Future Matters 2024

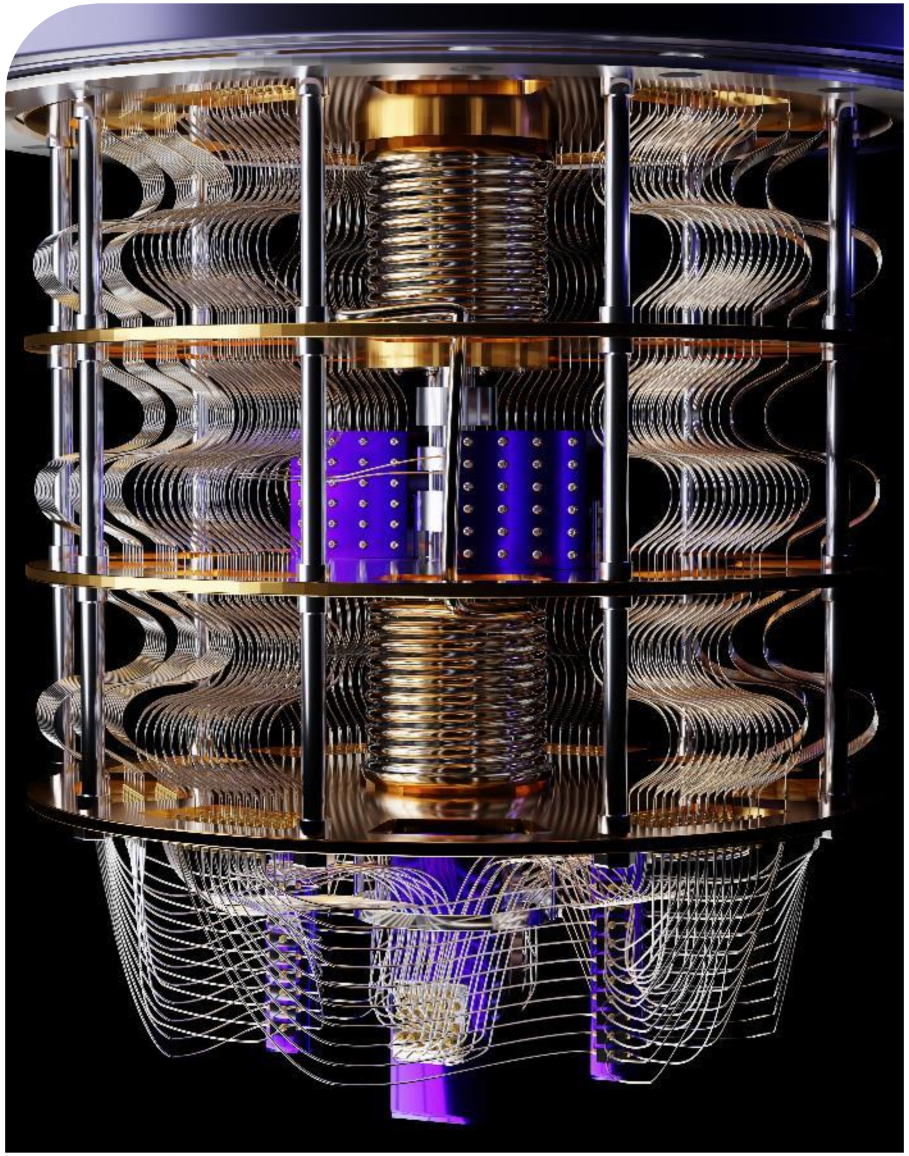
Post-Quantum Cryptography: Safeguarding ClearPath® for the Future

Mike Kain
Distinguished Engineer

Brian Wegleitner
Consulting Engineer

SEPTEMBER 2024

unisys



Addressing the Quantum Threat

- Today's encryption relies on computers being unable to solve certain kinds of problems through brute force
- Quantum computers solve problems that standard computers can't, including some used for securing encryption. **This is the Quantum Threat.**
- To minimize the threat to our clients, platforms are going to be quantum resistant by leveraging **Post Quantum Cryptography (PQC)** as early as possible by using newer cryptography algorithms which aren't susceptible to being broken by brute force.

“

Why Post Quantum Cryptography ?

