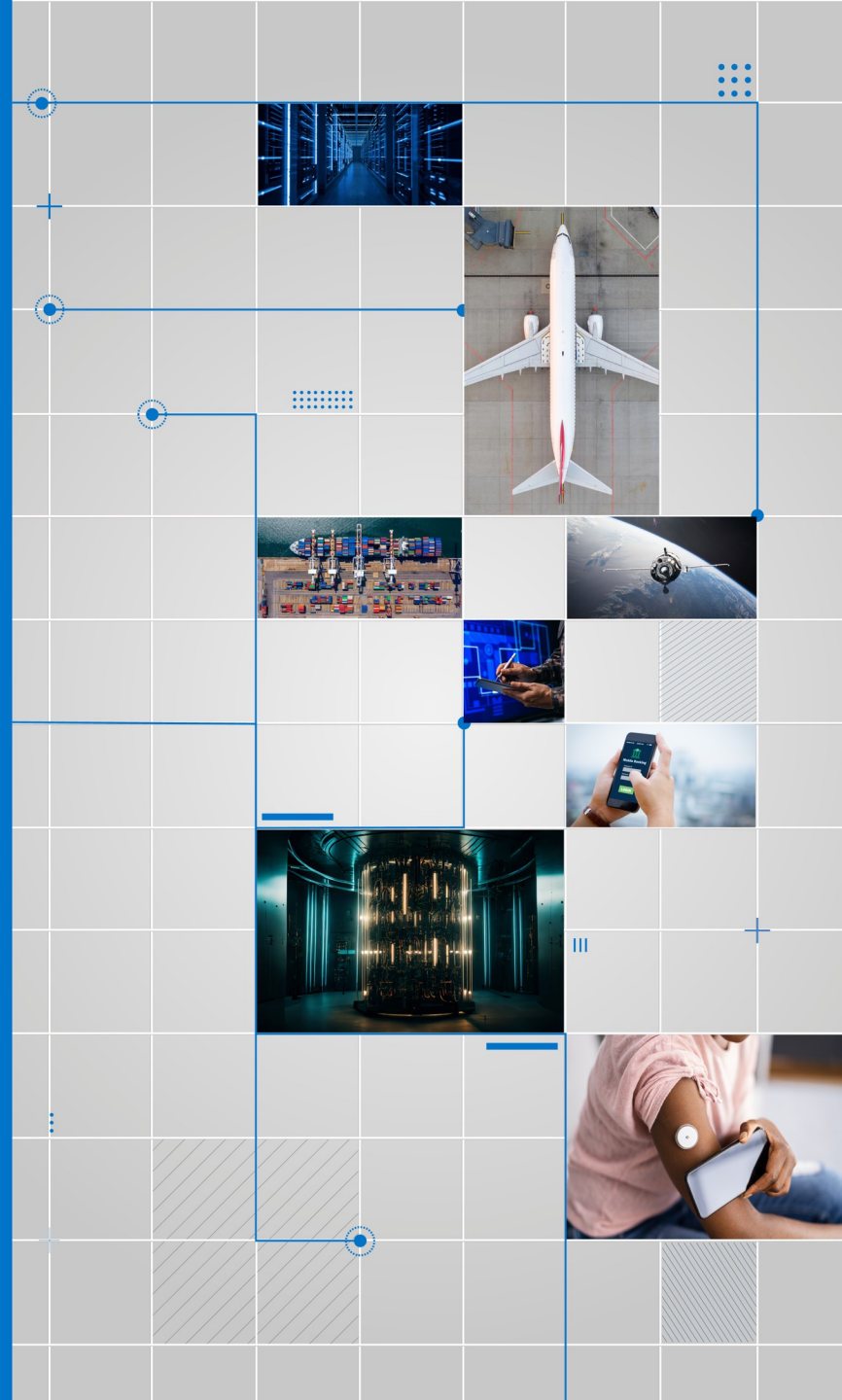
digicert®

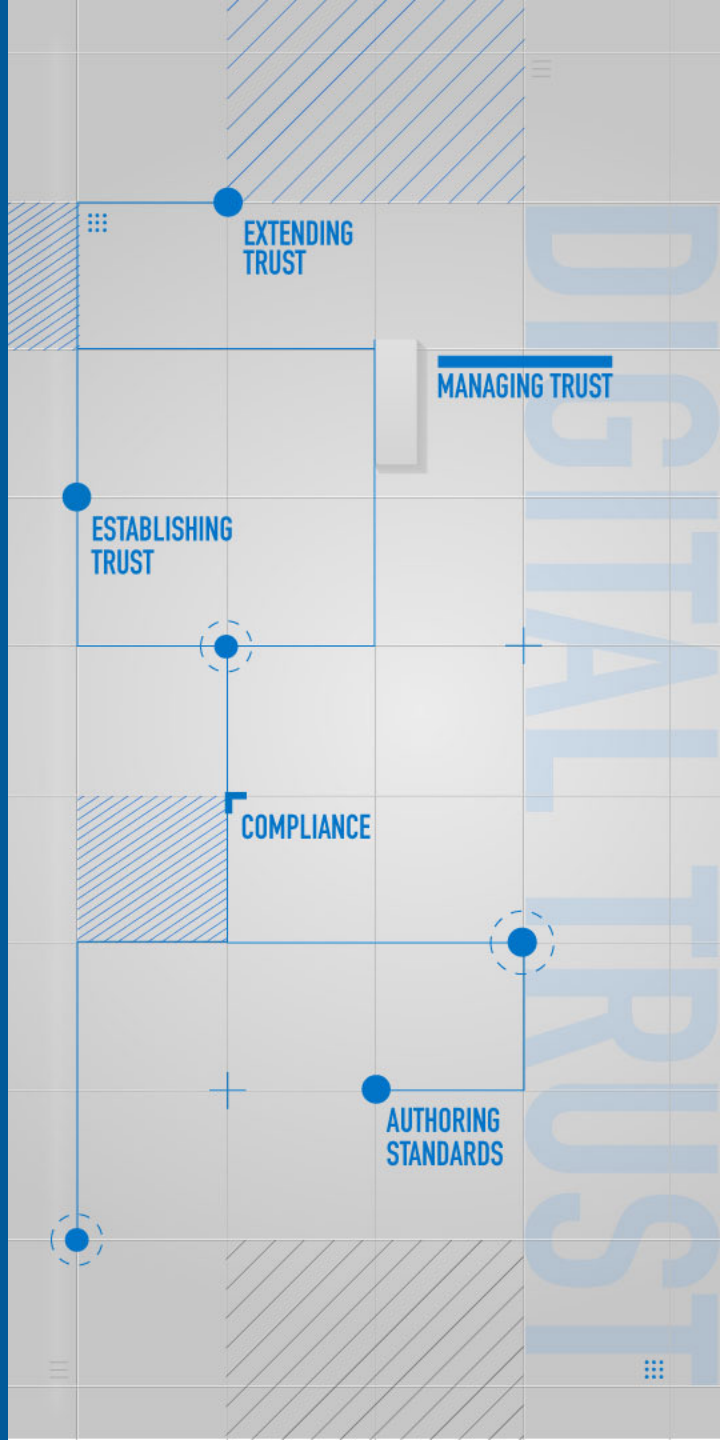
TRUST SUMMIT ROAD SHOW



PREPARING FOR THE FUTURE THREATS WITH TODAY'S SOLUTIONS

A strategic roadmap for preparation against quantum threat

digicert®



AGENDA

01 Introduction

02 Why Post Quantum Crypto (PQC) matters?

03 Current Progress towards quantum safe era

04 Migration Challenges & Crypto Agility

05 DigiCert’s Position

INTRODUCTION

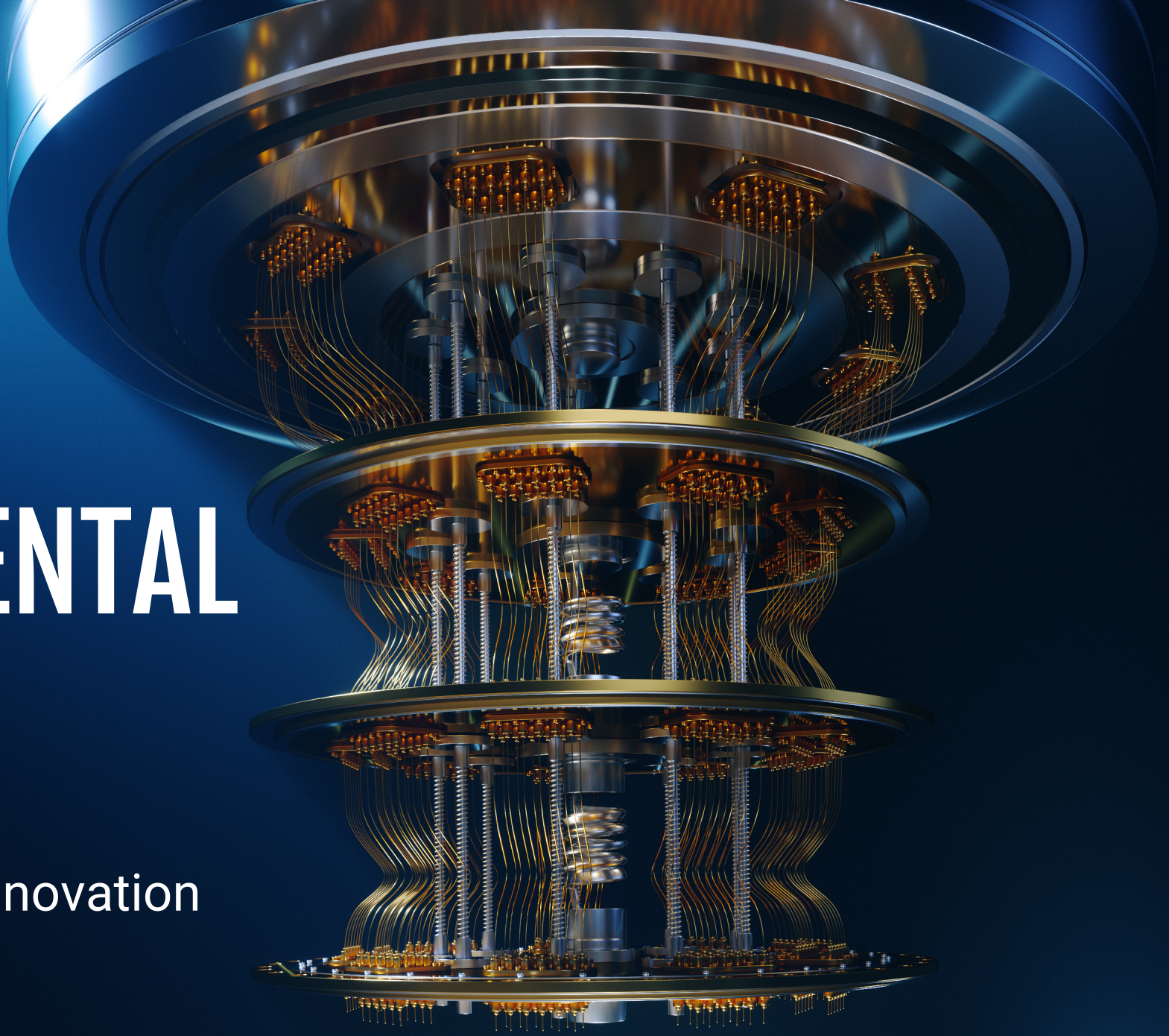
01

WHY POST QUANTUM CRYPTO (PQC) MATTERS?

02

QUANTUM COMPUTING HAS MONUMENTAL POTENTIAL

1000s of times faster
