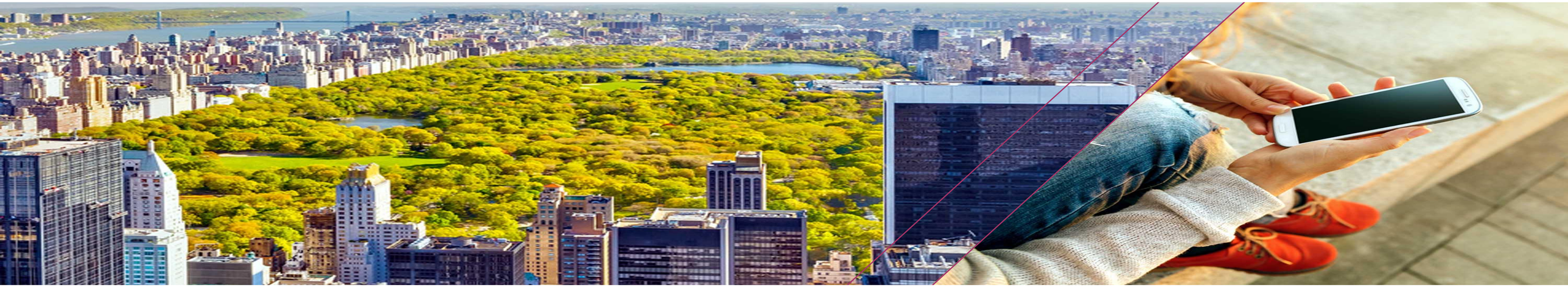
Quantum-Safe on IBM Z: Future proofing security in the Quantum era



Gregg Arquero

IBM Senior Software engineer - z/OS Security
gmarquer@us.ibm.com

Quantum Safe in the News

THE BIG STORY

The Quantum Apocalypse Is Coming. Be Very Afraid

What happens when quantum computers can finally crack encryption and break into the world's best-kept secrets? It's called Q-Day—the worst holiday maybe ever.

AMIT KATWALA

MAR 24, 2025 6:00 AM

"Quantum-Safe" Crypto Hacked by 10-Year-Old PC

Many challenges still lie ahead for postquantum cryptography

BY CHARLES Q. CHOI | 19 AUG 2022 | 7 MIN READ |

Charles Q. Choi is a contributing editor for IEEE Spectrum.

Chinese Researchers Tap Quantum to Break Encryption

But the time when quantum computers pose a tangible threat to modern encryption is likely still several years away.

The Next Big Cyber Threat Could Come from Quantum Computers... Is the Government Ready?

Posted on January 22, 2025

UK urges critical orgs to adopt quantum cryptography by 2035

By Bill Toulas — March 20, 2025 — 12:23 PM — 0

The UK's National Cyber Security Centre (NCSC) has published specific timelines on migrating to post-quantum cryptography (PQC), dictating that critical organizations should complete migration by 2035.

The new guidance aims to provide a structured migration plan with specified milestones for all organizations to follow. It will also serve to highlight the real security risks of falling behind.

"Quantum computing is set to revolutionize technology, but it also poses significant risks to current encryption methods," stated NCSC's CTO, Ollie Whitehouse.

count—
erging
could also be
e like

ederal strategy

Related Posts

Preparing for the Quantum Threat: The Urgent Need for Next-Generation Cryptography

As quantum computing advances, organizations must adopt future-proof security strategies to safeguard data against emerging threats

Thomas Lintemuth, Distinguished VP analyst, Gartner
March 19, 2025

4 Min Read **Quantum Latest News**

Computing

China achieves quantum supremacy claim with new chip 1 quadrillion times faster than the most powerful supercomputers

News By Alan Bradley published March 13, 2025

This new superconducting prototype quantum processor achieved benchmarking results to rival Google's new Willow QPU.

Quantum computing is coming for your cryptography, warns NCSC

No need to panic just yet, but plans to move to quantum-safe alternatives should be in place by 2028 at the latest

John Leonard
20 March 2025 • 3 min read

News • January 14, 2025 • 4 min read

2025: The year to become Quantum-Ready

by Mitra Azizirad, President and Chief Operating Officer of Strategic Missions and Technologies @ Microsoft

Source: IBM Consulting Cybersecurity Services Quantum Safe

We are entering a new cryptographic era!

- *Quantum Advantage: a computation performed more efficiently, cost-effectively, or accurately using quantum devices than classical computers alone*

- Quantum Researching are moving steadily towards Quantum Advantage

- Unlocks Innovation

- Solves previously unsolvable problems

- Opens new attack vectors for adversaries

- Breaks the cryptographic protections we have relied on for may years

Quantum Data Center of the Future
Poughkeepsie, NY

2029: Starling – 200 Logical Qubits
2033+:Blue Jay – 2000 Logical Qubits

The Problem

1. Symmetric key and hashing algorithms:

Impacted by quantum computing – algorithm strengths are reduced. As of today, there are no KNOWN vulnerabilities

Example Mitigations:

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

2. 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	***Already insecure***
AES	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 is at risk?

Internet Protocols

SSL/TLS or Wi-Fi encryption, Hyper-text Transfer Protocol (HTTP), SFTP, etc.

Critical Infrastructure

Car components & systems, electric grids, pipelines, etc.

Cryptocurrency

Bitcoin, coin wallets, transactions

Digital Identities

Signed software, Advanced Electronic Signatures (AES), etc.

Economic Systems

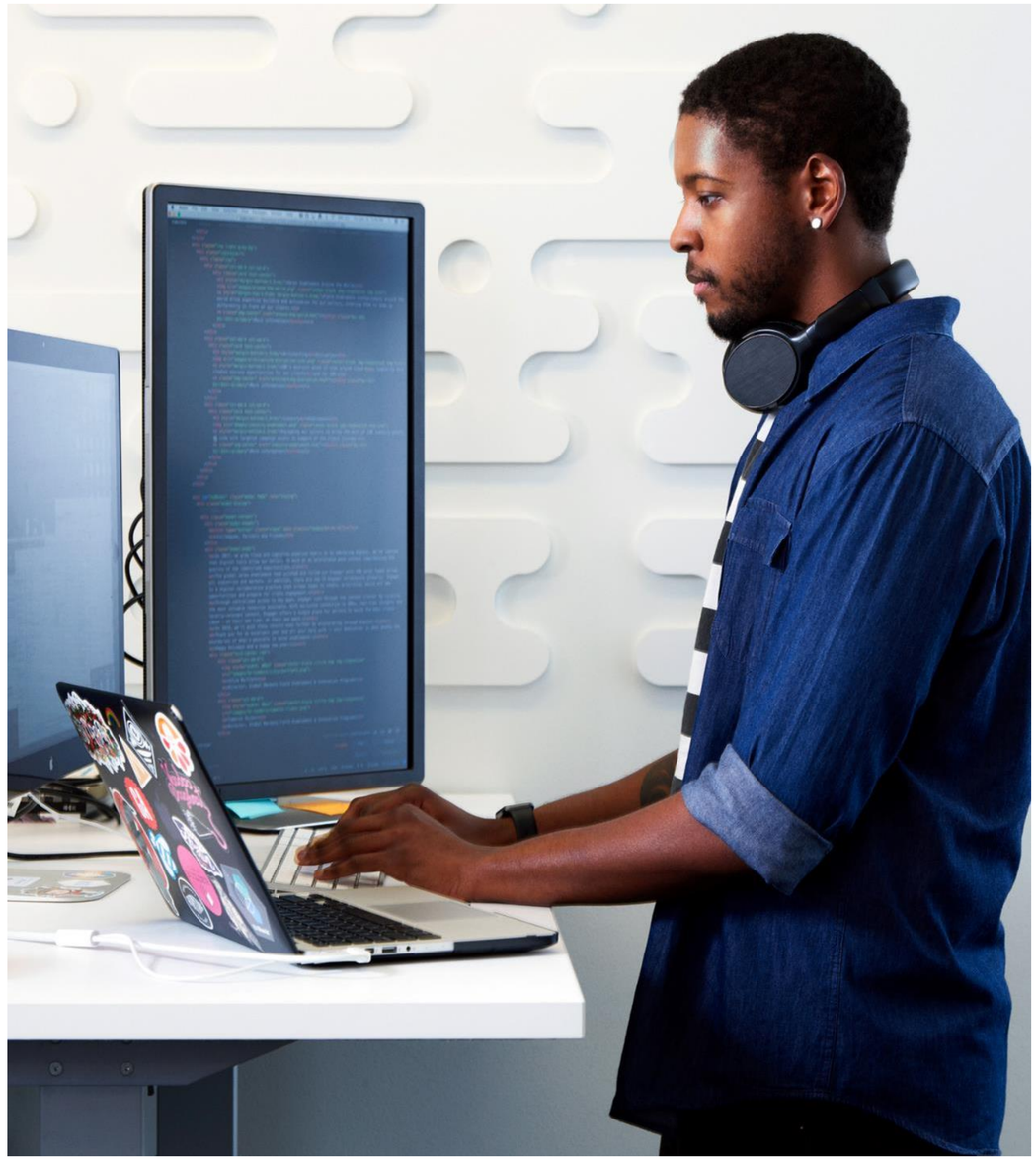
Payment card and banking transactions, payment systems, etc.