Federal and Financial are two industries in addition to Insurance that have a narrow **window** to act before a quantum attack, estimated for 2025

- McKinsey

Agencies shall identify **non-complaint systems** and timeline to transition to compliant encryption to include quantum resistant encryption

- Order from President Biden

Once Quantum Computers scale to 4000 qubits, current crypto standards leveraged by majority of businesses today will be

- obsolete

“People describe quantum as a new space race,”

- Inside Quantum Technology

Chance of quantum computer breaking RSA-2048 is **"non-negligible"** by 2026 and 50 to 70% likely **within 10 years**

- Global Risk Institute's 2021 Quantum Threat Timeline report

Classically encrypted data is at risk today thanks to SNDL data harvesting. QC will enhance and complement classical computers to address large datasets processing capabilities. Upgrade to PQ eclipses diligent planning and deep investments that went into Y2K prep. It’s an immense, high-impact event that will override existing crypto methods and make current infrastructure and application protections irrelevant

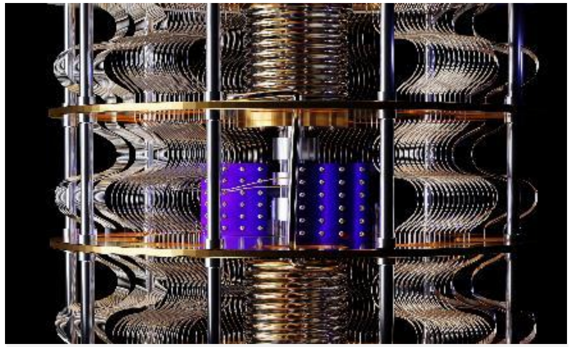
- Accenture

Core Concepts

Crypto Agility

Ability to insert new crypto and remove weak crypto as security landscape evolves.

- Parity with industry guidance
- Crypto policy management



Cryptographically-Relevant Quantum Computer (CRQC)

A quantum computer powerful enough to run algorithms that crack or weaken traditional cryptography

Post Quantum Cryptography (PQC)

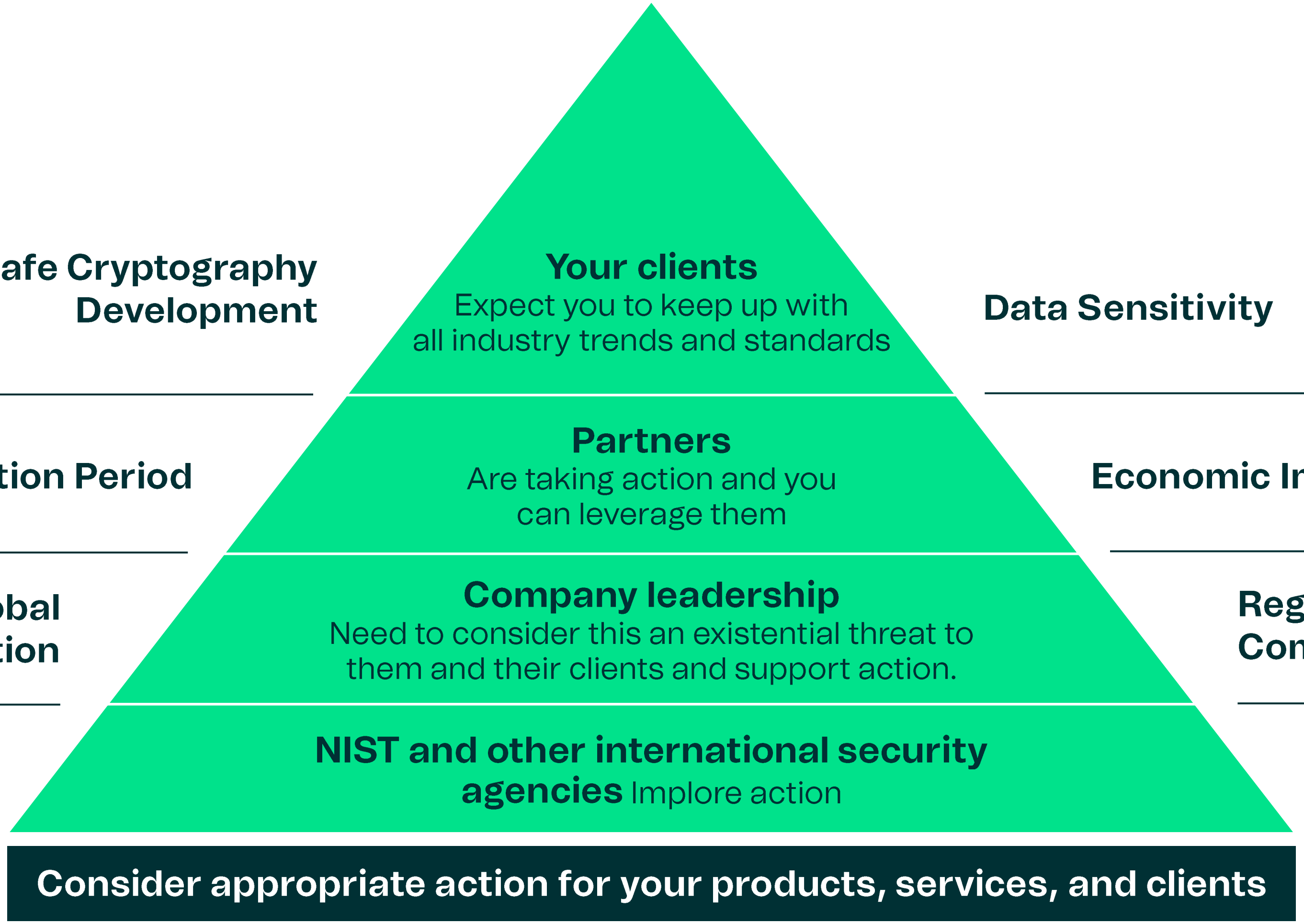
Cryptographic methods designed to protect against CRQCs.

