Post-Quantum

Cryptography Conference

Moving toward a Quantum Security Maturity Index

Tom Patterson

Global Lead, Quantum Security at Accenture

Considerations on Establishing a

Post Quantum Security Maturity Index

Tom Patterson

Global Lead , Accenture Quantum Security

PKI Consortium
Amsterdam, Netherlands
8 November 2023

PKI Consortium

accenture

Outline

01 Quantum Security Overview

02 Quantum Security Considerations

03 Quantum Security Regulations and Guidance

04 The Role of PKI in Quantum Defense

05 Considering a Maturity Index

06 Report from FS/ISAC Denver March 2023 Roundtable

07 Next Steps

The Risk to Data in Motion Is Real

Q Day is Coming

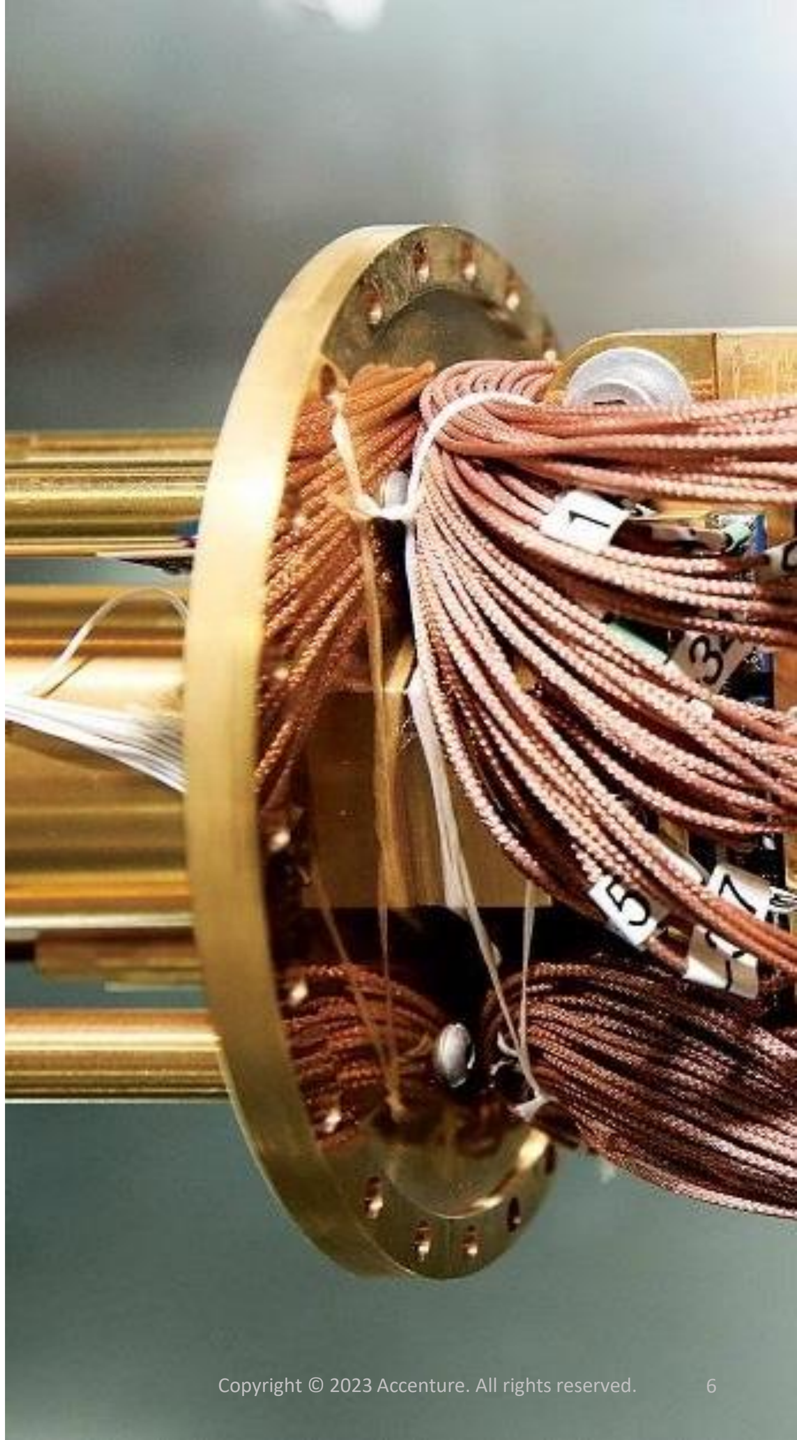
Q Day is Coming

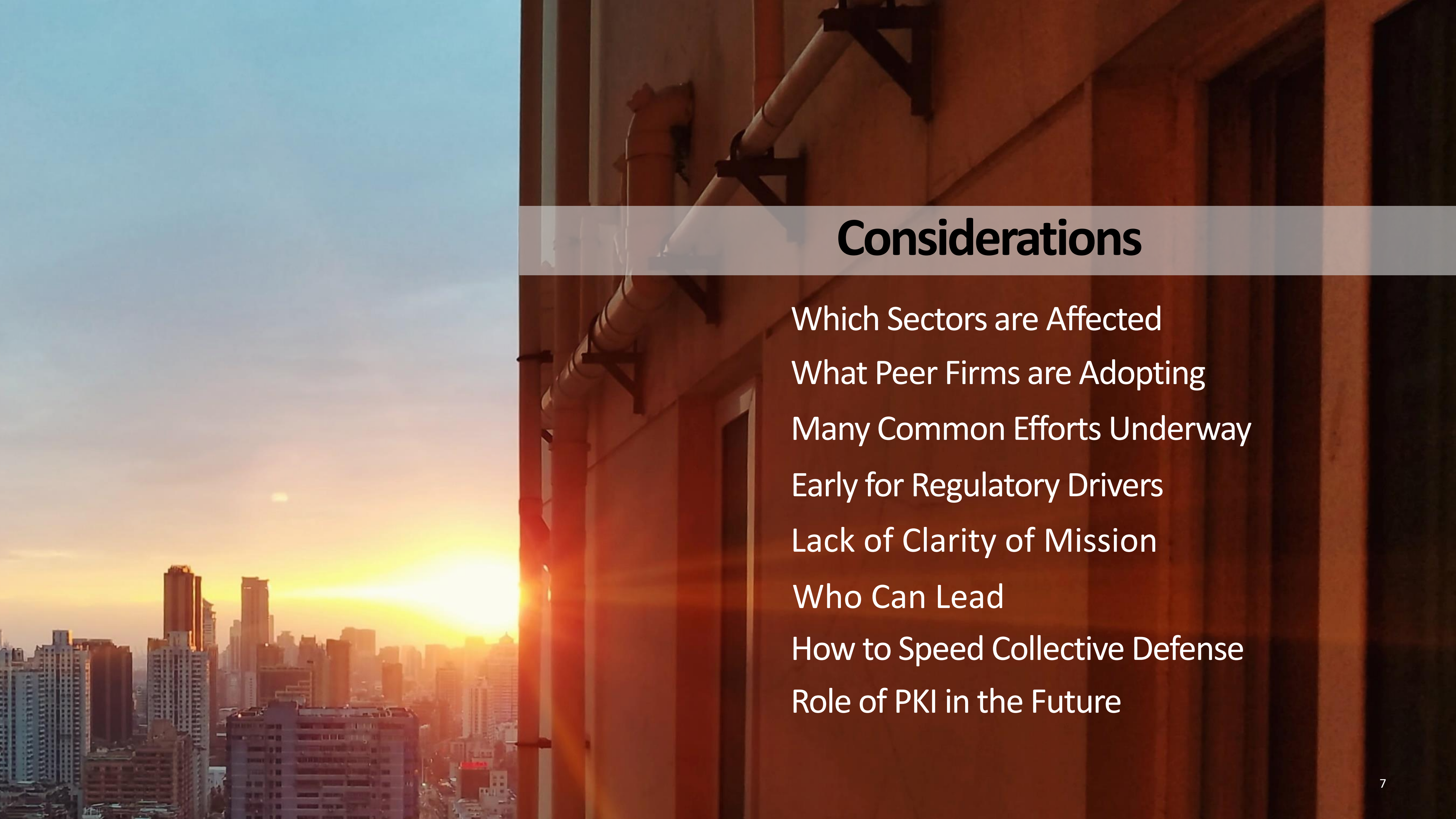
It’s Just Math

5 Things You Need To Know

Quantum Security | Overview

Bits to Qubits	1	On, Off, and Everything in Between Superposition and Entanglement
Quantum Computing	2	Factoring is Easy
Counting Qubits	3	2 – 433 – 1000 … 4099 – and noise
SNDL and Hybrid	4	Shorten the Event Horizon
PNRL	5	Prepare Now Relax Later

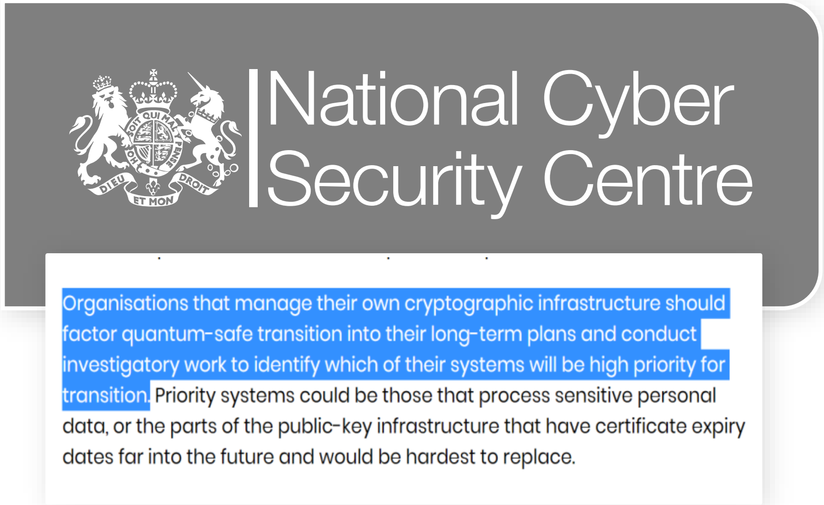




Considerations

- Which Sectors are Affected
- What Peer Firms are Adopting
- Many Common Efforts Underway
- Early for Regulatory Drivers
- Lack of Clarity of Mission
- Who Can Lead
- How to Speed Collective Defense
- Role of PKI in the Future