National Security

Key management, sensitive communications, intelligence data, etc.

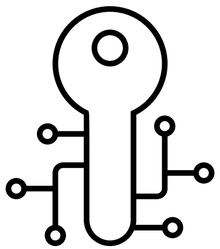
Quantum-Safe Cryptography

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.

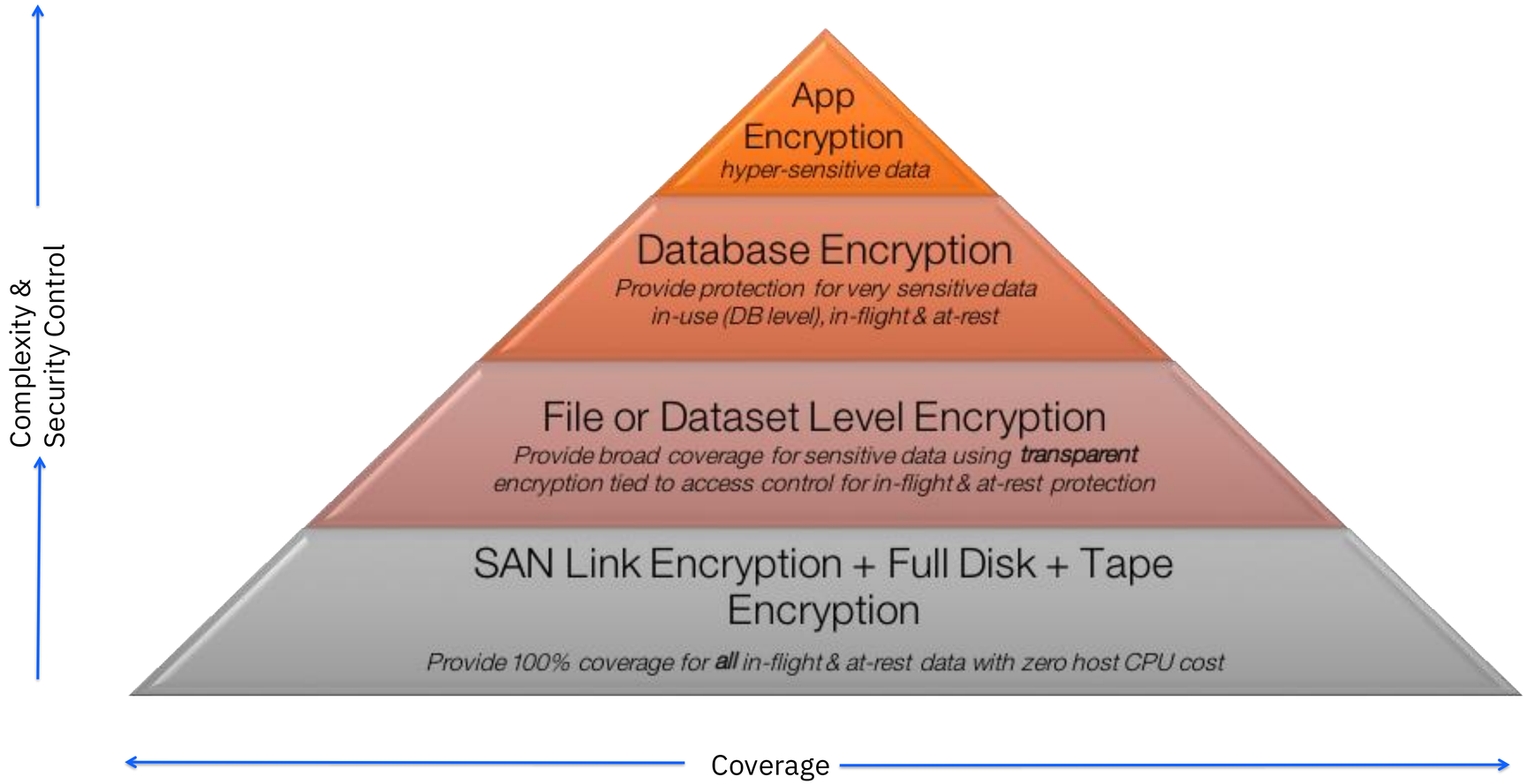


Source: https://www.etsi.org/technologies/quantum-safe-cryptography

Symmetric Cryptography

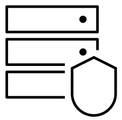
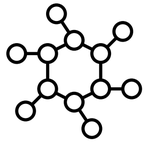
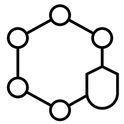
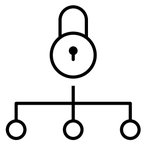


Defense in depth



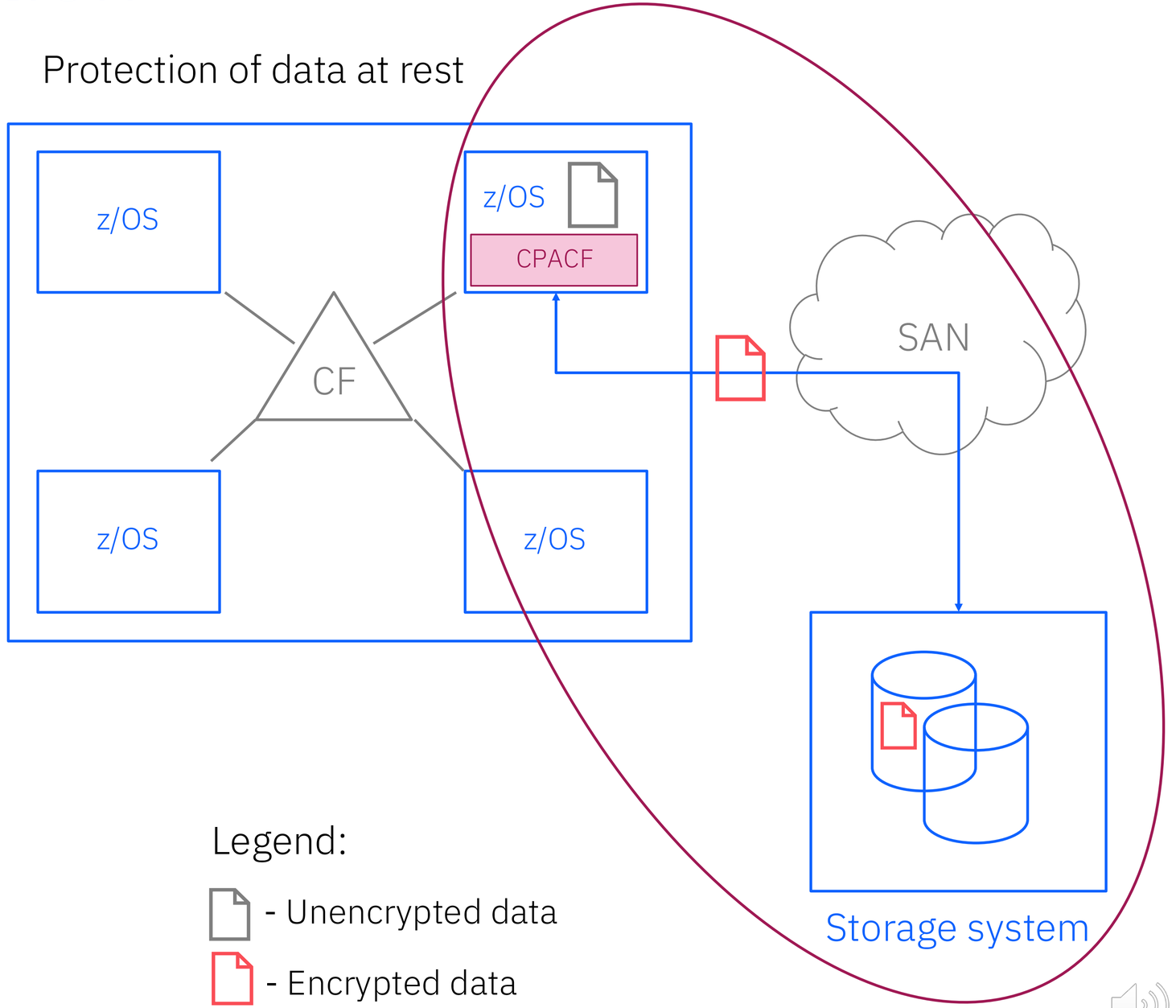
IBM Z Pervasive Encryption

Enabled through full-stack platform integration

Integrated Crypto Hardware		Hardware accelerated encryption on every core – CPACF performance improvements of up to 7x Next Gen Crypto Express8S – up to 2x faster than prior generation
Data at Rest		Broadly protect Linux volumes 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
Hyper Protect Virtual Servers		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 Unified Key Orchestrator for z/OS (UKO for z/OS) provides real-time, centralized secure management of keys and certificates with a variety of cryptographic devices and key stores