- New algorithms for classical computers
- Quantum key distribution (QKD)
- Quantum random number generation (QRNG)

Quantum Resistance (QRE)

Cryptographic algorithms implemented for classical computers that are resistant to attack from CRQCs

Case for Post Quantum Cryptography



Your clients
Expect you to keep up with
all industry trends and standards

Partners
Are taking action and you
can leverage them

Company leadership
Need to consider this an existential threat to
them and their clients and support action.

NIST and other international security agencies Implore action

Consider appropriate action for your products, services, and clients

Quantum-Safe Cryptography Development

Transition Period

Global Adoption

Impact on Current Encryption

Data Sensitivity

Economic Impact

Regulatory & Compliance Mandates

Public Awareness

Post Quantum Cryptography across the Industry

Leading Cloud Hyperscalers adopt PQC

Key services on **Amazon's** AWS including KMS now support post quantum algorithms

Microsoft and **Google** utilize PQC and have researchers actively contributing to OSS libraries

Large Corporations incorporate crypto agility and enhance the PQC space

IBM – Quantum Safe Platform

Apple – PQ3 iMessage protocol

Zoom – quantum end-to-end encryption

Accenture – QuSecure collaboration to bring PQC to space, adoption of crypto agility

Akamai, **Cloudflare** and other large internet CDNs and services

Telecoms provide the canvas for adoption of Quantum Key Distribution

Vodafone, **Verizon**, **OpenQKD** etc. lend their optical infrastructure to enable advanced quantum use cases

There are extensive efforts and investments underway to prepare for PQC

Industry Drivers

Steal Now Decrypt Later

Malicious actors are harvesting encrypted data in anticipation of powerful quantum computers being available

Industry Guidance

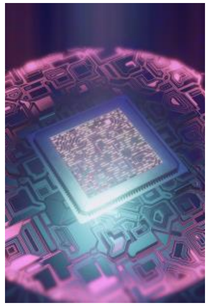
NIST - TLS 1.3 by January 1, 2024

NSA - Software signing with CNSA 2.0 starting in 2025

Client Requirements

Encryption in everything!

TLS 1.3 important for network connections



Quantum Advancement

NIST predicts CRQCs to arrive by 2030

IBM announced 100K qubit quantum computer by 2033

2023 paper shows potential for scalable silicon quantum processors

PQC Landscape

NIST PQC standard published in 2024

IBM z16 mainframe has “quantum-safe technologies”

Very proactive companies have already started this journey.