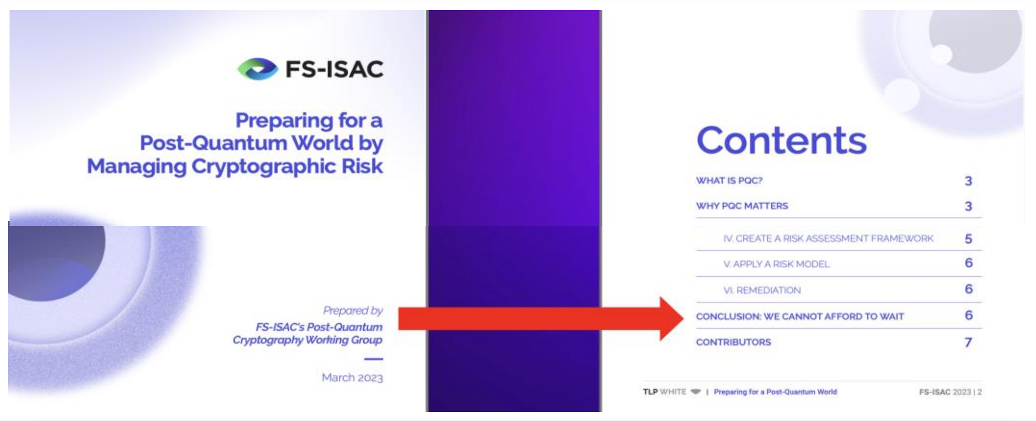
Current Guidance



National Cyber Security Centre

Organisations that manage their own cryptographic infrastructure should factor quantum-safe transition into their long-term plans and conduct investigatory work to identify which of their systems will be high priority for transition. Priority systems could be those that process sensitive personal data, or the parts of the public-key infrastructure that have certificate expiry dates far into the future and would be hardest to replace.

Quantum Computing Preparedness Act (H.R.7535)



FS-ISAC

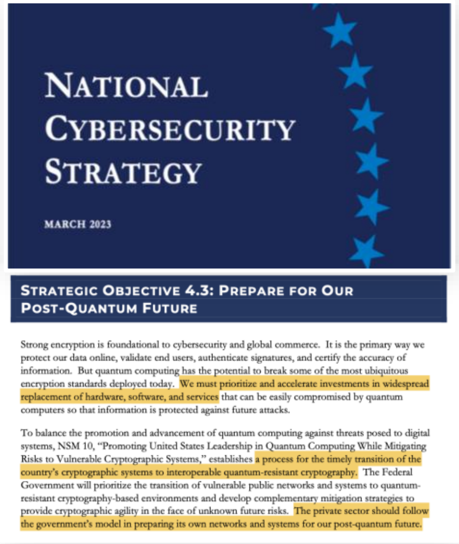
Preparing for a Post-Quantum World by Managing Cryptographic Risk

Prepared by FS-ISAC's Post-Quantum Cryptography Working Group

March 2023

Contents

TLP WHITE | Preparing for a Post-Quantum World FS-ISAC 2023 | 2



NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

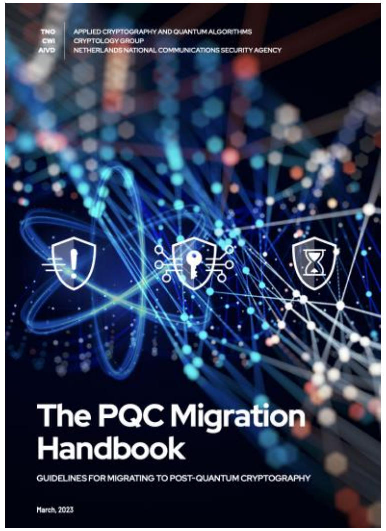
STRATEGIC OBJECTIVE 4.3: PREPARE FOR OUR POST-QUANTUM FUTURE

Strong encryption is foundational to cybersecurity and global commerce. It is the primary way we protect our data online, validate end users, authenticate signatures, and certify the accuracy of information. But quantum computing has the potential to break some of the most ubiquitous encryption standards deployed today. We must prioritize and accelerate investments in widespread replacement of hardware, software, and services that can be easily compromised by quantum computers so that information is protected against future attacks.

To balance the promotion and advancement of quantum computing against threats posed to digital systems, NSM 10, "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," establishes a process for the timely transition of the country's cryptographic systems to interoperable quantum-resistant cryptography. The Federal Government will prioritize the transition of vulnerable public networks and systems to quantum-resistant cryptography-based environments and develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks. The private sector should follow the government's model in preparing its own networks and systems for our post-quantum future.

White House Executive Orders

- NSM-8
- NSM-10

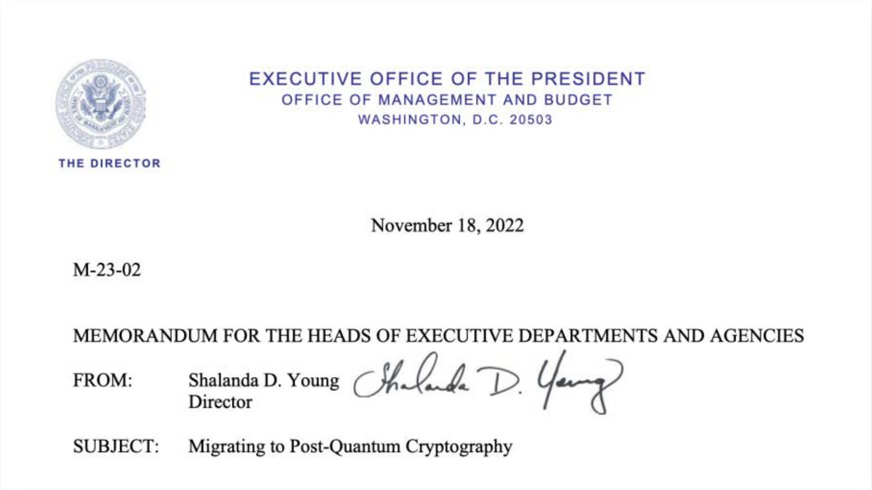


TNO | APPLIED CRYPTOGRAPHY AND QUANTUM ALGORITHMS
CWI | CRYPTOLOGY GROUP
AIVD | NETHERLANDS NATIONAL COMMUNICATIONS SECURITY AGENCY

The PQC Migration Handbook

GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY

March 2023



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

Accredited Standards Committee X9 Inc.