Accelerate discovery and innovation



SECURING TOMORROW, TODAY

The Urgent Shift to Post-Quantum Cryptography

The Inevitable Change

- Internet security's complete reinvention
- Quantum redefines 'if' into 'when'
- Quantum era disrupts current encryption

The Accelerating Threat

- Machine learning fast-tracks quantum
- Quantum threat looms closer, UNEXPECTEDLY
- Quantum error correction closer than ever

The DigiCert Advantage

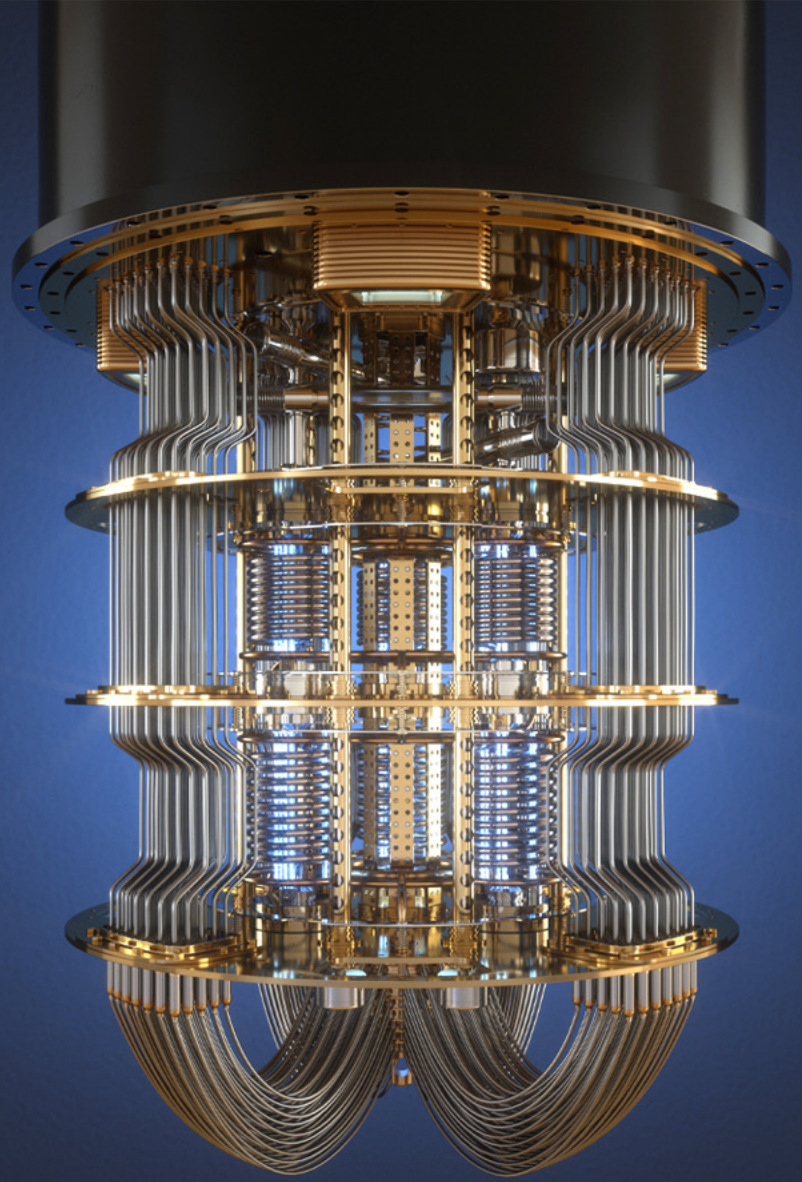
- 5+ years leading quantum research
- Experts in your corner, guiding from industry knowledge
- Proven public & private solutions