Quantum Resistance and Beyond

Near Term: QRE Implementation

Phase 1: Crypto Agility and Discovery

- Achieve and maintain parity with **industry standards** and capabilities that maximize protection and compatibility
- Transition to **third party crypto APIs** to reduce support costs and to accelerate access to new crypto
- **Systemwide management of crypto policy** for ease of configuration, monitoring, and enforcement

Phase 2: Quantum Resistance

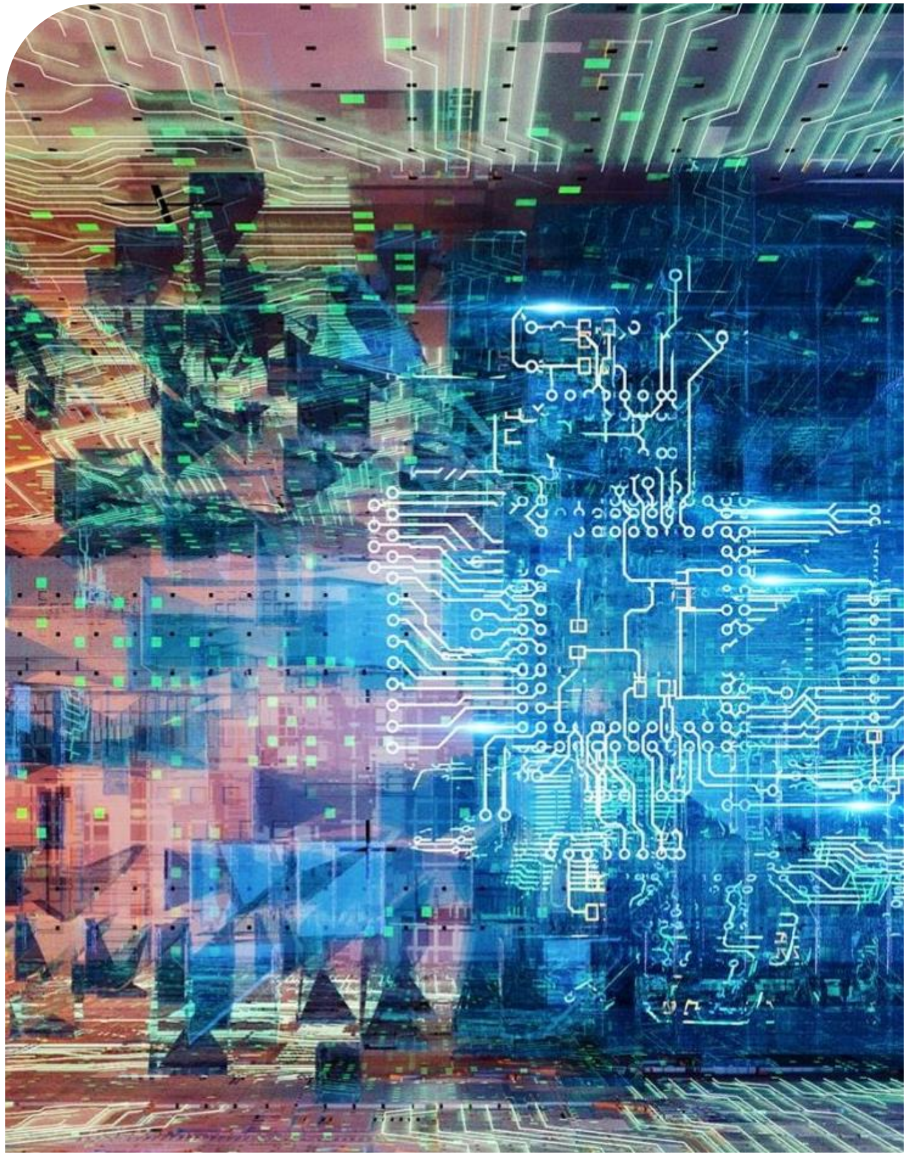
- **Adopt new NIST algorithms*** to provide quantum resistance. (Primarily for data in motion)
- **Strengthen existing algorithms** to provide resistance to quantum attack. (Primarily for data at rest)

Long Term: Post QRE

Future Considerations

- Integrate with **quantum key distribution** services for keys that can't be intercepted or attacked. (Requires vendor proprietary infrastructure with limited availability)
- Increase overall strength of crypto by supporting **Quantum Random Number Generator (QRNG) devices.** (If required)

- On August 14th, 2024, NIST formally approved FIPS for three Post Quantum Cryptography algorithms.
- *Current-generation QKD is shown to be impractical for common cryptographic use cases. This opinion is shared by security organizations like the NSA as well as eminent cryptographers.*