Financial Industry Standards

NIST

National Institute of Standards and Technology

Quantum Defense

across the Financial Sector

Strategy

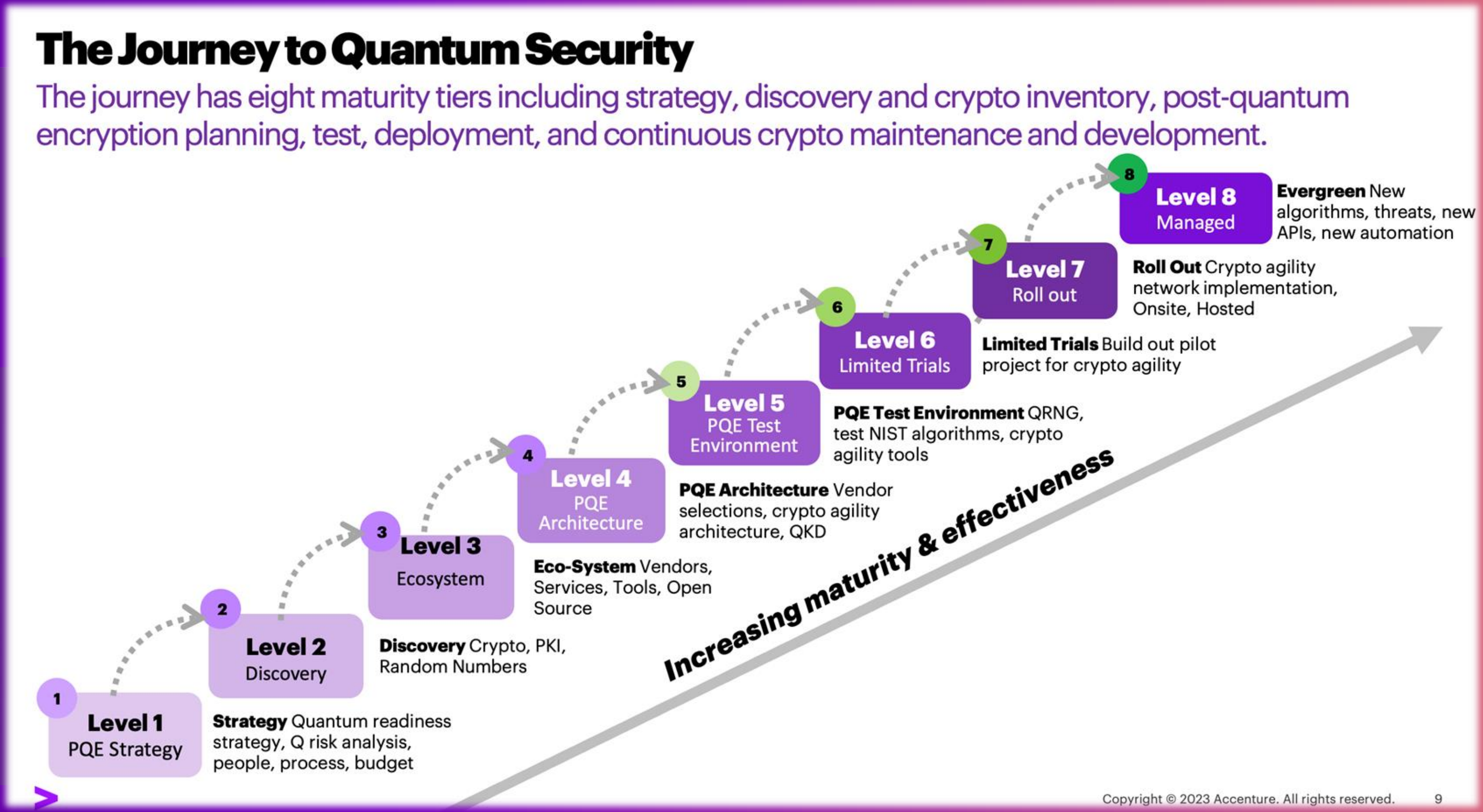
- Education
- Ecosystem
- Budgeting

Discovery

- Manual
- Tools
- AI

Remediation

- Post Quantum Crypto
- Crypto Agility
- Quantum Key Distribution



The Journey to Quantum Security

The journey has eight maturity tiers including strategy, discovery and crypto inventory, post-quantum encryption planning, test, deployment, and continuous crypto maintenance and development.

1 **Level 1** PQE Strategy — **Strategy** Quantum readiness strategy, Q risk analysis, people, process, budget

2 **Level 2** Discovery — **Discovery** Crypto, PKI, Random Numbers

3 **Level 3** Ecosystem — **Eco-System** Vendors, Services, Tools, Open Source

4 **Level 4** PQE Architecture — **PQE Architecture** Vendor selections, crypto agility architecture, QKD

5 **Level 5** PQE Test Environment — **PQE Test Environment** QRNG, test NIST algorithms, crypto agility tools

6 **Level 6** Limited Trials — **Limited Trials** Build out pilot project for crypto agility