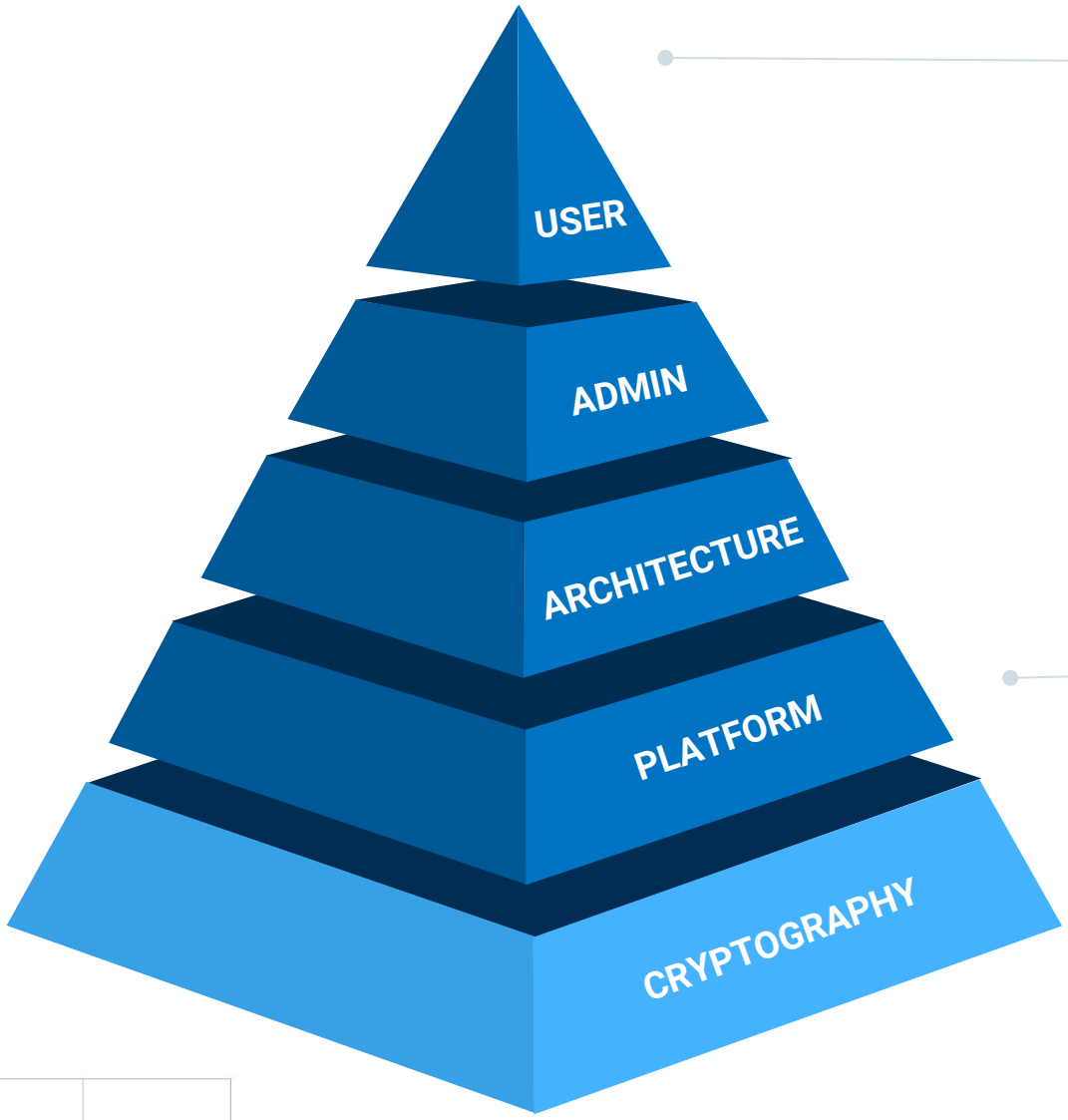
THE QUANTUM EFFECT ON TODAY'S CRYPTOGRAPHY

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





Cause of Security Breaches Today

Quantum: An Unprecedented Threat Looming

THE IMPACT OF QUANTUM COMPUTING

Breaks Security

- Harvest Now; Decrypt Later
- Sensitive Data Exposed
- Encryption Keys Cracked
- Tampered Documents & Software

Upends Business Plans

- Disrupted Supply Chains
- Strategic Plans Unveiled
- Mandatory System Overhauls

Cost & Resource Implications

- Surge in IT Spending
- Training Workforces
- Resource Redistribution

Solution Takes Years

- Not a “drop-in” fix
- Requires architecture changes
- Potential interoperability issues

WHY NOW

Quantum & AI = Act Now

- Emerging tech accelerates security threats
- Proactive measures are critical now