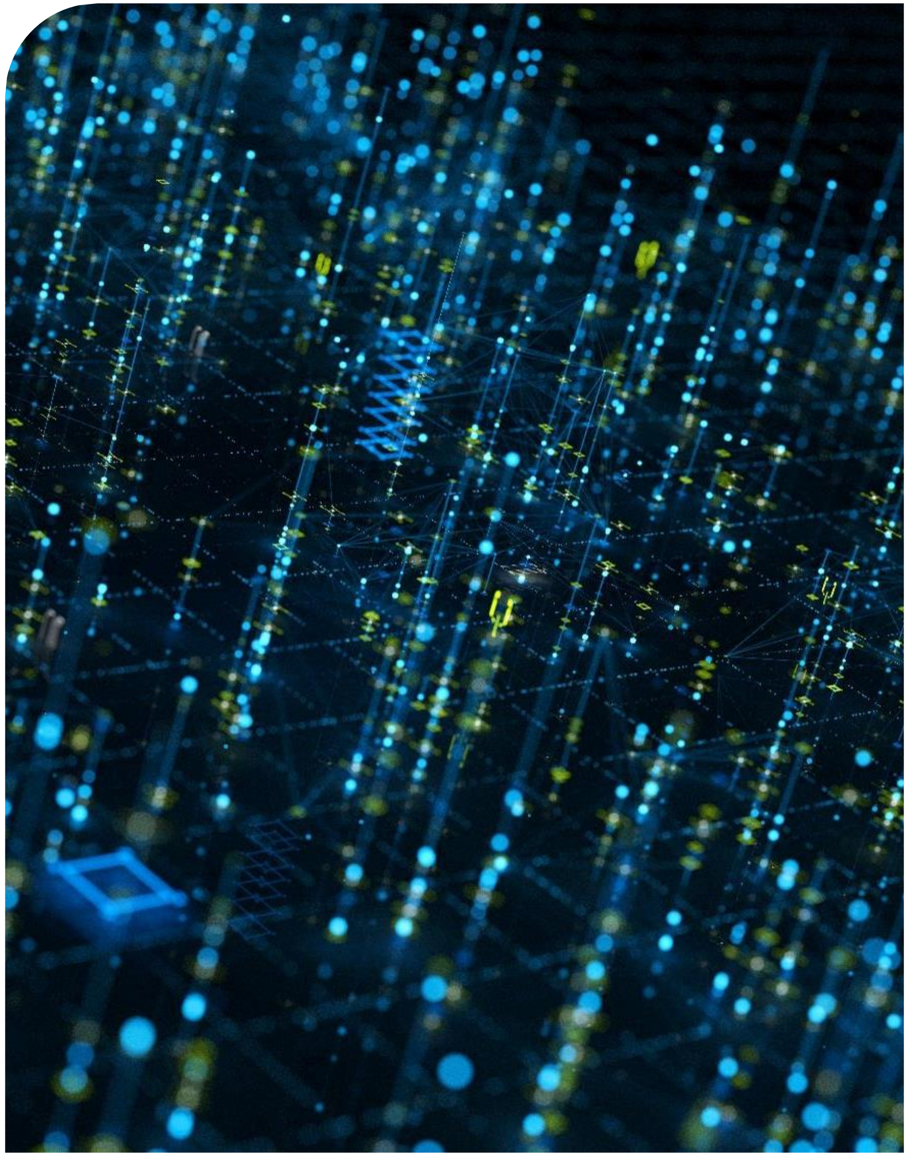
SNDL
(Steal Now, Decrypt Later)

Businesses need to be on high alert for data breaches, even if the data is encrypted.

Attackers or nation-states may try to capture data communications or data at rest in the hope that at a later time, the data encryption can be broken with quantum computers.

Businesses also have to consider how long that the data has value to the business and/or the individual.

Data that is still sensitive when CRQCs are available must be secured with QRE algorithms.