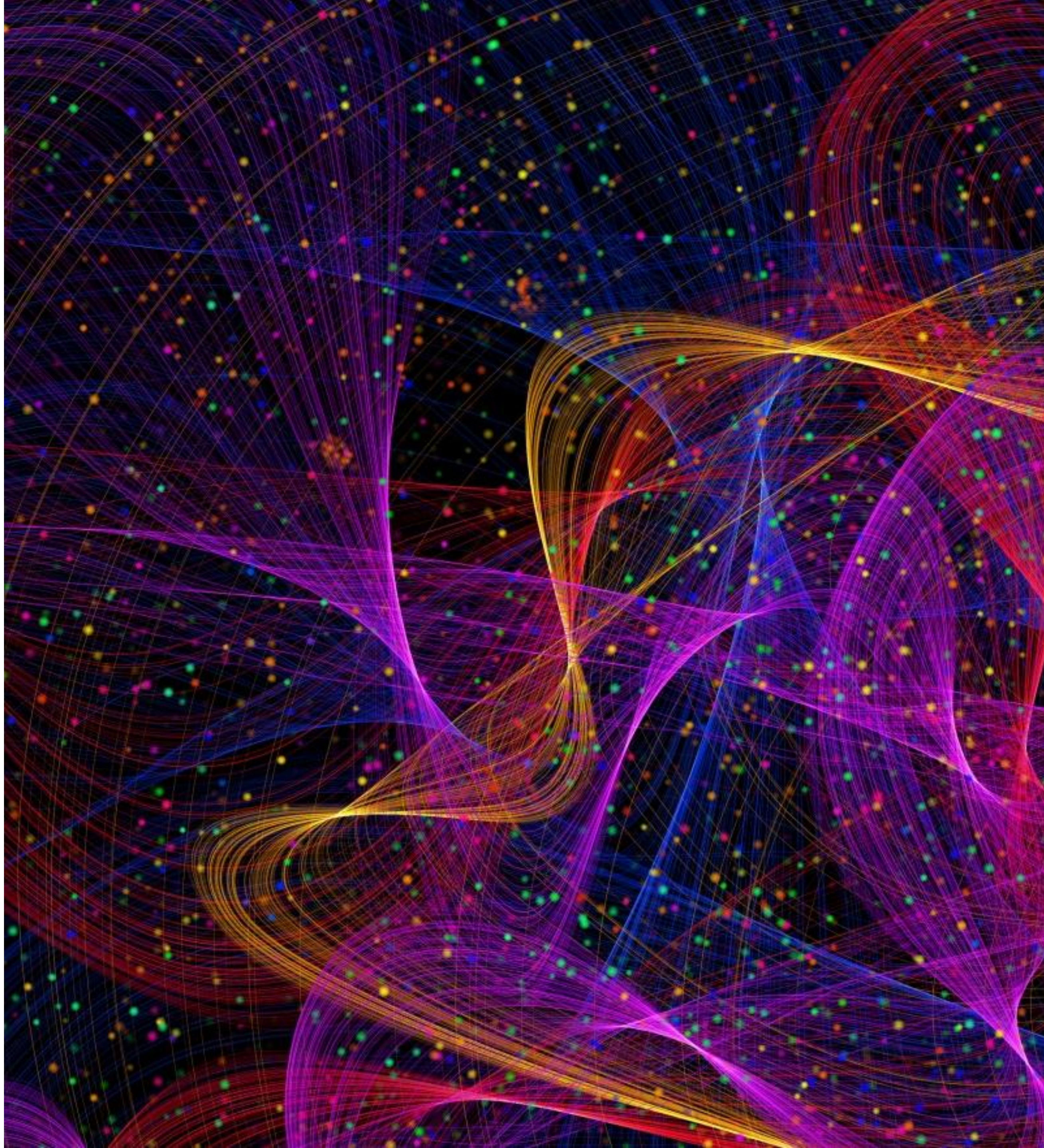
7 **Level 7** Roll out — **Roll Out** Crypto agility network implementation, Onsite, Hosted

8 **Level 8** Managed — **Evergreen** New algorithms, threats, new APIs, new automation

The Role of

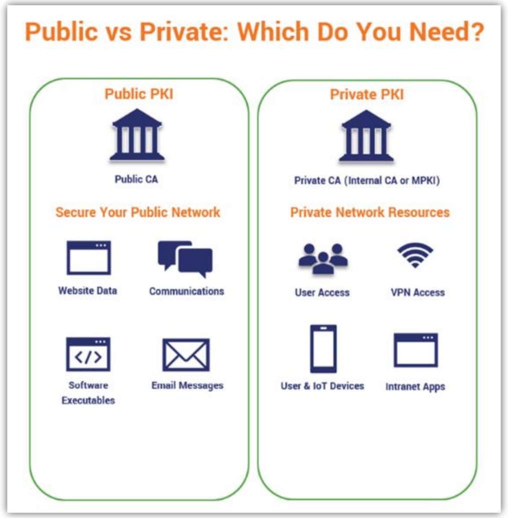
PKI

in the Collective Defense

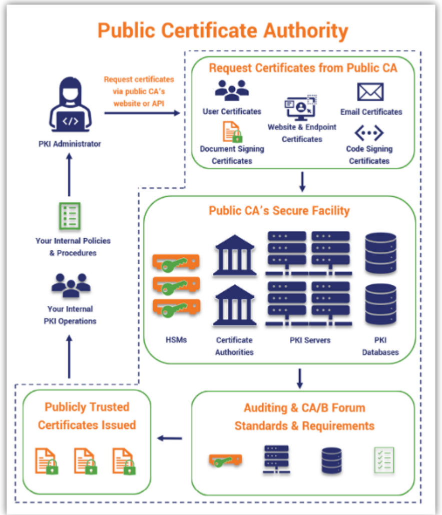


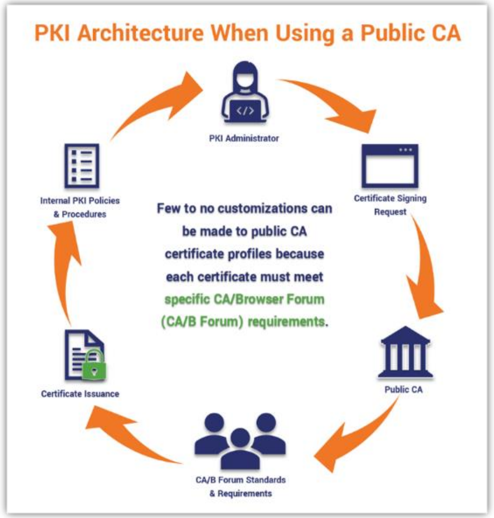
Public Key Infrastructure – the highly sophisticated chain on trust established over many years.