z/OS Data Set Encryption

- Application transparent & enabled by policy
- Host encryption via CPACF as data is written to or read from disk
- Supports Seq ext fmt, VSAM ext fmt, PDSE, JES2 spool, Db2, CICS, & IMS
- Includes HSM & DSS migration and backup of encrypted data sets
- Replicated data remains encrypted



z/OS Data Set Encryption Enhancements

Available Function

Data Set Type	Availability	Description
VSAM extended format data set encryption	3Q 2017	• Support VSAM (KSDS, ESDS, RRDS, VRRDS, LDS) extended format • Support transparent VSAM and VSAM/RLS access • KSDS may be compressed format
Sequential extended format data set encryption	3Q 2017	• Support sequential extended format • Support transparent BSAM/QSAM access • May be compressed format (Generic, Tailored, zEDC)
zFS encryption	3Q 2017	• Support for zFS file system data as encrypted and compressed.
PDSE encryption	3Q 2019	• Support data PDSEs (data members only) • Support transparent BSAM/QSAM/BPAM access • Data pages and directory pages are encrypted • Must be SMS-managed • New resource in FACILITY class to allow support
JES2 spool	2Q 2020	• Support the encryption of instream and SYSOUT data sets on SPOOL
Basic and Large format sequential data set encryption	4Q 2020	• Support DASD data sets that cannot be extended format • Support transparent BSAM/QSAM access • Support EXCP access, requiring changes to application. New API for EXCP callers. • Must be SMS-managed • New resource in FACILITY class to allow support

z/OS Data Set Encryption Enhancements

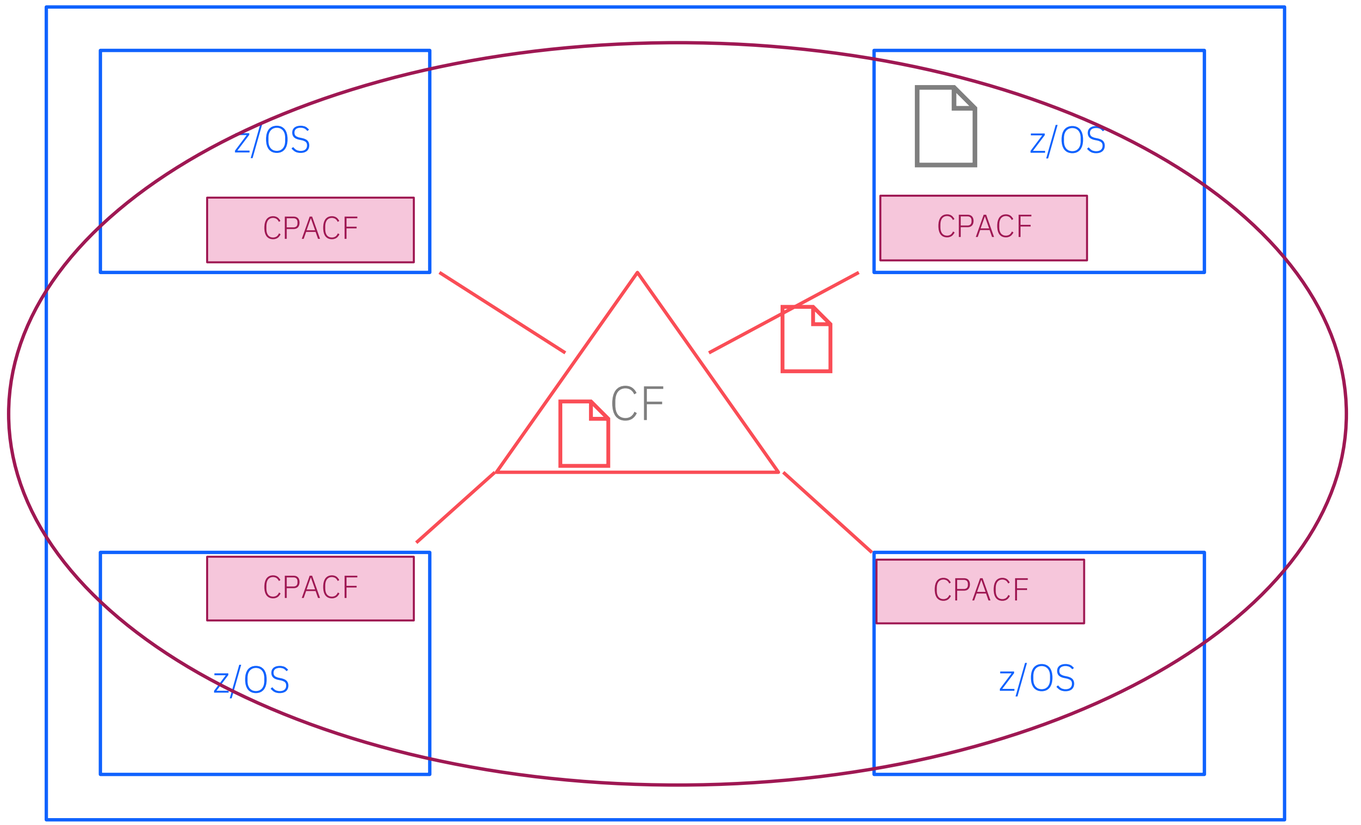
Available Function (Continue)

Supported Data Set Types / Functions	Availability	Description
PDSE zEDC compression	3Q 2021 [V2.5 w/ rollback to V2.3, V2.4]	• Allow encrypted PDSEs to be compressed by access methods
ICSF Archived Key	3Q 2021 [V2.5]	• Support archived keys designated as decrypt only • Supported for VSAM and sequential extended format, PDSE, Basic and large format
RACF DB Encryption	2Q 2022 [V2.5]	• Support for Encrypted VSAM DB in RACF
ICSF AES CIPHER Key panels	3Q 2023 [3.1 only]	• Allows simplified generation of new AES CIPHER keys for use in Data Set Encryption
Tape Data Set Encryption	TBA (Announced via SOD June 2022)	• Support for encryption within the access methods for tape data sets. This support is independent of any encryption that occurs in the tape subsystem.

Coupling Facility Encryption

- Host encryption via CPACF as data is written to or read from disk
- Data encrypted in the host and remains encrypted until decrypted by the host
- List & Cache structures only
- No application enablement required

Protection of data in-flight and in-use



z/OS Parallel Sysplex cluster

Legend:

- Unencrypted data

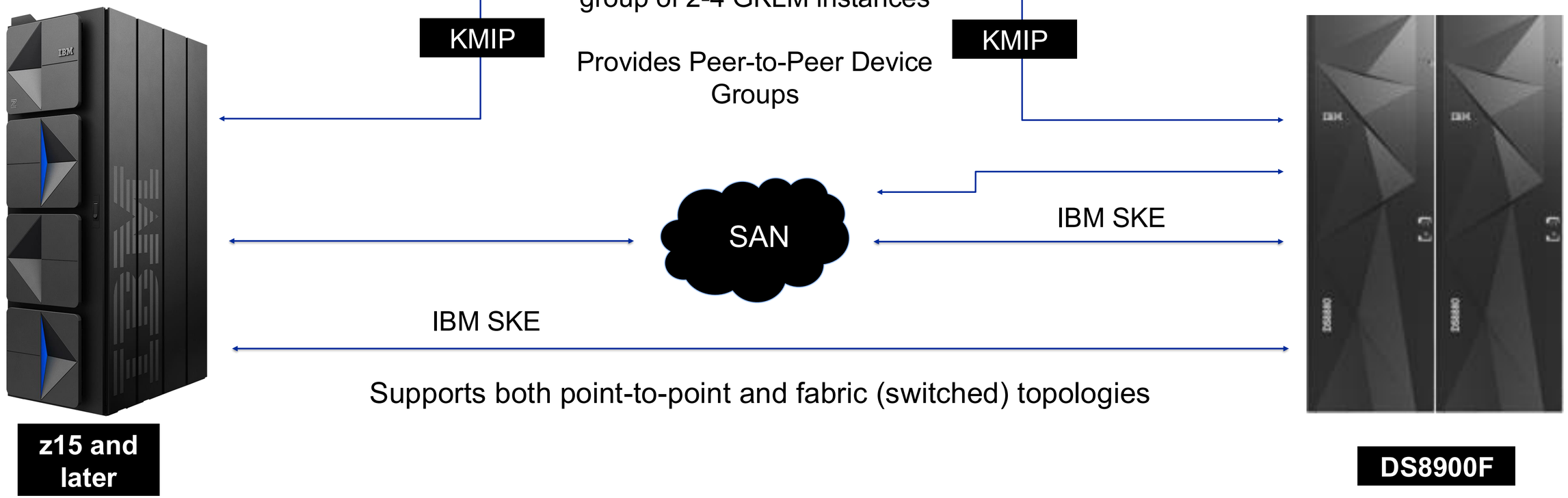
- Encrypted data

Fibre Channel Endpoint Security Components

KMIP = Key Management Interface Protocol
IBM SKE = IBM Security Key Exchange
GLKM = IBM Guardium Key Lifecycle Manager
SAN = Storage Area Network

Communication with External Key Manager on both Z and storage provided through network connection from Hardware Management Console (HMC)

CPACF and FC1146 are required



Statement Of Direction – AD24-0457

Published: 23 April 2024

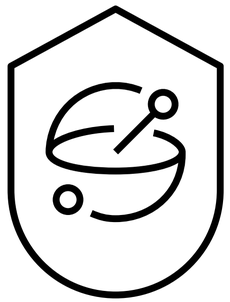
Link: https://www.ibm.com/docs/en/announcements/z-linuxone-2q-2024-statement-direction

Why: ”As many IBM Z® clients run the most mission critical applications, operate in highly regulated industries, and have an increasing amount of sensitive data, IBM must provide tools for securing client data and have a strong technology roadmap to continue to do so.”

