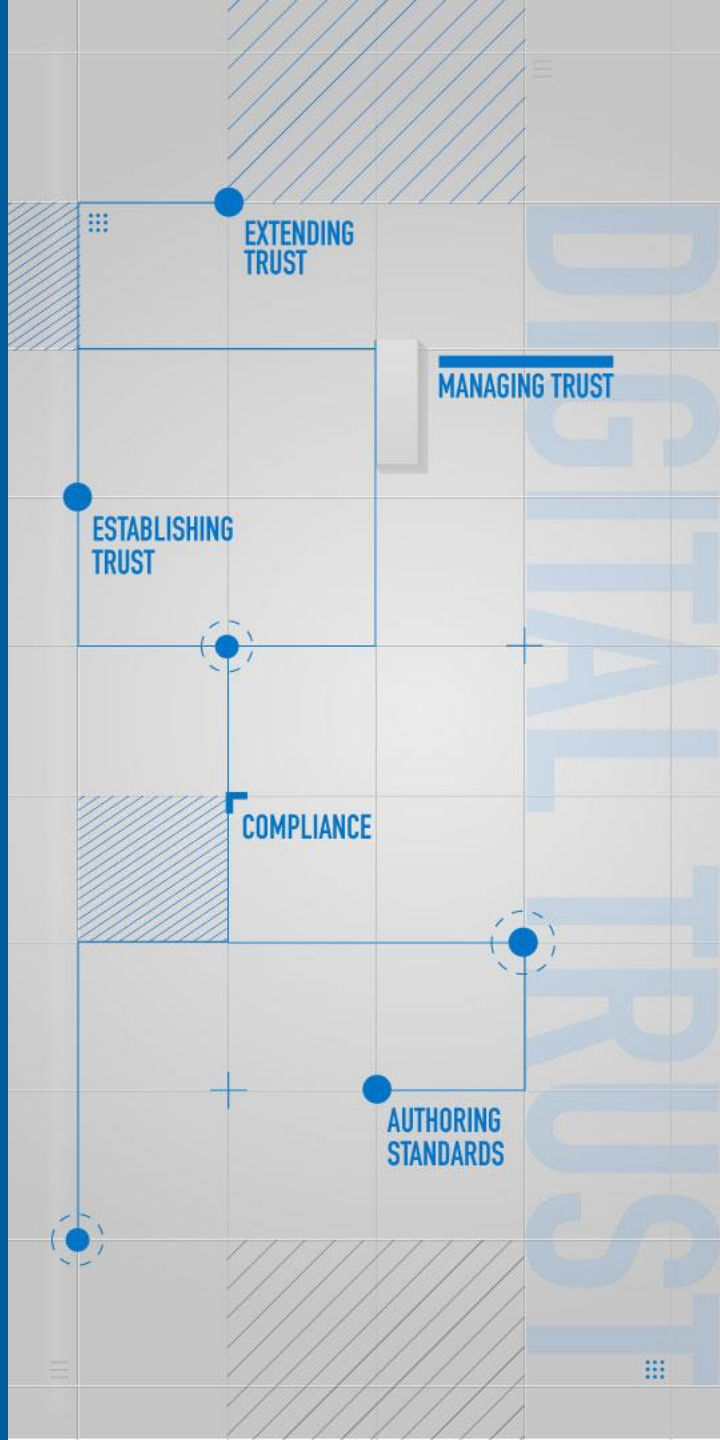
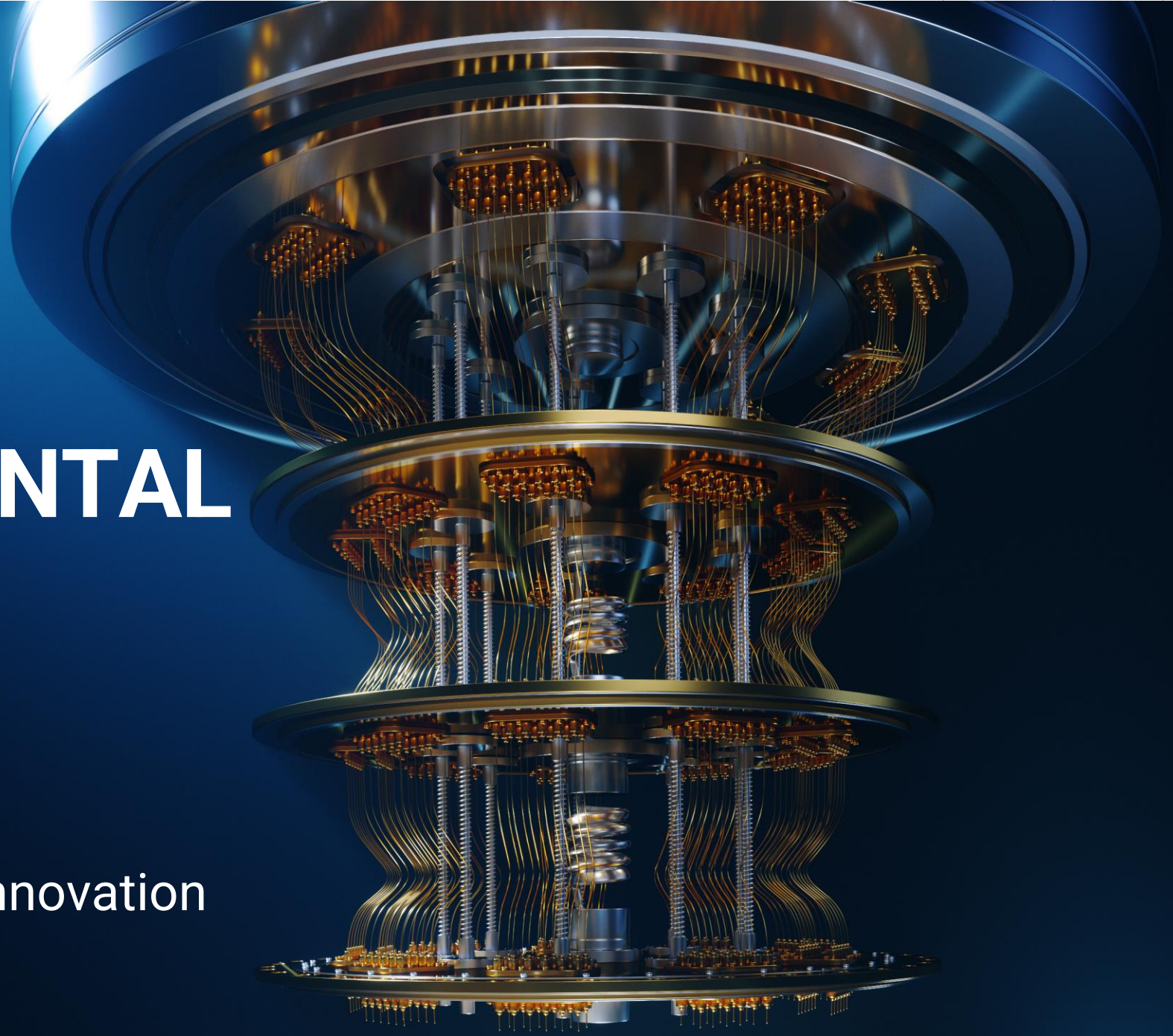
PREPARING FOR THE FUTURE THREATS WITH TODAY'S SOLUTIONS