Business are impacted dramatically, because they need to rely on third parties for Public PKI and they need to update their own Private PKI otherwise their user ids, access points, and applications will be vulnerable.

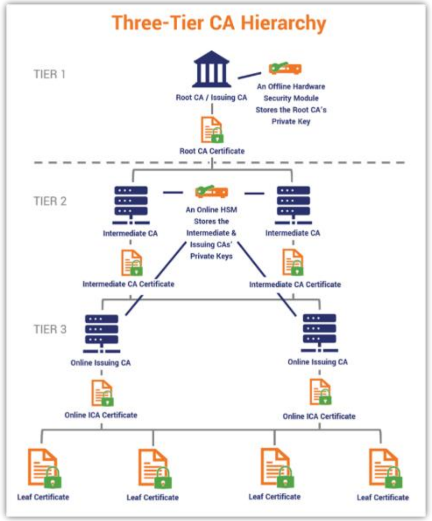


There are internal and external PKI infrastructures.

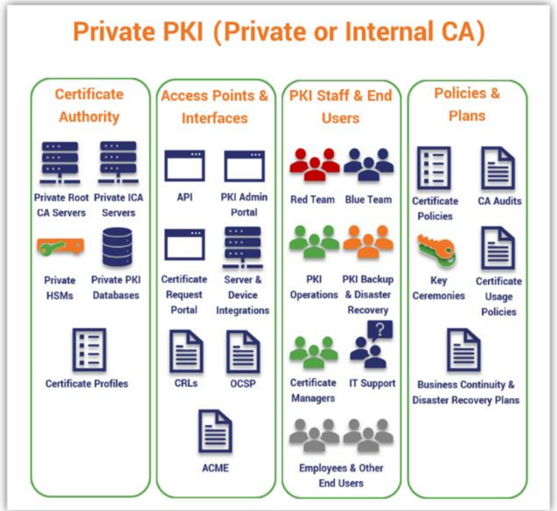

Public Certificate Authority
PKI Administrator
Request certificates via public CA's website or API
Request Certificates from Public CA
User Certificates
Website & Endpoint Certificates
Email Certificates
Document Signing Certificates
Code Signing Certificates
Your Internal Policies & Procedures
Your Internal PKI Operations
Public CA's Secure Facility
HSMs
Certificate Authorities
PKI Servers
PKI Databases
Publicly Trusted Certificates Issued
Auditing & CA/B Forum Standards & Requirements


PKI Architecture When Using a Public CA
PKI Administrator
Certificate Signing Request
Public CA
CA/B Forum Standards & Requirements
Certificate Issuance
Internal PKI Policies & Procedures
Few to no customizations can be made to public CA certificate profiles because each certificate must meet specific CA/Browser Forum (CA/B Forum) requirements.

The process to issue, renew, and update certificates is well established, but is laborious, complicated, and business critical.