What: ”IBM Fibre Channel Endpoint Security (IFCES) is an end-to-end solution that is designed to provide a means to help ensure the integrity and confidentiality of all data flowing on Fibre Channel links between authorized server and storage devices, creating a trusted storage network that encrypts data in flight.”

How: ”all new FICON-connected storage systems introduced after December 31, 2024, will be required to support IFCES to connect to z17+1”

Asymmetric Cryptography



1st Set of PQC Standards

- The fourth standard based on FALCON (FIPS 206) is planned for late 2026.

FIPS 203 – ML-KEM

- Module-Lattice-Based Key-Encapsulation Mechanism Standard
- A key encapsulation standard
- Formerly known as CRYSTALS-Kyber

FIPS 204 – ML-DSA

- Module-Lattice-Based Digital Signature Standard
- A digital signature standard for authentication
- Formerly known as CRYSTALS-Dilithium

FIPS 205 – SLH-DSA

- Stateless Hash-Based Digital Signature Standard
- A digital signature standard for authentication
- Formerly known as SPHINCS+

NIST 4th Round of KEMs Update

- 4th round evaluated to increase diversity of key-establishment algorithms.
- Candidate Algorithms (Round 4)
  - BIKE (Code-based)
  - Classic McEliece (Code-based)
  - HQC (Hamming Quasi-Cyclic)
- Outcome: HQC selected as new standardized KEM to complement ML-KEM

- Why HQC?
  - Based on well-studied Quasi-Cyclic Syndrome Decoding (QCSD) problem
  - No known trapdoors; transparent and formally analyzable
  - Offers lower decryption failure rates compared to BIKE, enhancing IND-CCA2 security
- Roadmap
  - NIST draft within ~1 year
  - Final Publication ~2027

Source: NIST IR 8545

2nd Round of Additional Signature Candidates

14 signature algorithms have advanced to the second round of evaluation (down from 40):

Multivariate-based
- UOV (Unbalanced Oil and Vinegar)
- QR-UOV (Quadratic Residue UOV)
- MAYO
- MQOM
- Mirath (MIRA/MiRitH merger)

Isogeny-based
- SQIsign (Supersingular Isogenies)
- LPERK

Lattice-based
- HAWK
- LESS
- RYDE

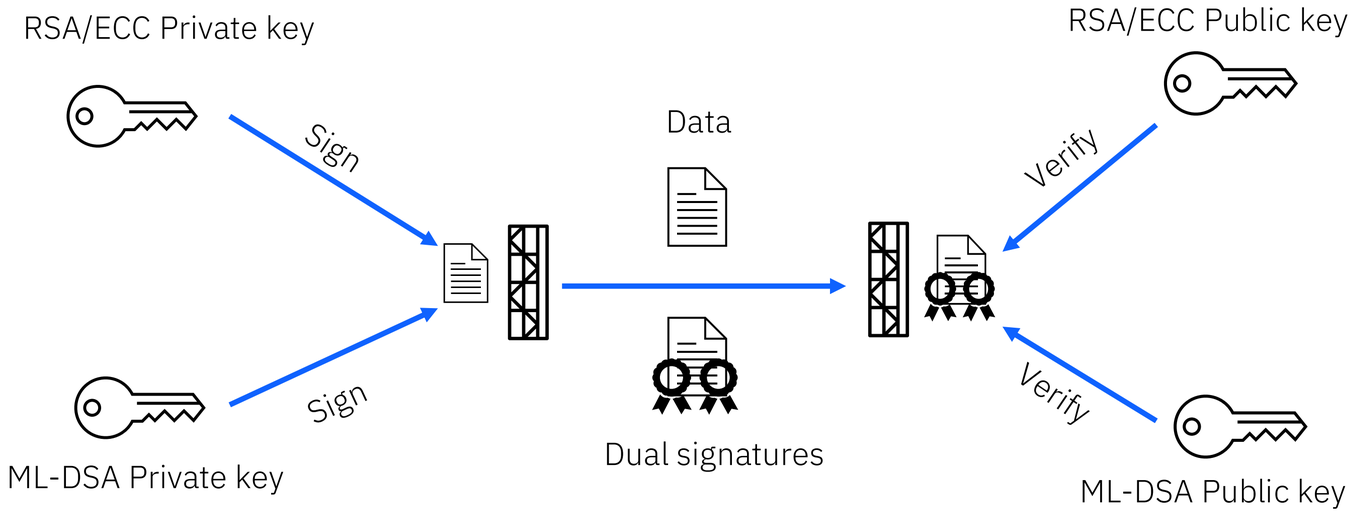
Hash-based
- SDitH
- SNOVA

Other / Hybrid Approaches
- CROSS
- FAEST
- PERK

Source : NIST

ML-DSA support

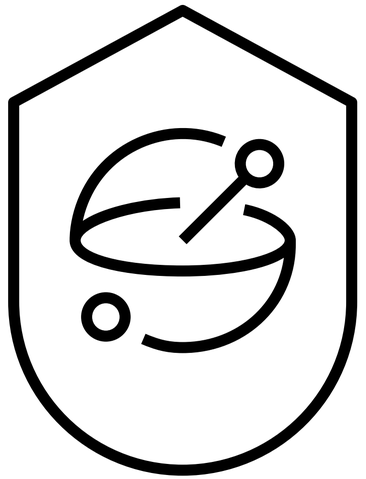
- ML-DSA is a Quantum-Safe Digital Signature Algorithm
- Can either supplement or replace traditional RSA/ECC digital signatures
- ICSF ML-DSA supported strengths:
  - 4,4
  - 6,5
  - 8,7
- Supported in both CCA and EP11 interfaces.
- Standardized as FIPS-204