A strategic roadmap for preparation against quantum threat

digicert®



QUANTUM COMPUTING HAS MONUMENTAL POTENTIAL



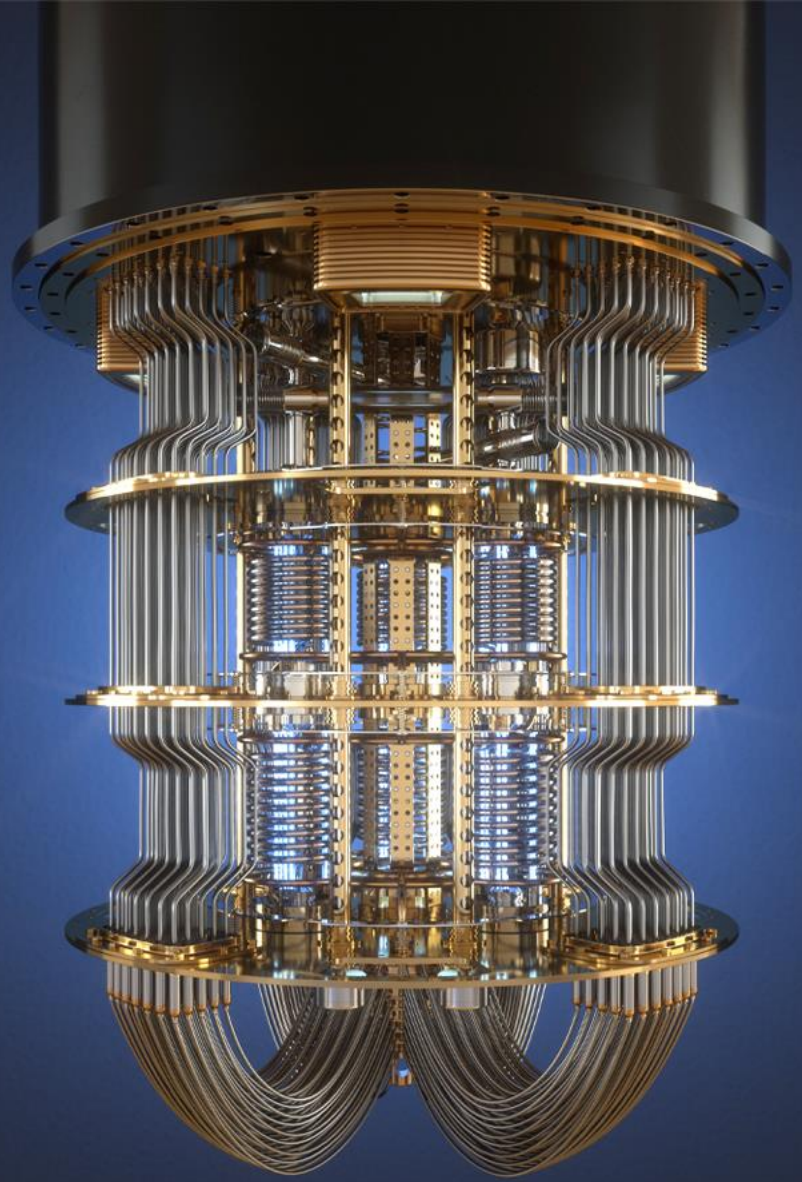
1000s of times faster
Accelerate discovery and innovation

THE QUANTUM EFFECT ON TODAY'S CRYPTOGRAPHY

Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symmetric	AES 128	128	64	Grover's Algorithm
	AES 256	256	128	

THE IMPACT OF QUANTUM COMPUTING

Breaks Everything | Complex Fix | Accelerating Timelines



HOW ARE SECURE COMMUNICATIONS VULNERABLE?