Compliance Readiness

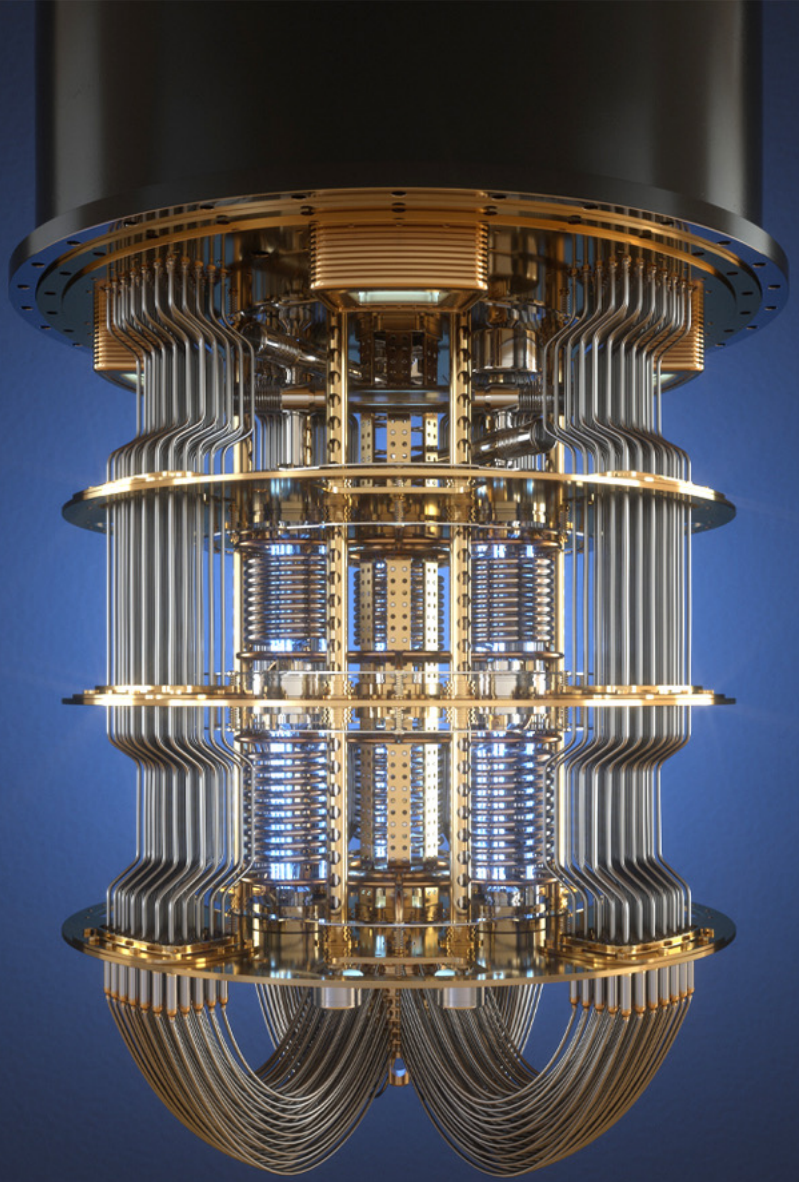
- Regulations evolve faster than adoptions
- Stay at-pace with early compliance

Future vulnerabilities, today’s risk

- Tomorrow’s threats need today's solutions
- Anticipate, don't wait for risks

Keep your edge

- Innovate and secure proactively

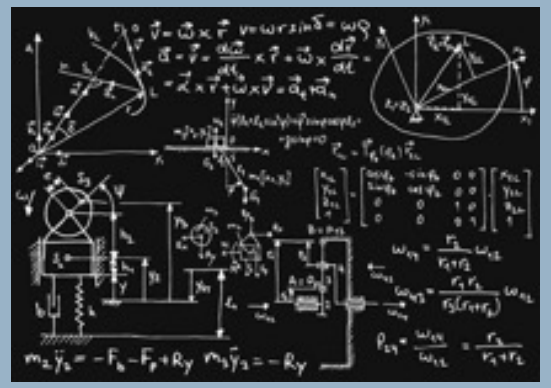


CURRENT PROGRESS TOWARDS QUANTUM SAFE ERA

03

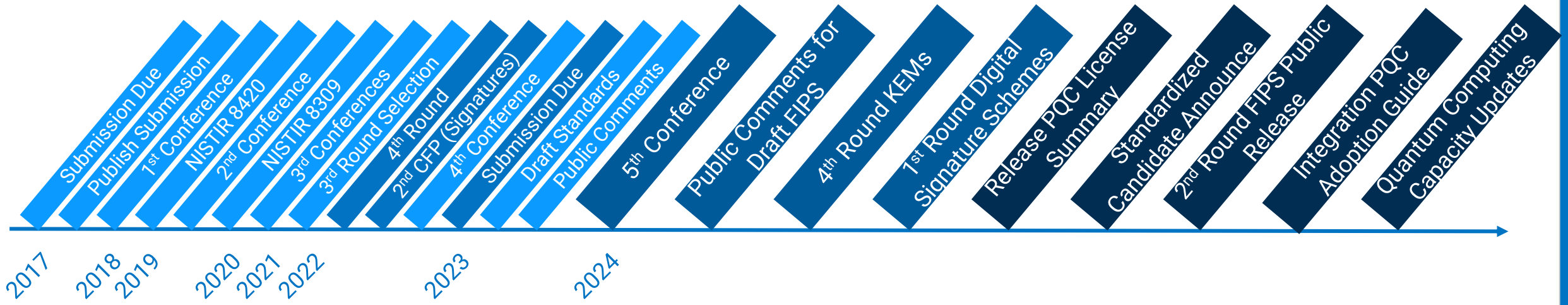
PATHWAYS TO QUANTUM SAFETY

Quantum Key Distribution



Quantum-Safe Cryptography

AN ACCELERATING PQC REGULATORY TIMELINE



Past

- NIST Process
- Executive Order
- NCCoE Migration
- Test Labs

Present (2024-2025)

- Implementing Protocols Now
- Prioritizing Immediate PQC Adoption
- Active Engagement in PQC Transition
- Urgent Integration of PQC Standards

Future

- Staying compliant
- Securing data/devices for the long run
- Staying crypto-agile during PQC era

QUANTUM-SAFE ASYMMETRIC ALGORITHMS (TABLE 1 OF 2)

Scheme	Family	Type	Secret Key (Octets)	Public Key (Octets)	Signature (Octets)	Ciphertext (Octets)	Shared Secret (Octets)
LMS	Stateful Hash-based	Signature	56 + (2,064 - 2,147,483,664)	32	1,296 - 9,328	–	–
XMSS	Stateful Hash-based	Signature	104 + (65,568 - 67,108,896)	32	2,500 – 2,820	–	–
SPHINCS	Stateless Hash-based	Signature	64 - 128	32 - 64	8,080 - 49,216		
BIKE	Code-based	KEM	3,194 - 11,749	1,478 - 11,217	–	1,478 - 11,217	32
Classic McEliece	Code-based	KEM	6,452 - 14,080	261,120 - 1,357,824	–	128 - 240	32
HQC	Code-based	KEM	40	3,125 - 8,897	–	6,234 - 17,777	64
LEDAcrypt	Code-based	KEM	24 - 40	1,872 - 8,520	–	1,872 - 4,616	32 - 64
NTS-KEM	Code-based	KEM	9,248 - 19,922	319,488 - 1,419,704	–	128 - 253	32
ROLO	Code-based	KEM	40	465 - 2,493	–	465 - 2,621	40 - 64
RQC	Code-based	KEM	40	853 - 2,284	–	1,690 - 4,552	64
Kyber	Lattice-based	KEM	1,632 – 3,168	800 – 1,568	–	736 – 1,568	32
FrodoKEM	Lattice-based	KEM	19,888 - 43,088	9,616 - 21,520	–	9,720 - 21,623	16 - 32
LAC	Lattice-based	KEM	1,056 - 2,080	544 - 1,056	–	712 - 1,424	32
NewHope	Lattice-based	KEM	1,888 - 3,680	928 - 1,824	–	1,120 - 2,208	32