Dual Signature Scheme

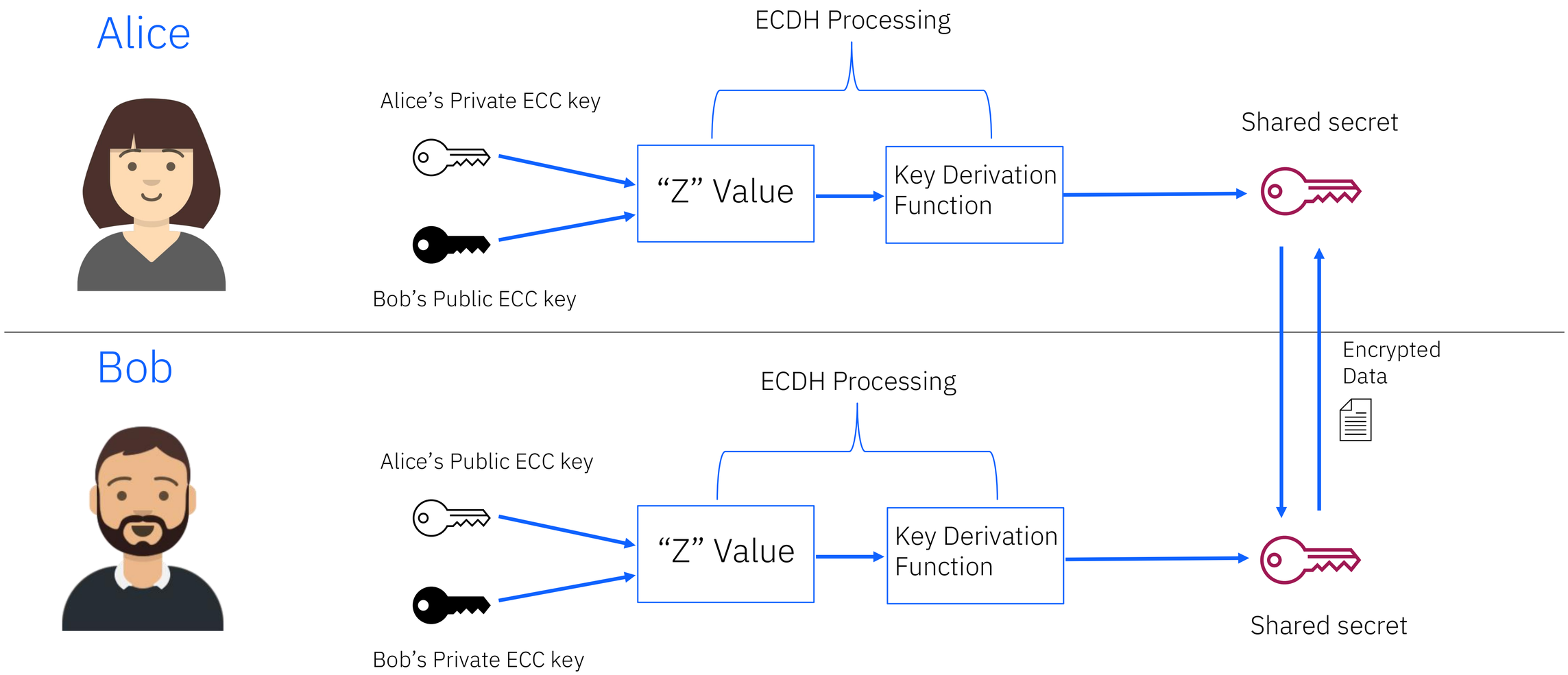
ML-KEM support

- ML-KEM is a Quantum-Safe Key Encapsulation Mechanism (KEM)
- Used in hybrid key exchange schemes to establish a shared secret between two parties
- ICSF ML-KEM supported strengths:
  - 512*
  - 768
  - 1024
- Supported in both CCA and EP11 interfaces
- Standardized as FIPS-203

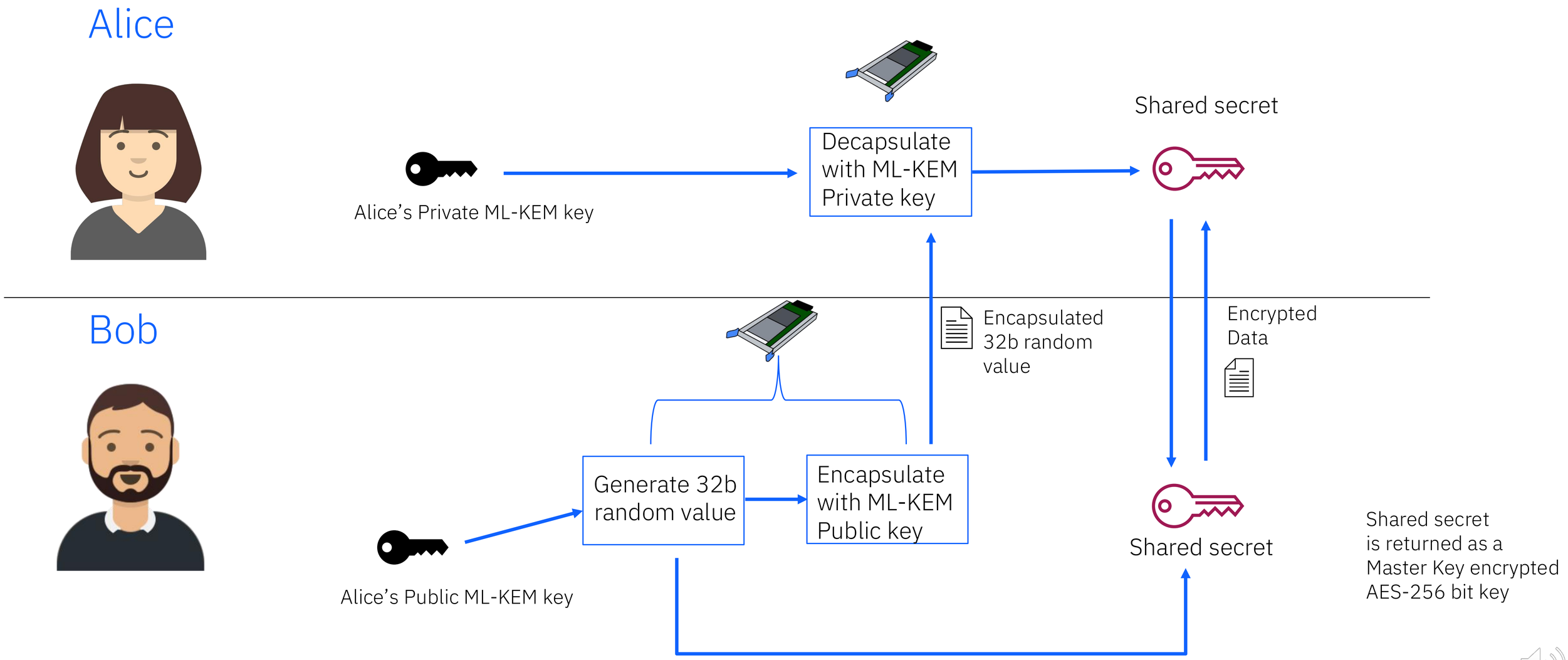


*Supported in EP11 only.