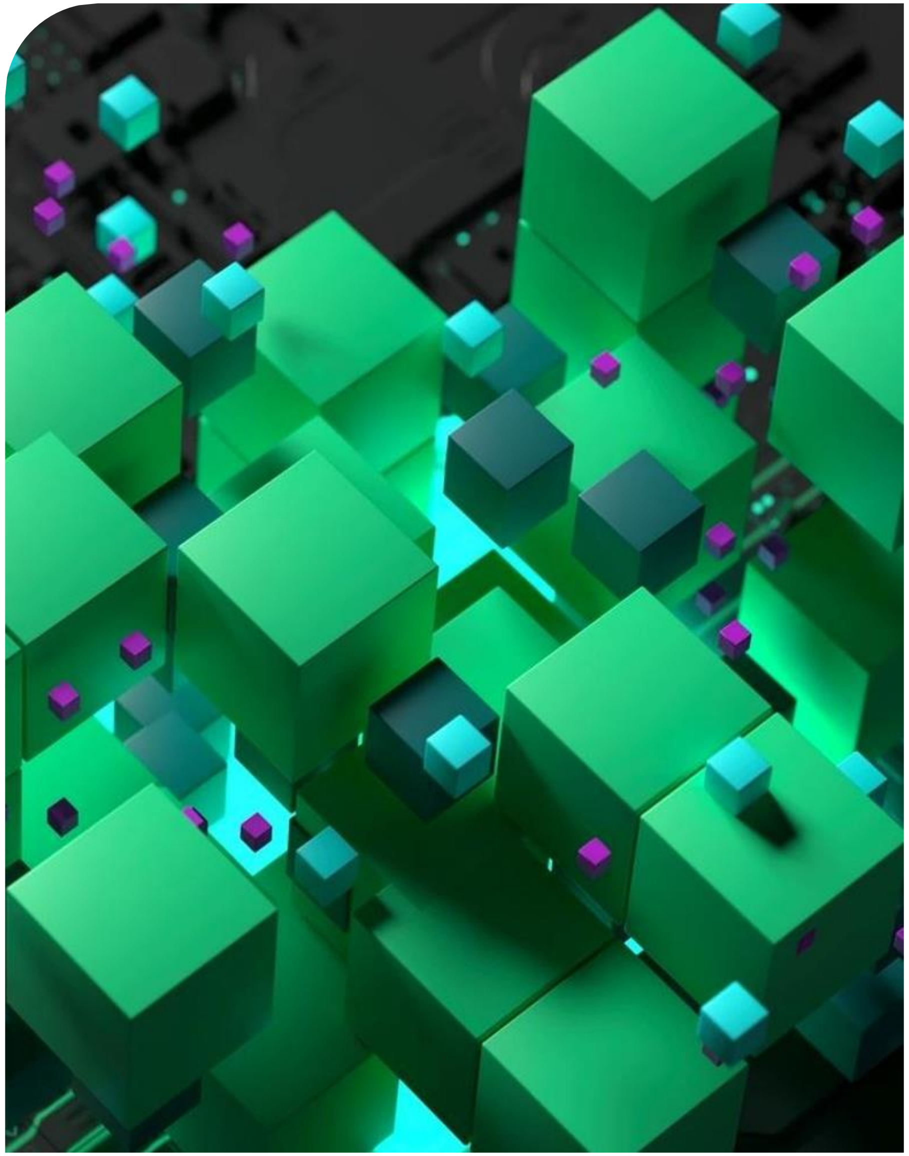


“Crypto Agility”

Computers and businesses now have a requirement to know what algorithms are being used or negotiated within their environments, taking special note of outdated and deprecated algorithms, and an ability to rapidly change those in use.

“Cryptographic Inventory”