QUANTUM-SAFE ASYMMETRIC ALGORITHMS (TABLE 2 OF 2)

Scheme	Family	Type	Secret Key (Octets)	Public Key (Octets)	Signature (Octets)	Ciphertext (Octets)	Shared Secret (Octets)
NTRU	Lattice-based	KEM	935 - 1,592	699 - 1,230	–	699 - 1,230	32
NTRUPrime	Lattice-based	KEM	1,125 - 1,999	897 - 1,322	–	897 - 1,184	32
Round5	Lattice-based	KEM	16 - 32	445 - 14,264	–	549 - 14,288	16 - 32
SABER	Lattice-based	KEM	1,568 - 3,040	672 - 1,312	–	736 - 1,472	32
Three Bears	Lattice-based	KEM	40	804 - 1,584	–	917 - 1,697	32
Dilithium	Lattice-based	Signature	96 - 2096	896 – 1,760	1,387 – 3,366	–	–
Falcon	Lattice-based	Signature	4,097 – 8,193	897 – 1,793	618 – 1,233	–	–
qTesla	Lattice-based	Signature	1,216 - 12,352	1,504 - 38,432	1,376 - 5,920	–	–
GeMSS	Multivariate-based	Signature	13,415 - 77,712	36,0643 - 3,210,845	33 - 75	–	–
LUOV	Multivariate-based	Signature	32	5,120 – 77,312	311 – 4,390	–	–
MQDSS	Multivariate-based	Signature	16 – 24	46 – 64	20,854 – 43,728	–	–
Rainbow	Multivariate-based	Signature	95,232 - 1,256,551	152,576 - 1,746,432	64 - 204	–	–
SIKE	Supersingular Isogeny-Based	KEM	374 - 644	330 - 564	–	346 - 596	16 - 32
Picnic	Zero-Knowledge Proof/MPC	Signature	16 - 32	32 - 64	13,802 - 209,506	–	–

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	Proposed Name-Released
Key encapsulation for secure communications	Secure identities and electronic signatures	Security for long term use cases	Security for fast transaction processing

DIGICERT PQC PERFORMANCE TESTBED

key sizes	p11_keygen_duration (secs)	p11_sign_duration (secs)	signature len (bytes)	publicKey len bytes
SphincsSha2_128F	0	2	17088	32
SphincsSha2_128S	3	26	7856	32
SphincsSha2_192F	0	4	35664	48
SphincsSha2_192S *	5	80	16224	48
SphincsSha2_256F *	0	8	49856	64
SphincsSha2_256S *	4	84	29792	64
SphincsShake_128F	1	17	17088	32
SphincsShake_128S*	48	339	7856	32
SphincsShake_192F*	1	29	35664	48
SphincsShake_192S*	72	615	16224	48
SphincsShake_256F*	3	55	49856	64
SphincsShake_256S*	45	500	29792	64

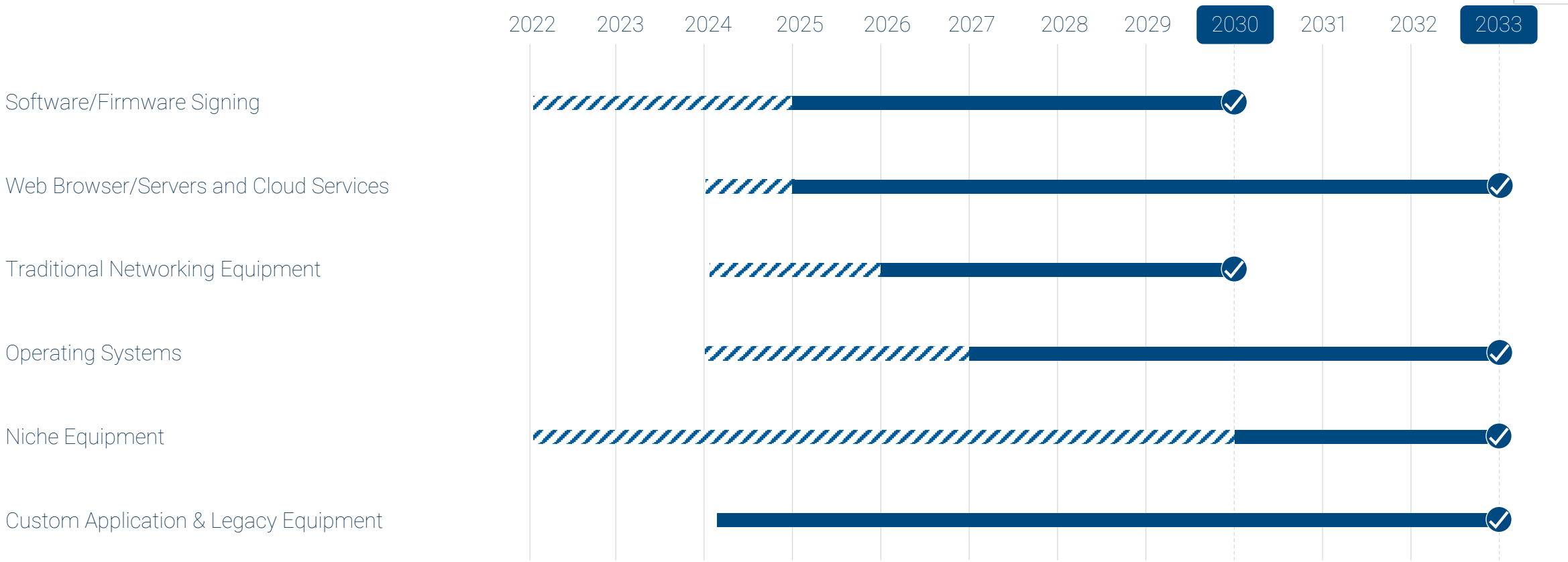
key sizes	p11_keygen_duration (msecs)	p11_sign_duration (msecs)	signature len (bytes)	publicKey len
MLDSA-44	661	1878	2420	1312
MLDSA-65	668	1875	3293	1952
MLDSA-87	705	1931	4595	2592

MIGRATION CHALLENGES & CRYPTO AGILITY

04

COMMERCIAL TRANSITION TIMELINE

CNSA 2.0 Adoption



Visual adapted from CNSA *Announcing the Commercial National Security Algorithm Suite 2.0, Figure 1: Transition timeline*

