensure integrity of the email content and non-repudiation w.r.t. the sender	Outlook
	Legal Document Signing	An asymmetric encryption algorithm (e.g., RSA) is used to sign a contract in order to ensure authenticity	DocuSign
	Transaction Signing	An asymmetric encryption algorithm (e.g., RSA) is used to sign a transaction/payment in order to ensure authenticity	Bitcoin/Payment/E-commerce systems

IBM Quantum Safe: Use Cases and Examples (cont.)

Core Area of Cryptographic	Example Use Case	Example Use Case Details	Example Technology
Authentication	Server Authentication	An asymmetric encryption algorithm (e.g., RSA) is used to verify the signature of a CA on the digital certificate presented to the client	TLS
	Client Authentication	An asymmetric encryption algorithm (e.g., RSA) is used to verify the signature of a CA on the digital certificate presented to the server	TLS
	Virtual Private Network (VPN)	A virtual private (encrypted) network for host-to-remote or site-to-site connections leveraging a combination of asymmetric and symmetric encryption algorithms ensuring confidentiality, integrity, authentication	SSL/TLS VPN, IPSec VPN
	User Authentication	An asymmetric encryption algorithm (e.g., RSA) is used to decrypt a challenge posed by the server to the client	SSH
Key Exchange / Network Security	Database Client/Server Handshake	An asymmetric encryption algorithm (e.g., DH) is used to agree on a symmetric encryption key between the database client and server	DB2
	TLS Client/Server Handshake	An asymmetric encryption algorithm (e.g., RSA) is used to agree on a symmetric encryption key between the TLS client and server	TLS
	SSH Client/Server Handshake	An asymmetric encryption algorithm (e.g., RSA) is used to agree on a symmetric encryption key between the TLS client and server	SSH

Secure Boot for Linux on IBM z16

- Initially introduced on IBM z15 and IBM® LinuxONE III platforms
- Operating system loader verifies that components loaded from ***SCSI disks or NVMe*** devices come from a trusted source
- With Secure Boot enabled, an IPL fails if a component containing code is not signed or cannot be verified
- Can be implemented with RHEL, Ubuntu, or SLES distributions

60

- With IBM z16 and IBM® LinuxONE Emperor 4 family, Linux® users will now be able to utilize Secure Boot from ***ECKD*** as well as from SCSI or NVMe
- Utilizes some building blocks similar to Validated Boot for z/OS®