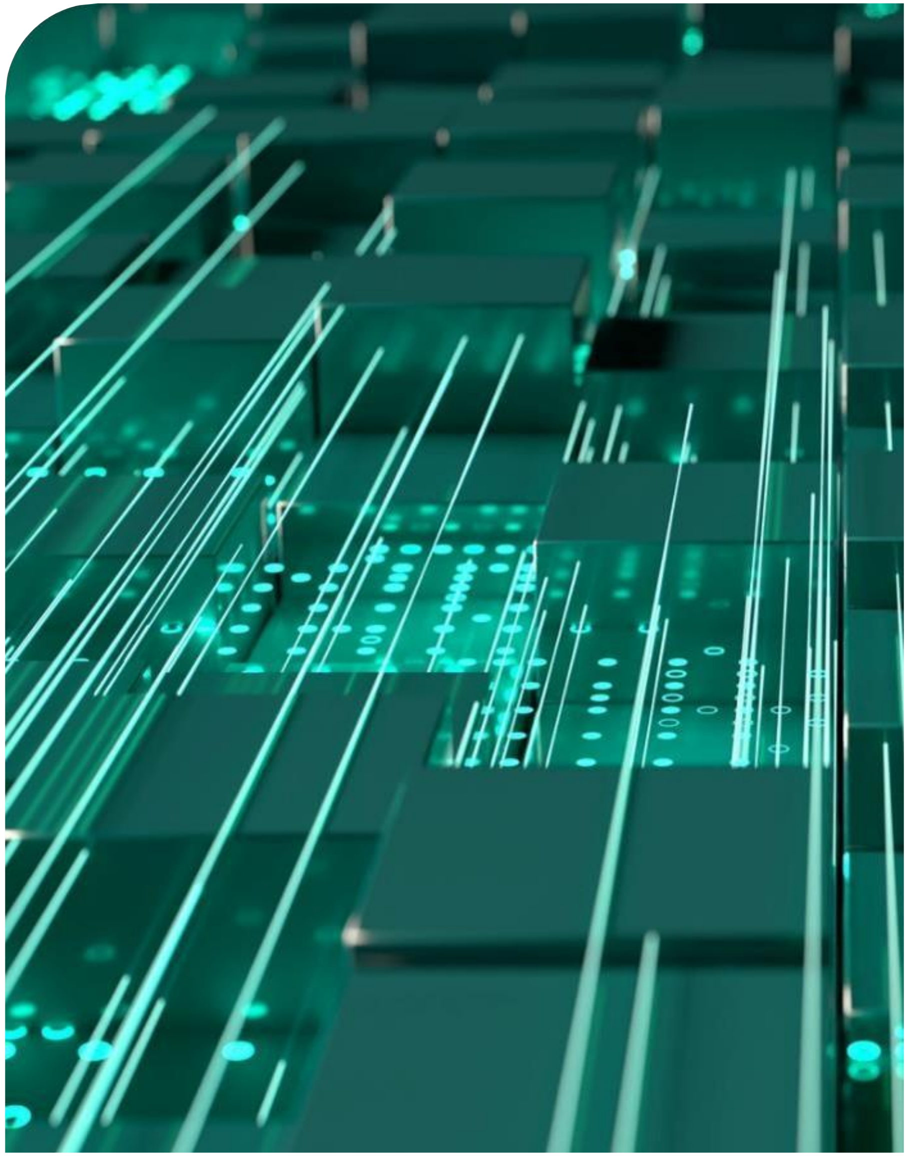
Where you use cryptography, how, and from what supplier.



Monitoring Cryptography

One of the most important points is to devise how to monitor what cryptographic algorithms are in use and where.

But once you know where all the pieces are, you have to run your business and keep an eye in real-time of what protocols, what versions, and what cryptographic algorithms are in use and where (especially with negotiated protocols). If unwanted or deprecated algorithms are being used (especially with systems outside of your control), then risk is introduced and changes are necessary. If deprecated algorithms are used, then risk is introduced and changes are necessary.



QRE Standards

New cryptography standards approved as of August, 2024:

- ML-KEM (was: Kyber) FIPS 203 - public key distribution (like RSA)
- ML-DSA (was: Dilithium) FIPS 204 - digital signatures
- SLH-DSA (was: SPHINCS+) FIPS 205 – digital signatures

Once the cryptography is standardized, it must be integrated into network protocols and other use cases (in progress), such as:

- TLS 1.3
- SSH
- IPSEC
- Kerberos
- Data at Rest / Storage Encryption
- And all other uses

This is where the IETF currently is working.

This is nothing new, but it will occur at a much faster rate than the past and will likely occur even faster in the future.

The journey to quantum resistance

- Automated monitoring
- Policy-based decisions at the platform level
- Auditing/Logging of cryptography inventory

Cryptographic Inventory checklist

Data at Rest (Steal Now, Decrypt Later)

- Where is encryption used – disk, file, database
- Where credentials are stored, passwords, secrets
- Data Life Expectancy – will the data be valid 2 years from now? 5?   10?
  - Are there any regulation or compliance directives which will drive results?
- Inventory:
  - Platforms
  - Operating Systems
  - Key Management Processes
  - Cryptography in use
- Monitoring process for environment and data access (active, persistent, automated)

Cryptographic Inventory checklist

Data in motion (Sniff Now, Decrypt Later)

- Inventory all network traffic, both encrypted and unencrypted
- Identify network zones – points for data capture / firewalls / choke points
- Encrypted communications – what protocols are in use? TLS? SSH? IPSEC? SMB/CIFS? Other?
- Are there communications that should be encrypted?
- Inventory:
  - Platforms (including network core infrastructure such as routers, etc.)
  - Operating systems
  - Applications
  - Key management processes
  - Monitoring processes for networking – to track dynamically what algorithms are in use (most cryptographic algorithms are negotiated).