Traditional ECDH Key Exchange

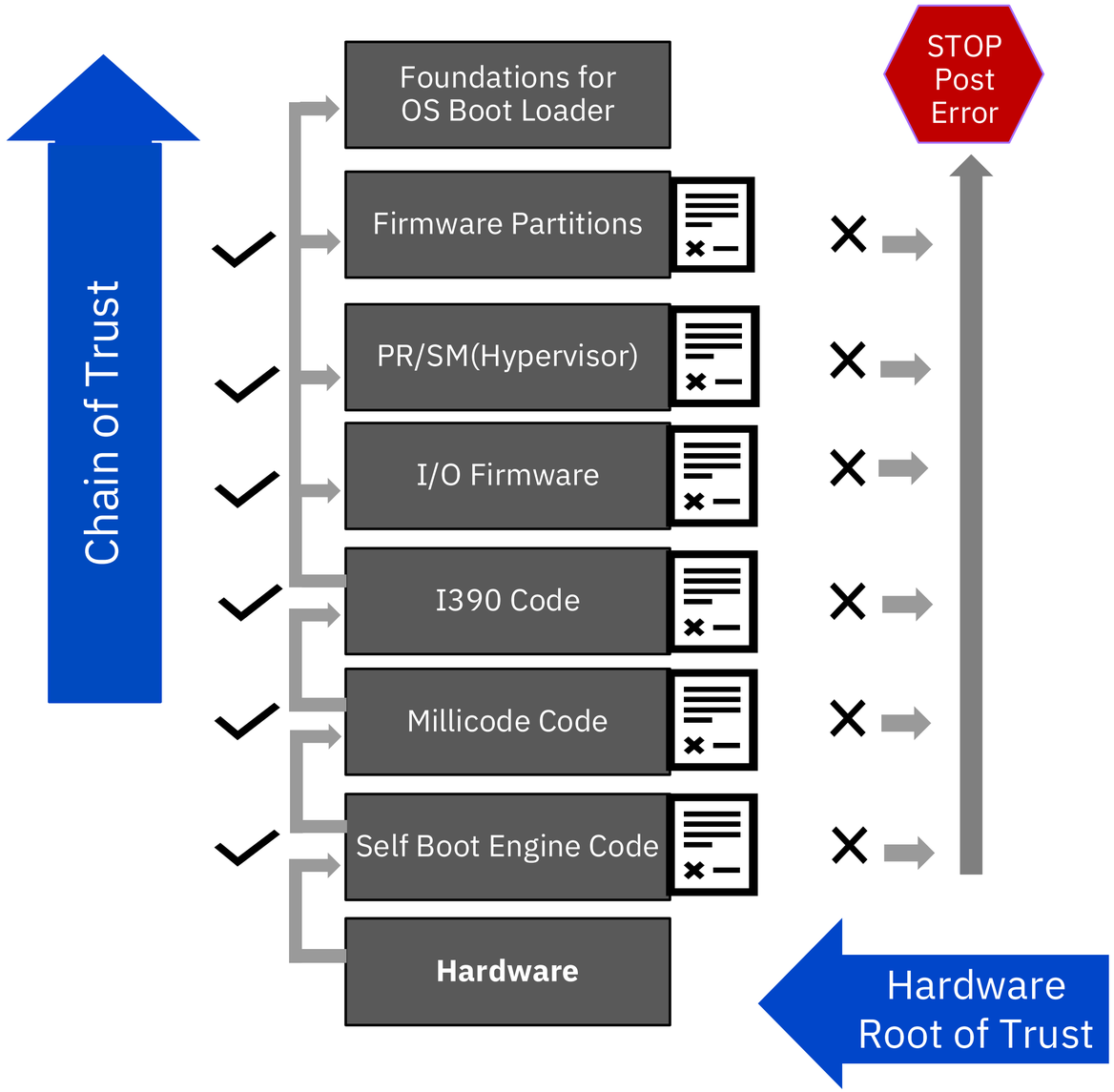


Quantum-Safe Key Exchange with ML-KEM



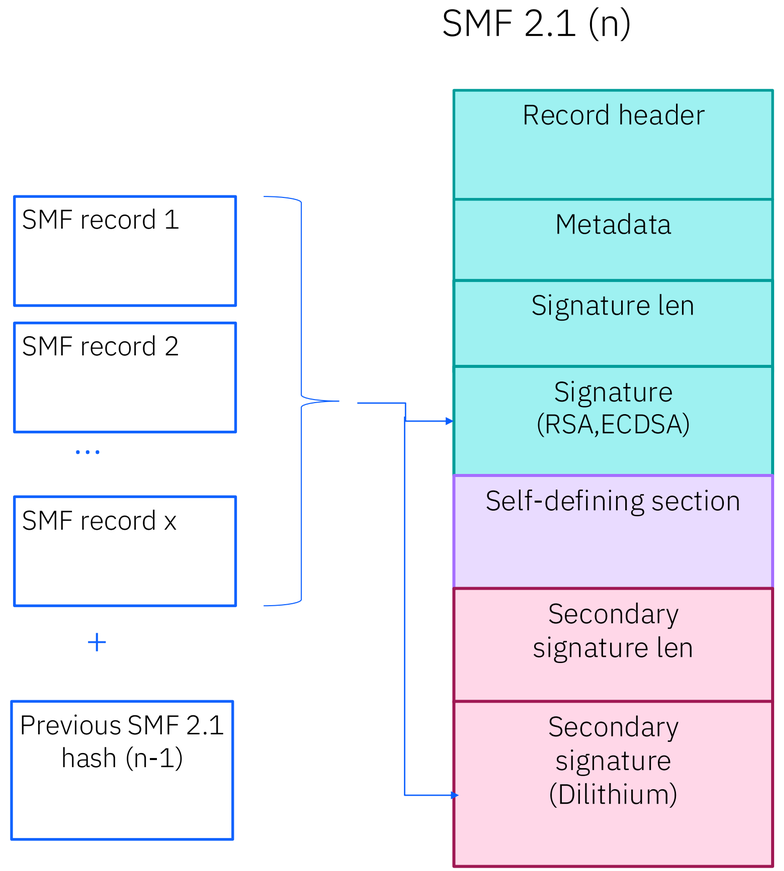
Secure Boot Enhancements

- Secure boot protects system integrity by verifying firmware components during Initial Machine Load (IML)
- Starting on z16, Secure boot takes advantage of a dual signature scheme using the ECC and CRYSTALS-Dilithium algorithms
- Provides two layers of protection which future proofs against attacks from unauthorized firmware (malware)

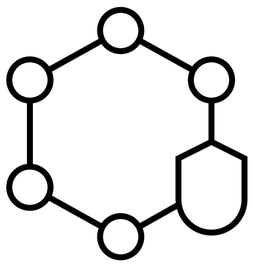


SMF Alternate Signature Support

- CRYSTALS-Dilithium Digital Signature Algorithm supported as a secondary signature in SMF Type 2 Subtype 1 & Subtype 2 records
- Both signatures will be contained within the SMF Type 2 signature record
- Must be used in conjunction with primary signatures and only for SMF records recorded to log streams
- Key creation handled with ICSF PKCS #11 services

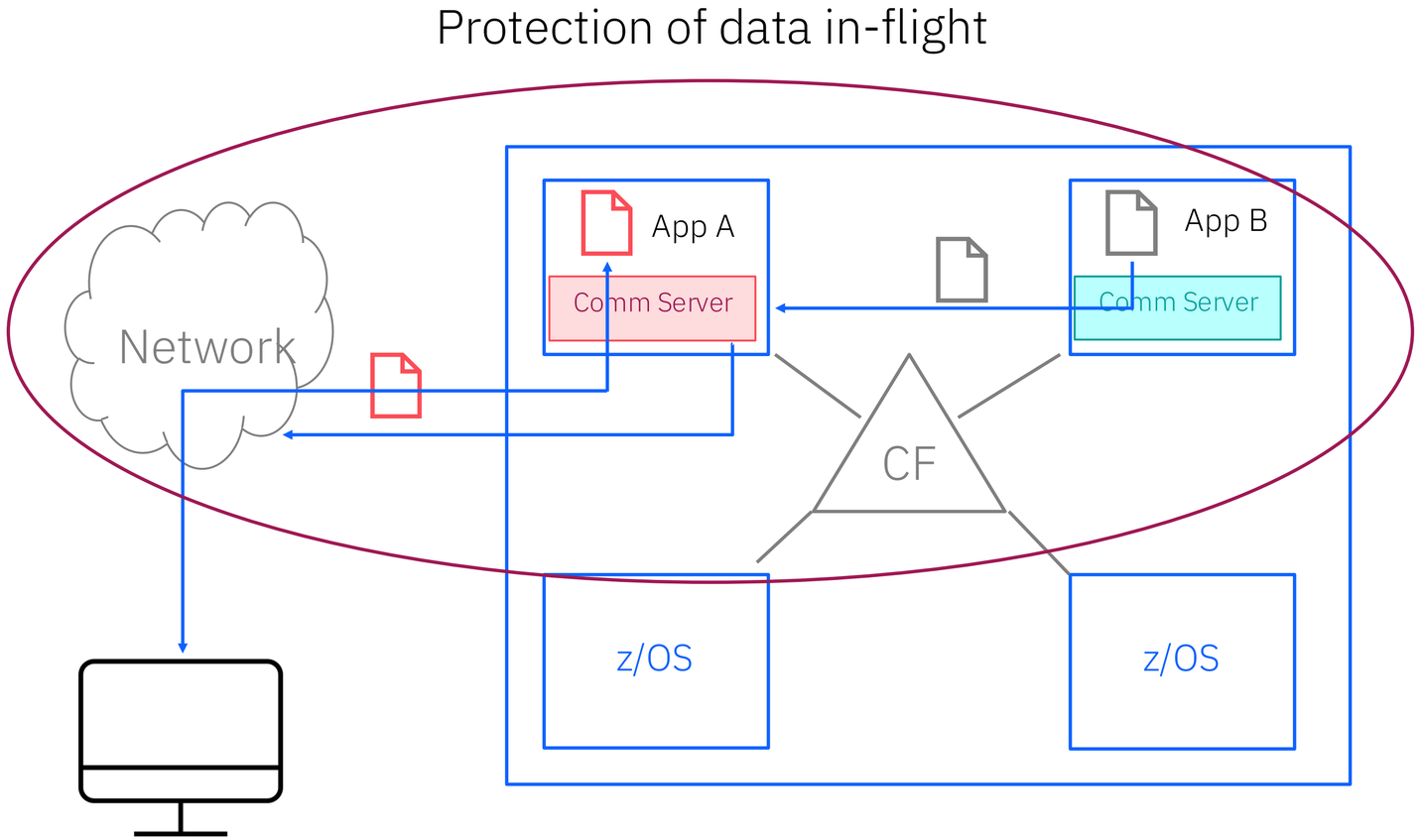


Network Security



z/OS Network Security

z/OS Encryption Readiness Technology (zERT) provides intelligent network security discovery and reporting capabilities by monitoring TCP and Enterprise Extender traffic for TLS/SSL, IPsec and SSH protection as well as cleartext.



zERT features

zERT Discovery

- **SMF 119 subtype 11** "zERT Connection Detail" records
- These records describe the complete cryptographic protection history of each TCP and EE connection
- At least one record is written for each connection - and each describes all cryptographic protection for that connection
- Well suited for real-time monitoring applications
- Depending on your z/OS network traffic, these could be generated in very high volumes

zERT Network Analyzer

- **Web-based (z/OSMF) UI** to query and analyze zERT Summary (subtype 12) records
- The latest network analyzer PTF always contains an up-to-date fresh install image
- Intended for z/OS network security administrators (typically systems programmers)
- Comes with Communications Server at no extra charge, but relies on Db2 for z/OS

zERT Aggregation

- **SMF 119 subtype 12** "zERT Summary" records
- These records describe the repeated use of security sessions over time
- Writes one zERT Summary record at the end of each recording interval for each
  security session active during the interval
- Well suited for reporting and analysis
- Can greatly reduce the volume of SMF records (over Discovery) while providing the same level of cryptographic detail

zERT Policy-Based Enforcement

- Real-time monitoring based on user-written policy rules
- Directs the TCP/IP stack to take specific actions when a user-defined security policy is or is not met for a new TCP connection
- Notification and defensive actions supported

IETF Standards Update

- The Internet Engineering Task Force (IETF) has standardized RFC 9881, defining the use of ML-DSA in X.509 certificates and CRLs
- Multiple IETF drafts are in progress covering Hybrid and Composite post-quantum mechanisms in X.509
- TLS, IPsec, and SSH are progressing through draft post-quantum standards.
- Final Standards for ML-KEM in TLS 1.3 are anticipated in late 2026