Secure Communication Protocol

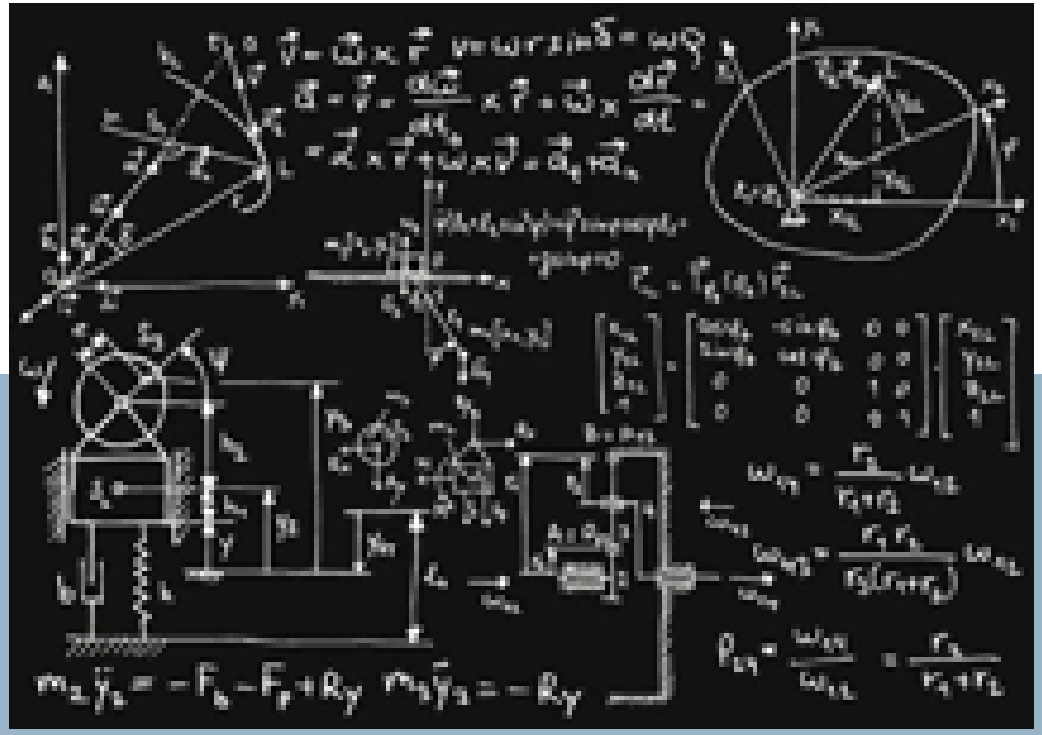
Shor's Algorithm breaks current public-key algorithms

Key Establishment

Authentication

Grover's Algorithm weakens symmetric encryption (square root)

Encrypted Transmissions



Quantum-Safe Cryptography

QUANTUM RESISTANCE IN THE REAL WORLD

ML-KEM	ML-DSA	SLH-DSA	FN-DSA
Crystals-Kyber	Crystals-Dilithium	SPHINCS+	FALCON
FIPS-203	FIPS-204	FIPS-205	FIPS-206
Key encapsulation for secure communications	Secure identities and electronic signatures	Security for long term use cases	Security for fast transaction processing

NIST TIMELINES (NOV 2024)

4.1.1. Digital Signatures

Table 2 lists currently approved quantum-vulnerable digital signature algorithm standards.

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

NIST.IR.8547

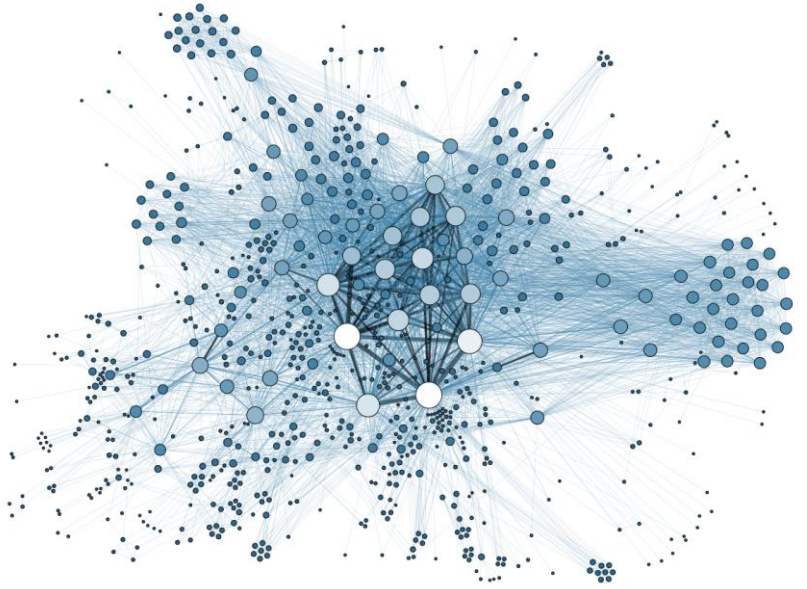
THE MIGRATION CHALLENGE

Key Establishment vs. Authentication

Key establishment can be easily upgraded because the client and server negotiate which algorithm to use.