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

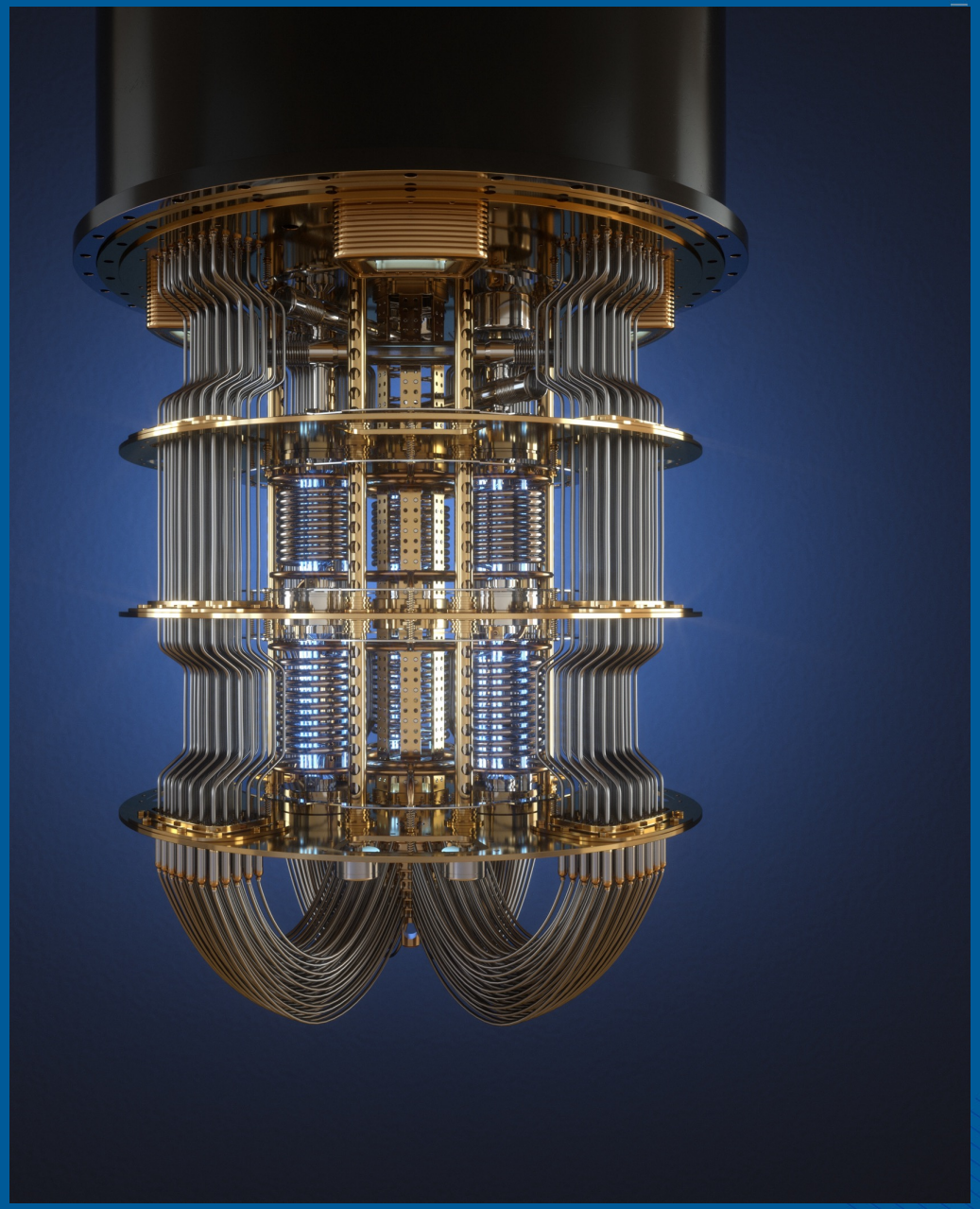
NIST ON CRYPTO AGILITY

"As the replacements for currently standardized public key algorithms are not yet ready, a focus **on maintaining crypto agility is imperative.**

Until new quantum-resistant algorithms are standardized, **agencies should continue to use the recommended algorithms currently specified in NIST standards."**

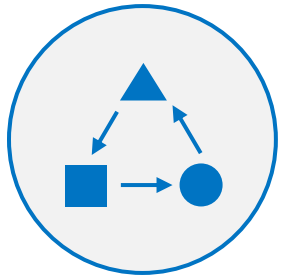
- "Report on Post-Quantum Cryptography", NIST, April 2016

NIST
National Institute of
Standards and Technology



THE CHALLENGE

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



Maintain
Interoperability

Migrate Critical
Systems Faster

Reduce
Switching Costs

HOW ARE SECURE COMMUNICATIONS VULNERABLE?

Secure Communication Protocol

Shor's Algorithm breaks current public-key algorithms

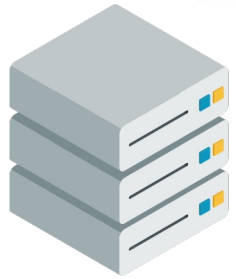
Key Establishment

Authentication

Grover's Algorithm weakens symmetric encryption (square root)