TLS 1.3 Migration

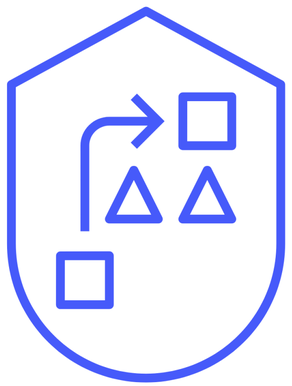
- TLS 1.3 provides the foundation for post-quantum cryptography in enterprise network security

- Key changes in TLS 1.3:
  - Only AES-GCM and ChaCha20-Poly1305 are supported for AEAD ciphers
  - Mandatory Forward Security – Ephemeral keys required via Ephemeral Diffie-Hellman (DHE / ECDHE)
  - Handshake completed in 1 Round Trip vs 2 in TLS 1.2

- Considerations:
  - Prioritize AES-GCM cipher suites as ChaCha20-Poly1305 is currently implemented in software only
  - CPU consumption will likely increase as TLS 1.3 provides stronger cryptographic protections
  - Minimize the number of ClientKeyShares as each generates a new key pair

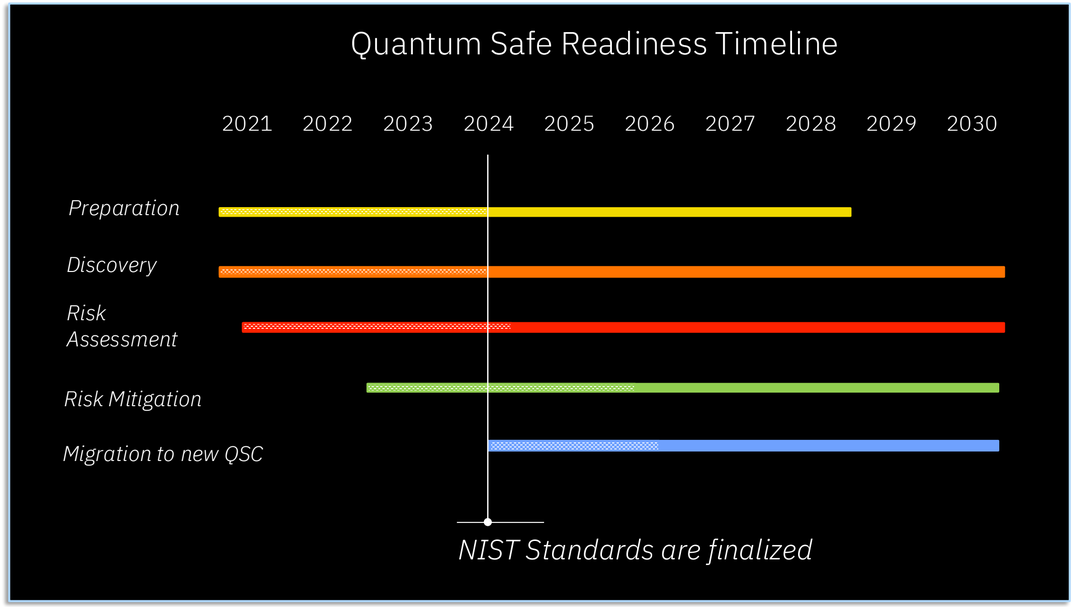
- Review the IBM documentation to get started on TLS 1.3 migration.

Planning and Migration



Quantum Safe Readiness

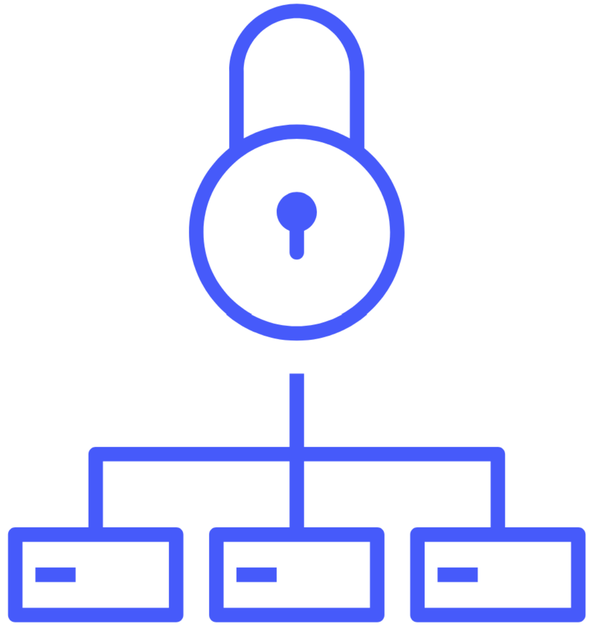
Preparation	• Educate teams/Security Stakeholders. • Follow standards community and quantum-safe computing . • Research Migration Best Practices. • *Redbook : Transition to Quantum Safe Cryptography on IBM Z®*
Discovery	• Create a crypto inventory (reusable security asset) – Inventory cryptographic assets and cryptography use – Inventory data handled by the organization – Inventory suppliers of cryptographic assets • Aid crypto discovery with existing tools and New for IBM z17™ - Crypto Discovery and Inventory Tool
Risk Assessment	• Perform Gap Analysis to discover security risks • Understand internal and external dependencies. • Leverage risk assessment reports to prioritize your execution roadmap • Quantum Safety Assessment with IBM Lab Services
Risk Mitigation	• Reconsider and/or possibly redesign how crypto is consumed in your environment. • Determine best mitigation action: retire it, accept it, or fix it • Quantum Safety Assessment with IBM Lab Services
Migration to Post Quantum Crypto (PQC) / Quantum Safe	• Update old and build new applications, leverage application transparent technology, • z17, Crypto Express 8S, ICSF, Java on z/OS Security, etc. • Protection of data at rest w/ Pervasive Encryption • Protection of data in flight w/ AT-TLS*



*Note: Clients should move to TLS 1.3 now in preparation for Quantum safe TLS.

A Cryptographic Inventory Includes...

- The application under evaluation
- The feature that uses cryptography
- Algorithms used
- Crypto algorithm implementation
- Crypto vendor (IBM or open-source)
- Plus more...



IBM Tooling to Aid Crypto Inventory and Quantum Safe Migration

IBM Z Crypto Discovery & Inventory

- Gain enhanced visibility into cryptographic posture on Z
- Help with compliance by applying internal and regulatory policies
- Prioritize weak cryptography to acceleration remediation planning

Dynamic Crypto Usage Tracking

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

UKO - Crypto Analytics Tool

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

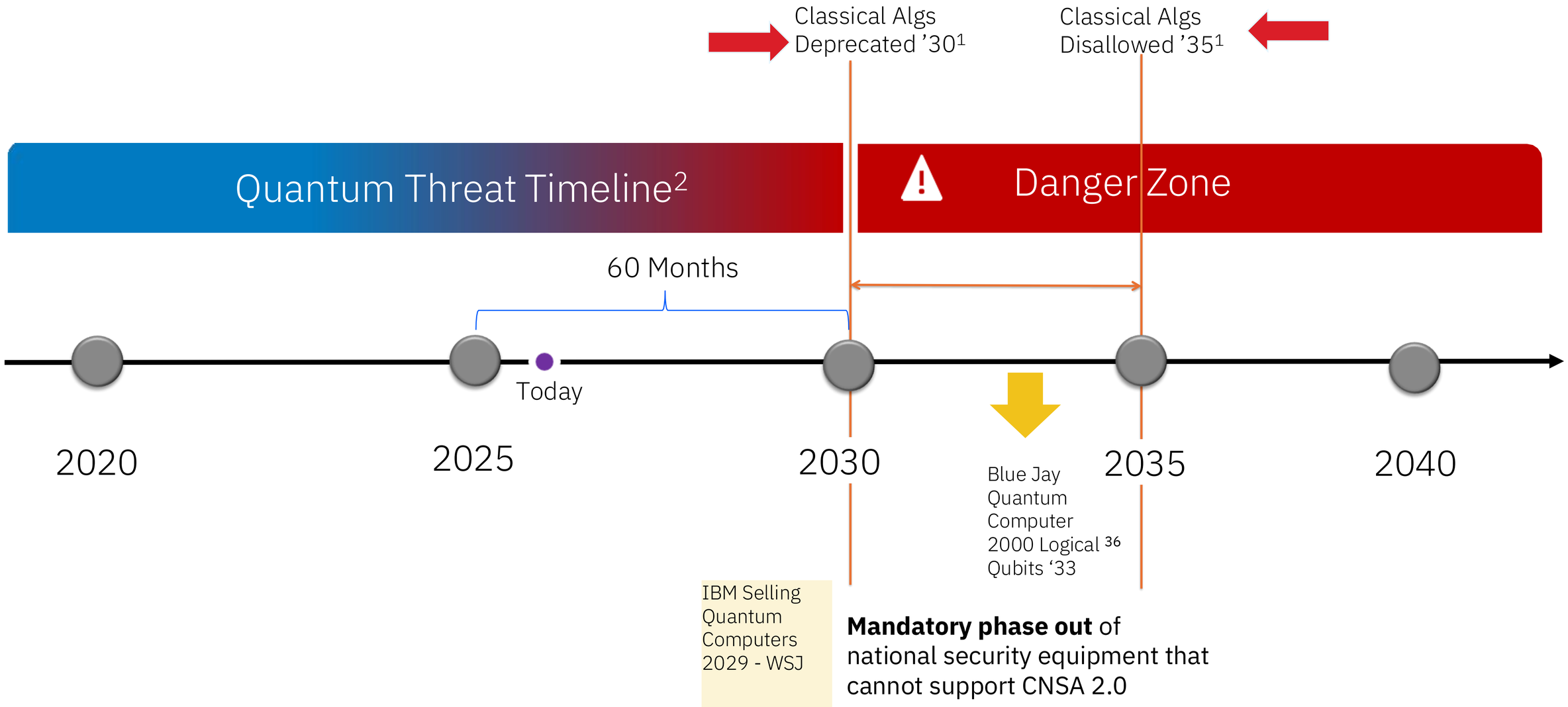
z/OS Encryption Readiness Technology (zERT)

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

IBM Quantum Safe Explorer (distributed environment)

- Scan applications to locate cryptographic artifacts and vulnerabilities
- Create various cryptographic inventory reports

When will the quantum threat materialize?