1. Use quantum-safe key transport or key agreement algorithms
2. Use hybrid keys, a mix of both classic and quantum-safe algorithms

The complexity and interconnectivity of public key infrastructure demands action today in order to be ready for the quantum age, and difficult to do while maintaining backward compatibility.



A ROAD FULL OF PROBLEMS

Google Chrome's new post-quantum cryptography is causing some issues

News By Craig Hale published yesterday

Chrome 124 not working? Try this

Image credit: Shutterstock (Image credit: Shutterstock)

Cloud Security, Encryption

Chrome users report broken connections after Chrome 124 release

Steve Zurier April 29, 2024

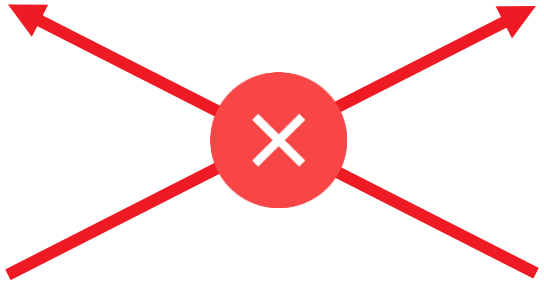
(Adobe Stock Images)

Google Chrome users have been reporting having trouble connecting to websites, servers, and firewalls after Chrome 124 was released last week with quantum-resistant X25519Kyber768 encryption.

CERTIFICATES SUPPORT A SINGLE ALGORITHM

Classical

Classical



User/server needs to select which certificate to use

PKI management costs increase

Quantum-safe

Quantum-safe

Certificate Viewer: gov.bc.ca

General | Details

Issued To

Common Name (CN)	gov.bc.ca
Organization (O)	Government of the Province of British Columbia
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	Entrust Certification Authority - L1K
Organization (O)	Entrust, Inc.
Organizational Unit (OU)	See www.entrust.net/legal-terms

Validity Period

Issued On	Wednesday, July 10, 2024 at 11:05:05 AM
Expires On	Tuesday, July 22, 2025 at 11:05:04 AM

SHA-256 Fingerprints

Certificate	b09bf9343eb8d2adf8f1039f20280e8d3e7ec2777b947cb35293b52b1c85ea50
Public Key	00a22f5d59b9a1ecb46cce94e00a6d72317e2c45b11e9bab9d1191830fa8781b

Certificate Viewer: gov.bc.ca

General | **Details**

Certificate Hierarchy

- Entrust Root Certification Authority - G2
  - Entrust Certification Authority - L1K
    - gov.bc.ca

Certificate Fields

- Not Before
- Not After
- Subject
- Subject Public Key Info
  - Subject Public Key Algorithm
  - Subject's Public Key
- Extensions
  - Certificate Basic Constraints

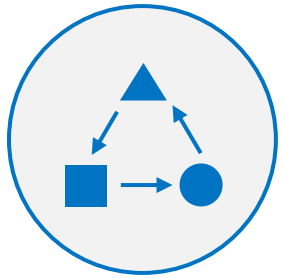
Field Value

PKCS #1 RSA Encryption

Export...

OTHER CHALLENGES

With increased connectivity, the scale of what needs to be updated also increases.



Maintain
Interoperability

Migrate Critical
Systems Faster

Reduce
Migration Costs

WHAT IS CRYPTO AGILITY?

A design feature that enables updates to future cryptographic algorithms and standards without the need to modify or replace the surrounding infrastructure.

-The US Department of Homeland Security

ROAD TO CRYPTO AGILITY

Discover

Identify and assess quantum vulnerabilities across your digital certificate ecosystem.