Encrypted Transmissions

A HARVEST & DECRYPT ATTACK ON VPN

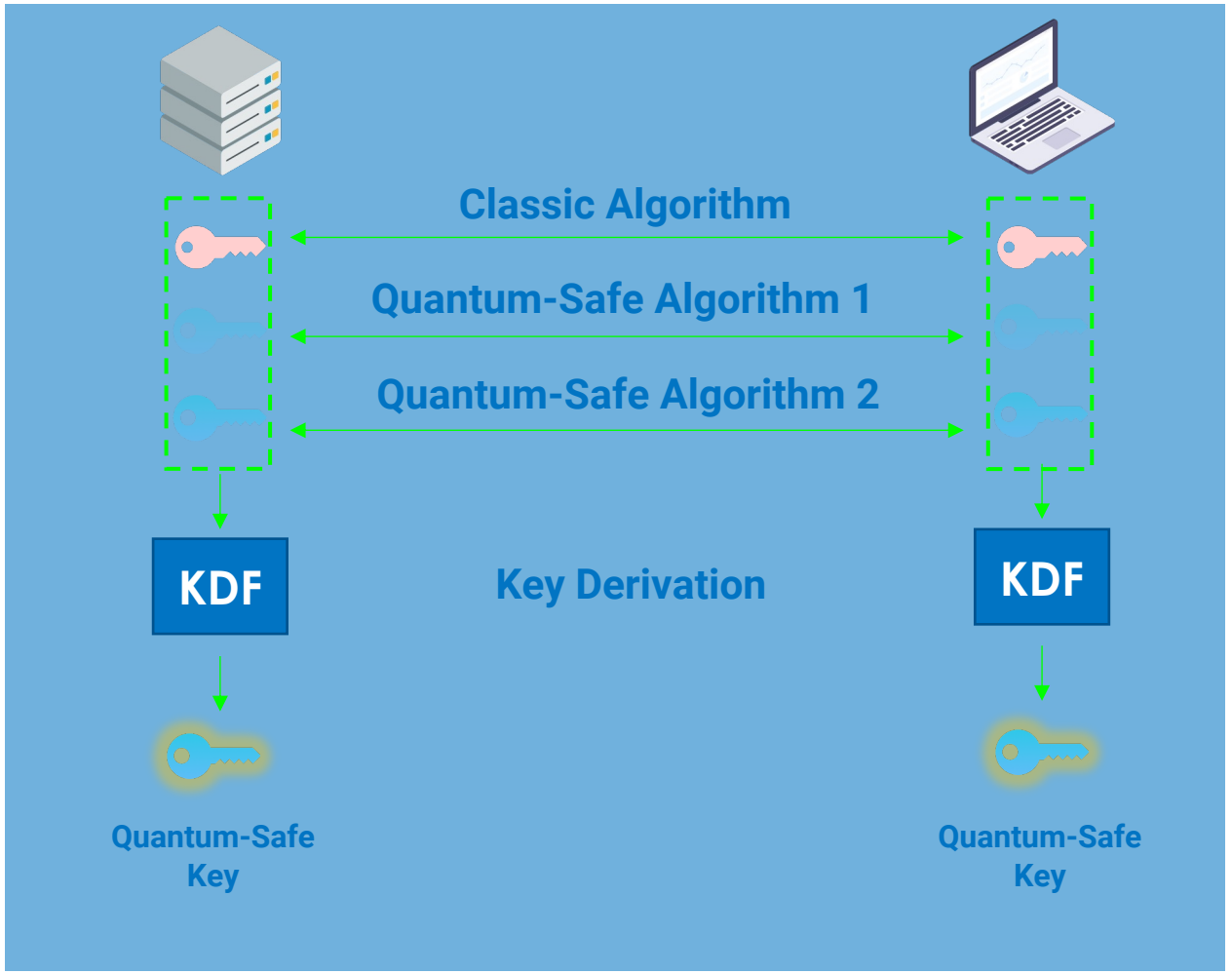


VPN Session

Handshake | **Data Exchange**

Quantum attack using Shor's algorithm → **Key Establishment** → Obtain private key → **Ciphertext** → Decrypt using extracted key

HYBRID KEY ESTABLISHMENT



THE MIGRATION CHALLENGE

Key Establishment vs. Authentication

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

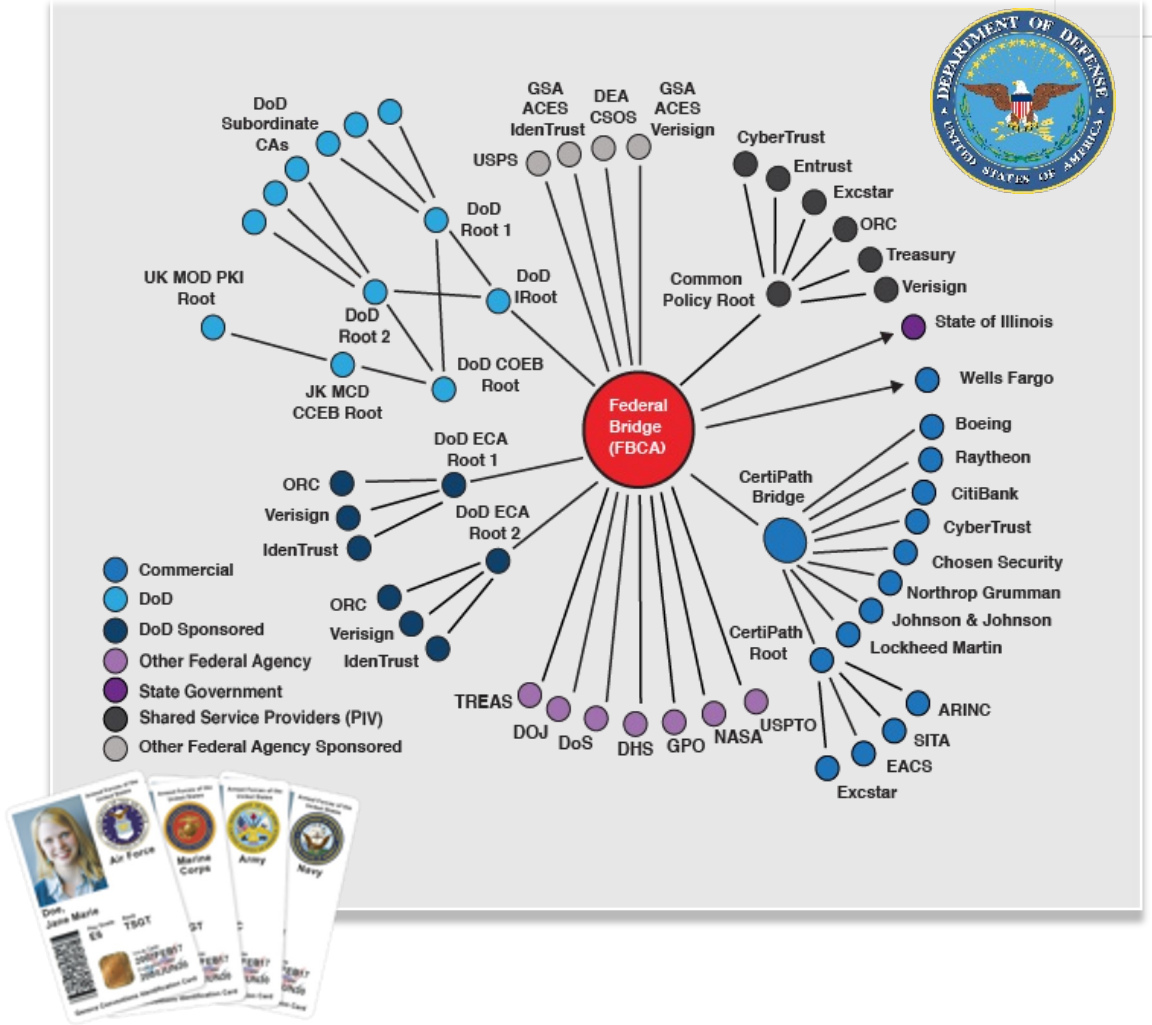
1. Use quantum-safe key transport or key agreement algorithms
2. Use hybrid keys, a mix of both classic and quantum-safe algorithms

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.

DOD PKI MIGRATION

There's more than 4.5 million active users in the DoD identity management system.

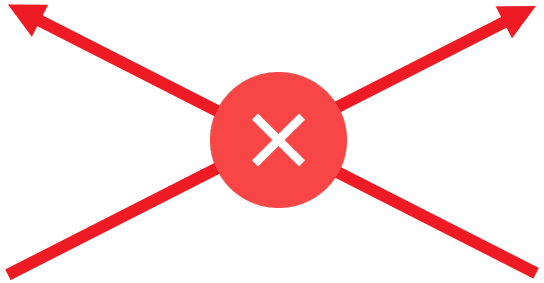
Creating a quantum-safe duplicate infrastructure is time-consuming and cost prohibitive.