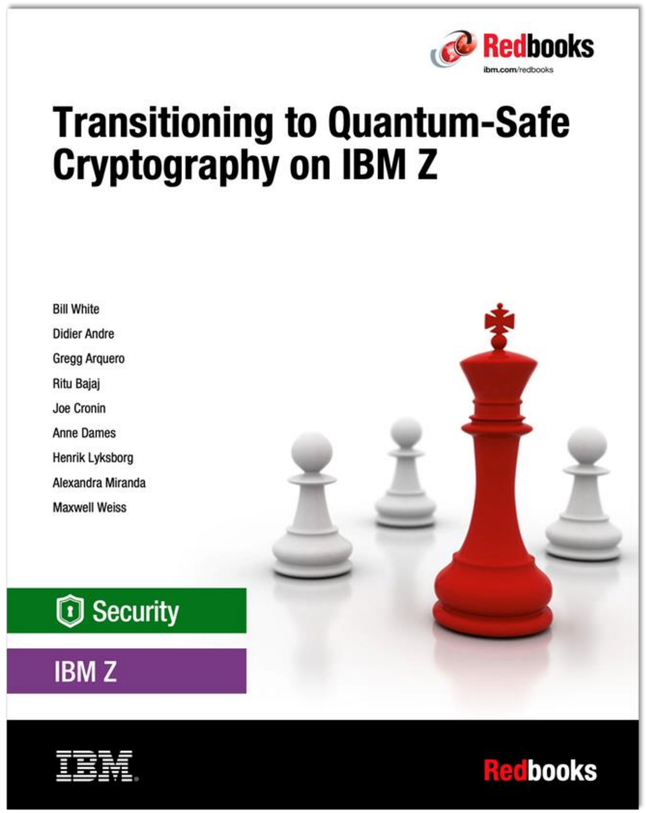
[1] NIST SP 800-131A Rev 3

[2] Source: Dr. Michele Mosca, University of Waterloo, Canada

“Act now – it will be less expensive, less disruptive, and mistakes caused by rushing and scrambling are less likely to be made.” – Dustin Moody - NIST

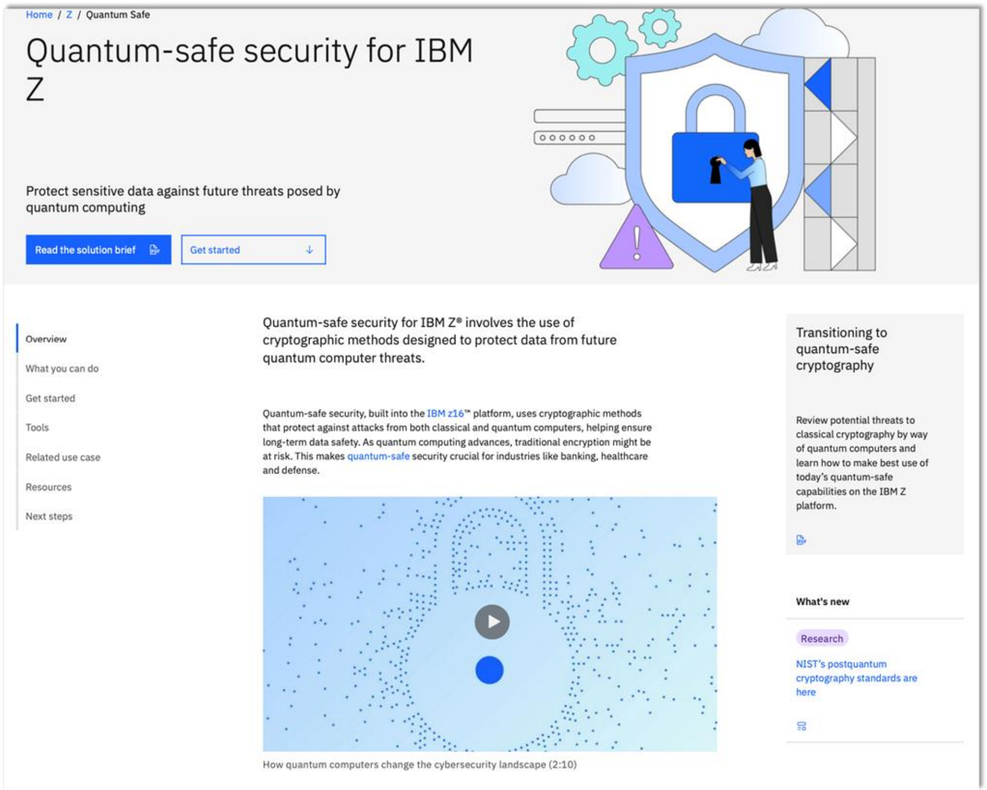
Learn More ...

Download our Redbook



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

Visit our website

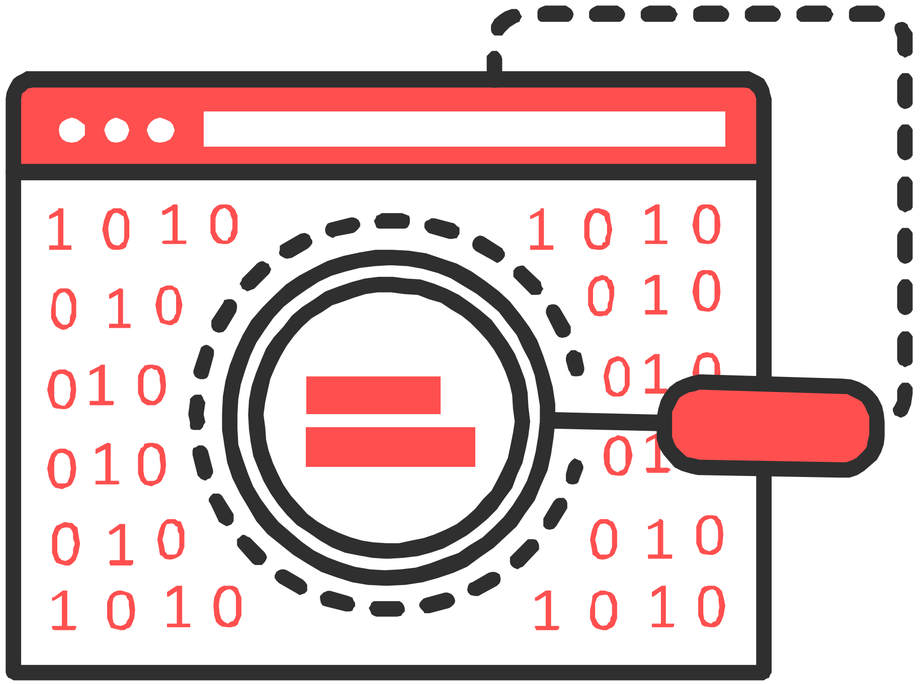


https://www.ibm.com/z/quantum-safe

Additional Resources

- ICSF Publications: https://ibm.biz/BdPmSL
- IBM Crypto Education Community: https://ibm.biz/BdPmSu
- Getting started with z/OS Data Set Encryption Redbook

Questions?



Your feedback is important!

SHARE
EDUCATE ▸ NETWORK ▸ INFLUENCE

Submit a session evaluation for each session you attend:

www.share.org/evaluation

Experience more with IBM

Visit us at the IBM Booth #113

After a full day of technical sessions, take a break with us!

Connect with our experts, snap a photo with the z17 Plexi or the latest Telum II, and get an up-close look at our Spyre Accelerator.

Come back each day for fresh topics and demos at our expert stations.

Think 2026

Join 5000+ senior business and technology leaders who are seizing the AI revolution to unlock unprecedented growth and productivity at **Think 2026**.

Find out more information using the QR code below.

IBM Digital Asset Haven

IBM Digital Asset Haven is the operational backbone for financial institutions and regulated enterprises entering the digital asset economy.

Find out more information using the QR code below.