Manage

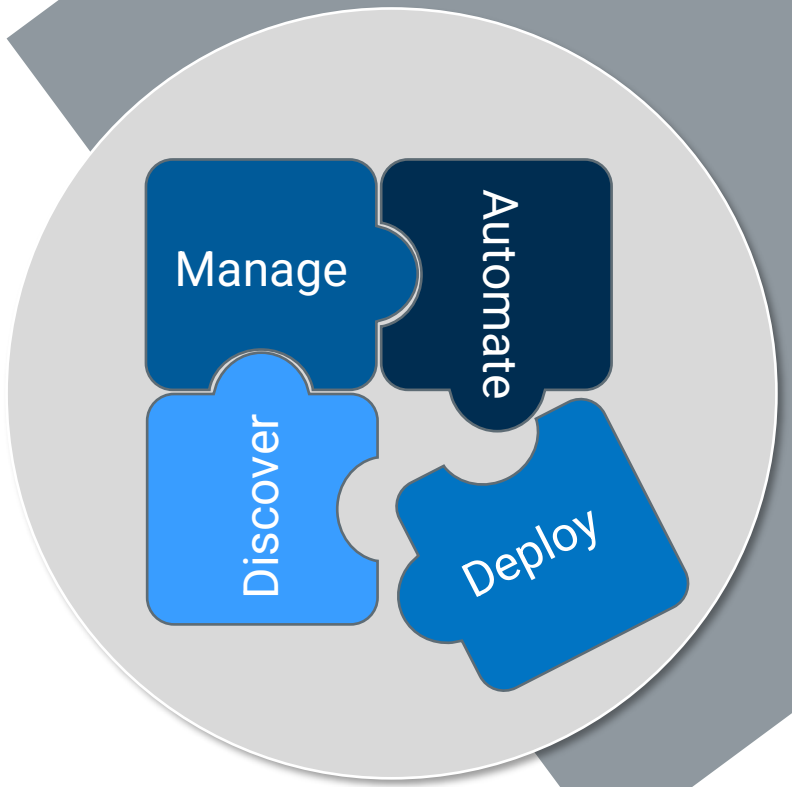
Optimize certificate lifecycle across networks with scalable and automated management tools.

Automate

Facilitate efficient PQC transition through automated workflows, reducing error and operational costs.

Deploy

Enable swift deployment of quantum-safe certificates, ensuring minimal disruption and maximized performance.



DIGICERT PQC ADVISORY PROGRAM

1

Educate

- Stakeholder Engagement & Training

2

Assess

- Full scope risk Assessment

3

Plan

- Integration & implementation roadmaps

4

Deploy

- Testing and Deployment Best Practices

5

Track

- Future-Proofing Enterprise Systems

DIGICERT PQC PLAYGROUND

Complimentary tools to enable integration, interoperability, and performance testing.
DigiCert experts will help you interpret results to create the right strategic plan.

- Generate certificates to test authentication, digital signatures, key encapsulation
- Understand the integration effort required across your environment
- Identify interoperability risks across internal and external providers
- Measure the computing resources required to support PQC at scale

LABS.DIGICERT.COM

PQC READY PLATFORM

digicert® ONE

ENTERPRISE TRUST	DEVICE TRUST	SOFTWARE TRUST	DOCUMENT TRUST	DNS TRUST
PUBLIC TRUST (CERTCENTRAL)	DEVICE TRUST MANAGER	SOFTWARE TRUST MANAGER	DOCUMENT TRUST MANAGER	DNS TRUST MANAGER
PRIVATE TRUST	TRUSTCORE			PERFORMANCE MONITORING
CLM & PKI SERVICES (TRUST LIFECYCLE MANAGER)				

Every Product Within DigiCert's Private Hierarchy Portfolio Supports All three
Post Quantum Cryptography signatures

ITU

IETF

ETSI

SAE INTERNATIONAL

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Accredited Standards Committee X9 Inc. Financial Industry Standards

ISO

CALL TO ACTION

Next week you should:

- Conduct your own research on how large-scale quantum computing will impact public-key cryptography and how it will affect your business.
- Involve your partners and vendors.

In the first three months following this presentation you should:

- Perform an archeological expedition to understand how cryptography is used in your organization
- Identify and prioritize high-value assets for migration

Within six months you should:

- Collaborate with your internal team to create a migration plan
- Share your needs with key vendors to ensure their roadmap aligns

digicert®

kevin.hilscher@digicert.com

Kevin Hilscher
Product Management |
Cybersecurity | IoT | Ex-MSFT