CERTIFICATES SUPPORT A SINGLE ALGORITHM

Classical

Classical



User/server needs to select which certificate to use

PKI management costs increase

Quantum-safe

Quantum-safe

AGILITY IN UNCERTAINTY

Quantum ready means staying nimble and responsive as quantum technology unfolds.

ROAD TO CRYPTO AGILITY

Discover

Identify and assess quantum vulnerabilities across your digital certificate ecosystem.

Manage

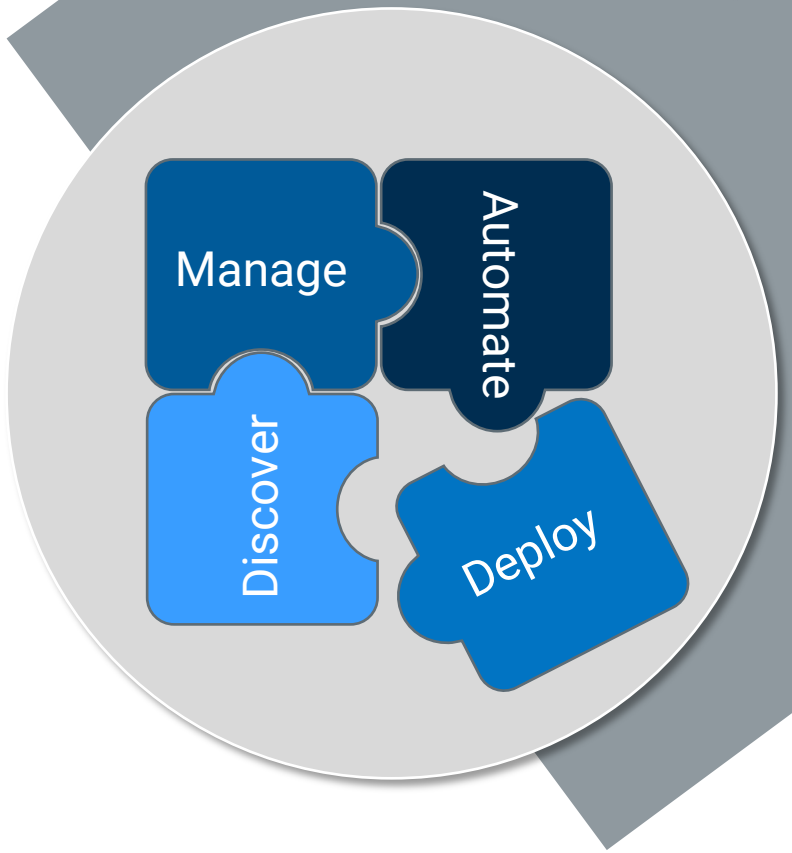
Optimize certificate lifecycle across networks with scalable and automated management tools.

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'S POSITION

05

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)	IOT TRUST MANAGER	SOFTWARE TRUST MANAGER	DOCUMENT TRUST MANAGER	DNS TRUST MANAGER
PRIVATE TRUST	TRUSTCORE			PERFORMANCE MONITORING
CLM & PKI SERVICES (TRUST LIFECYCLE MANAGER)				

Quantum-safe algorithms are the key to future-proof security.

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

APPLY WHAT YOU HAVE LEARNED TODAY

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

In the first three months following this presentation you should:

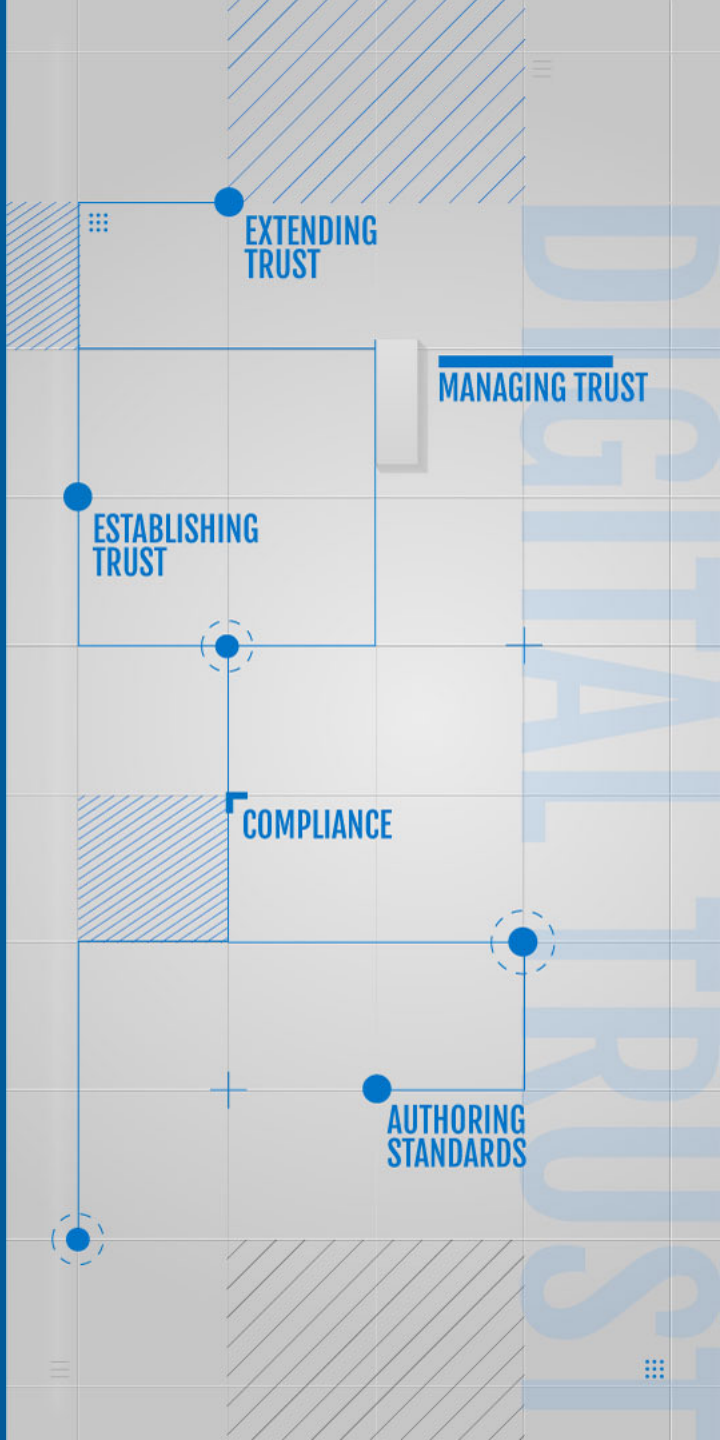
- Perform an archeological expedition to understand how cryptography is used in your organization
- Identify and prioritize high-value assets for migration

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®

avesta@digicert.com



digicert®

TRUST SUMMIT ROAD SHOW