ClearPath MCP

- Cryptographic Inventory completed.
- TLS 1.3 available as MCP 21.0 (63.0) Interim Corrections
  - CTB 11738 (MVP1 - server) and CTB 11892 (MVP2 – client) have more details
  - Will allow you to start integration with TLS 1.3 on endpoints which talk to MCP.
- Cryptographic Use Telemetry feature under development for MCP 20.0 (62.0) and MCP 21.0 (63.0) releases as well as MCP 22.0 (64.0)
  - Enables each product to log its use of cryptography for visibility/telemetry.
  - New major/minor type defined just for this telemetry (20,7)
  - Then will allow clients to sample sumlogs for cryptography in use
  - Basis for future cryptographic monitoring and policy in MCP.
  - Will be announced via CTB when ready.
- Other features and content being planned (cryptographic policy/agility, etc)

ClearPath OS 2200

- Cryptographic inventory completed
- Review communications configuration
  - Default cipher suites
  - TLS 1.3 - CP 20.0 on Dorado x600 1.0, x500 2.2, x400 3.2, CSS 3.0 or higher
- Review application usage
- Review PCAPs
  - Capture using TRACE NET commands of CPCommOS
  - Filter for review using WireShark
- PQC algorithms & cipher suites
  - OpenSSL & Microsoft

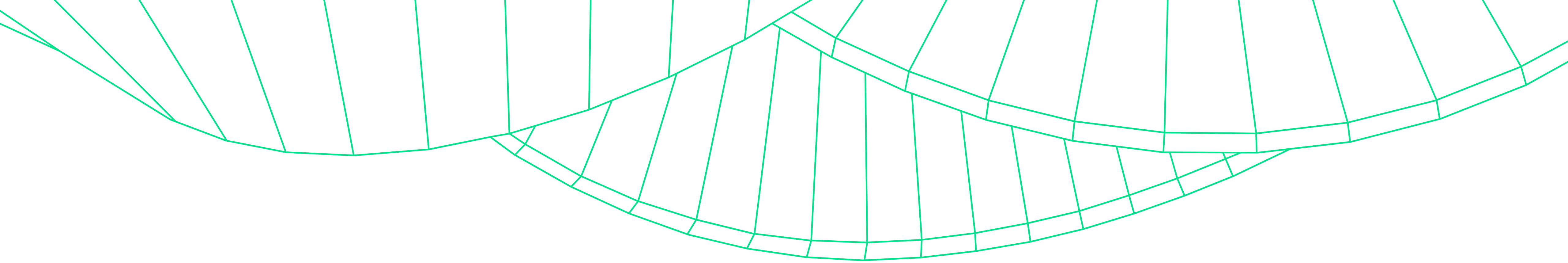
ClearPath Cross-Platform

ePortal, Data Exchange, BIS, EOM, AB Suite

- Cryptographic Inventory completed.
- Working with each product team to understand platform roadmap and how/where vendors are making it quantum-resistant.
  - Microsoft
  - SUSE/OpenSSL

ClearPath Services

- Has the quantum resistance topic come up in your company yet?
- Do you know where your network traffic is encrypted and where it’s not?
- Do you know what algorithms are in use for each connection (either internal or with partners?)
- Do you need help from Unisys in any part of this journey?



Questions?

Thank you

For more information, please contact
Michael.Kain@Unisys.com
Or Brian.Wegleitner@Unisys.com.

unisys

unisys.com

The Information contained in this document is confidential and commercially sensitive. In consideration of the receipt of this document, recipient agrees not to reproduce or make this information available in any manner to any third party or any person who does not have immediate responsibility for evaluation of its contents. All brands and products referenced in this proposal are acknowledged to be trademarks or registered trademarks of their respective owners.

Further, the information contained herein is accurate to the best of Unisys' knowledge at the time of publication. In no event shall Unisys have any liability whatsoever whether in contract, tort (including negligence or negligent misstatement) or under statute for any inaccurate or incomplete information contained in this document. Any information provided herein is based on relevant information available at the present time and is only an estimate. Any prices contained in this document are and subject to change. Unisys' offer is provided on a "subject to contract" basis. The Customer and Unisys will not become legally bound to each other unless and until a formal written contract has been executed on behalf of both parties by their respective authorized representatives.