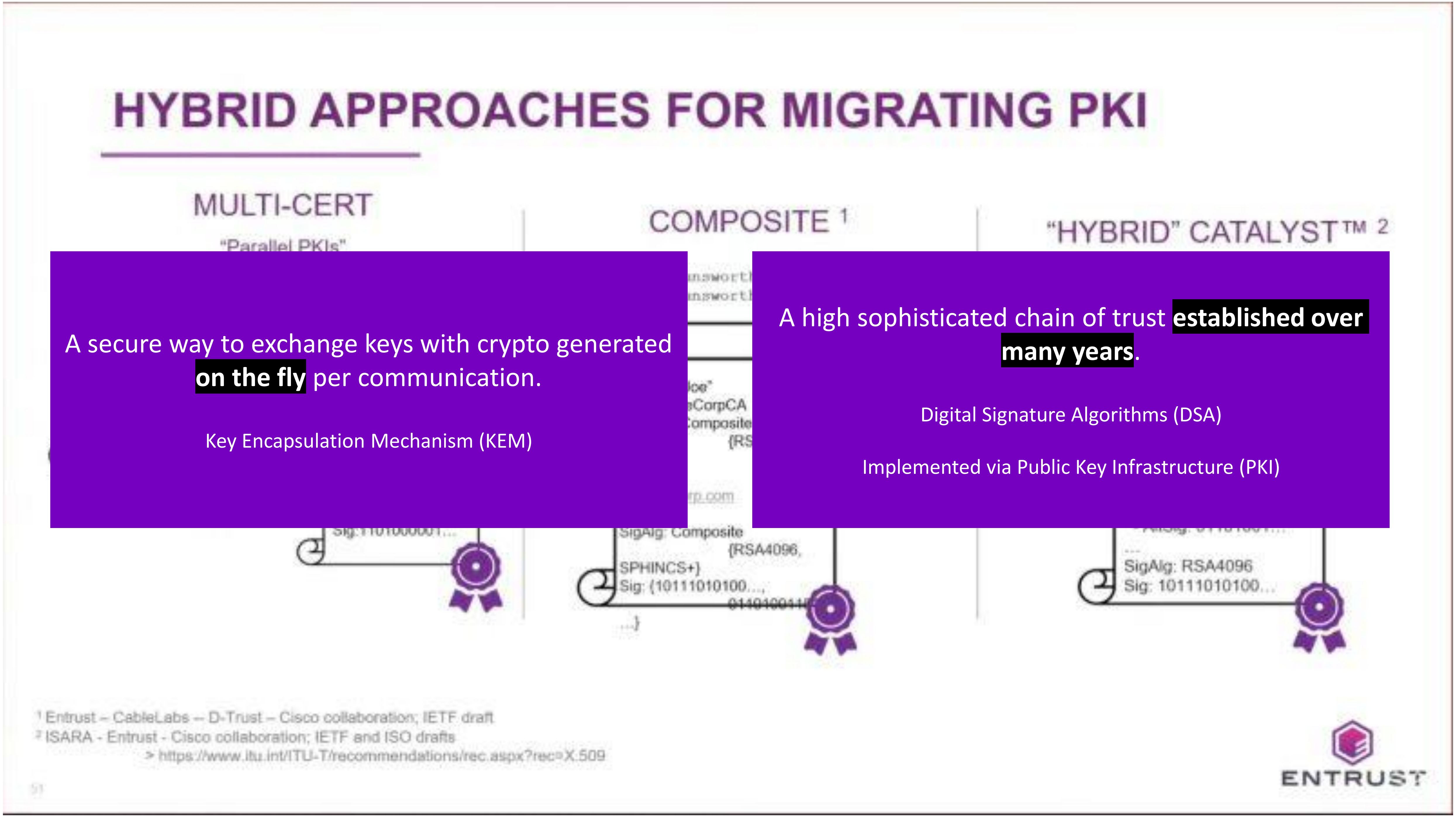


Changes take time to ripple down the chains of trust.



It requires a dedicated team within the security organization to manage and operate PKI.

Source: https://www.thesslstore.com/blog/pki-architecture-fundamentals-of-designing-a-private-pki-system/



HYBRID APPROACHES FOR MIGRATING PKI

MULTI-CERT

"Parallel PKIs"

Sig: 1101000001...

COMPOSITE [1]

nsworth

nsworth

Joe"

eCorpCA

Composite

{RS

rp.com

SigAlg: Composite {RSA4096, SPHINCS+}

Sig: {10111010100..., 01101001...

...}

"HYBRID" CATALYST™ [2]

AltSig: 01101001...

...

SigAlg: RSA4096

Sig: 10111010100...

A secure way to exchange keys with crypto generated **on the fly** per communication.

Key Encapsulation Mechanism (KEM)

A high sophisticated chain of trust **established over many years**.

Digital Signature Algorithms (DSA)

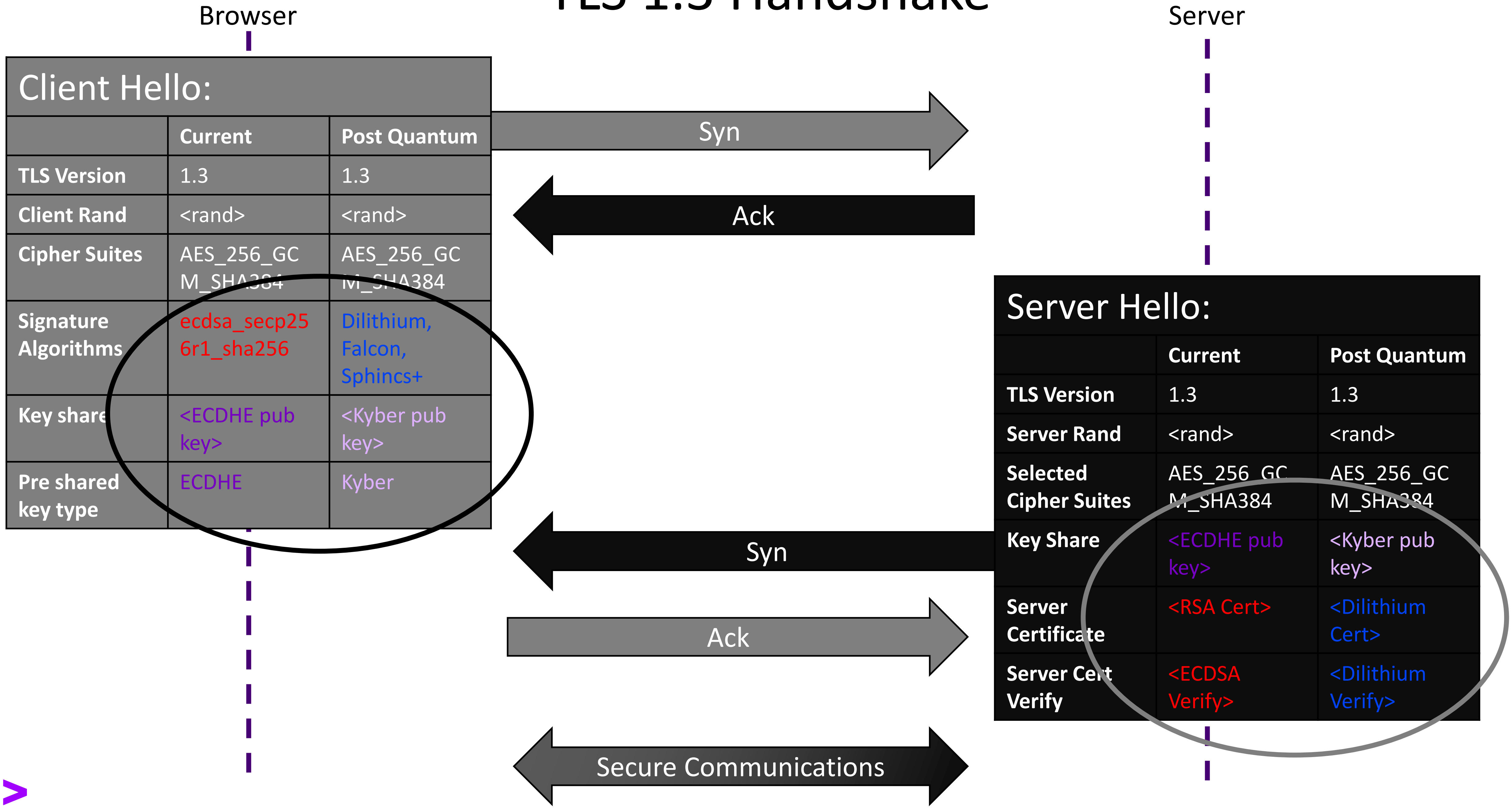
Implemented via Public Key Infrastructure (PKI)

[1] Entrust – CableLabs – D-Trust – Cisco collaboration; IETF draft

[2] ISARA - Entrust - Cisco collaboration; IETF and ISO drafts

> https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509

TLS 1.3 Handshake



Browser

Server

Client Hello:

	Current	Post Quantum
TLS Version	1.3	1.3
Client Rand	<rand>	<rand>
Cipher Suites	AES_256_GCM_SHA384	AES_256_GCM_SHA384
Signature Algorithms	ecdsa_secp256r1_sha256	Dilithium, Falcon, Sphincs+
Key share	<ECDHE pub key>	<Kyber pub key>
Pre shared key type	ECDHE	Kyber

Syn

Ack

Server Hello:

	Current	Post Quantum
TLS Version	1.3	1.3
Server Rand	<rand>	<rand>
Selected Cipher Suites	AES_256_GCM_SHA384	AES_256_GCM_SHA384
Key Share	<ECDHE pub key>	<Kyber pub key>
Server Certificate	<RSA Cert>	<Dilithium Cert>
Server Cert Verify	<ECDSA Verify>	<Dilithium Verify>

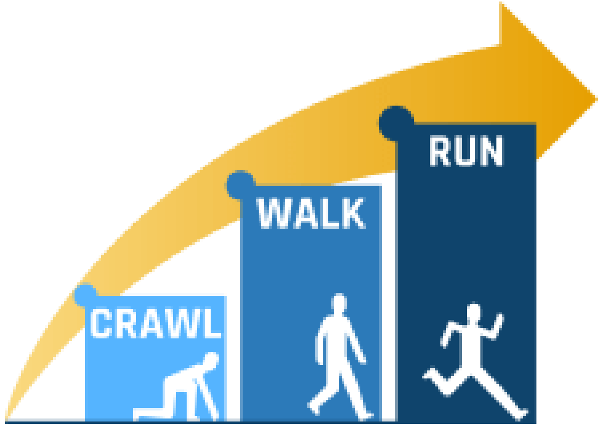
Syn

Ack

Secure Communications

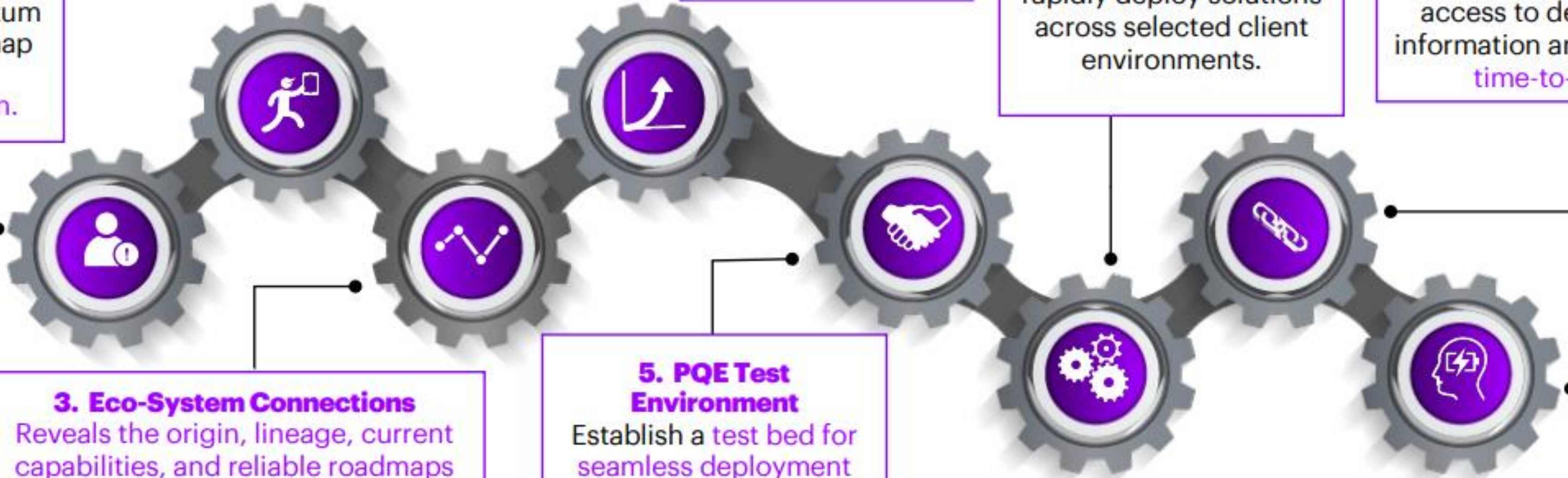
Considering a Maturity Index

POTENTIAL BENEFITS



- Improve Quantum Defenses
- Consistently Measure Progress
- Share Knowledge
- Prioritize Actions and Budgets

Considering Maturity Index Domains and Levels



1. PQE Strategy
The process of building strategy begins with analysis and collaboration, assisting client leadership to create a strategic Quantum readiness roadmap based on the corporate vision.

2. Discovery
Based on the client's needs, high value scanning tools combine with SME analysis to discover and remediate crypto components within your environment.

3. Eco-System Connections
Reveals the origin, lineage, current capabilities, and reliable roadmaps of 3rd party crypto enabled products and services in your extended environment. Set benchmarks and interoperability over time.

4. PQE Architecture
Develop a fully integrated crypto agility architecture for migration to quantum safety.

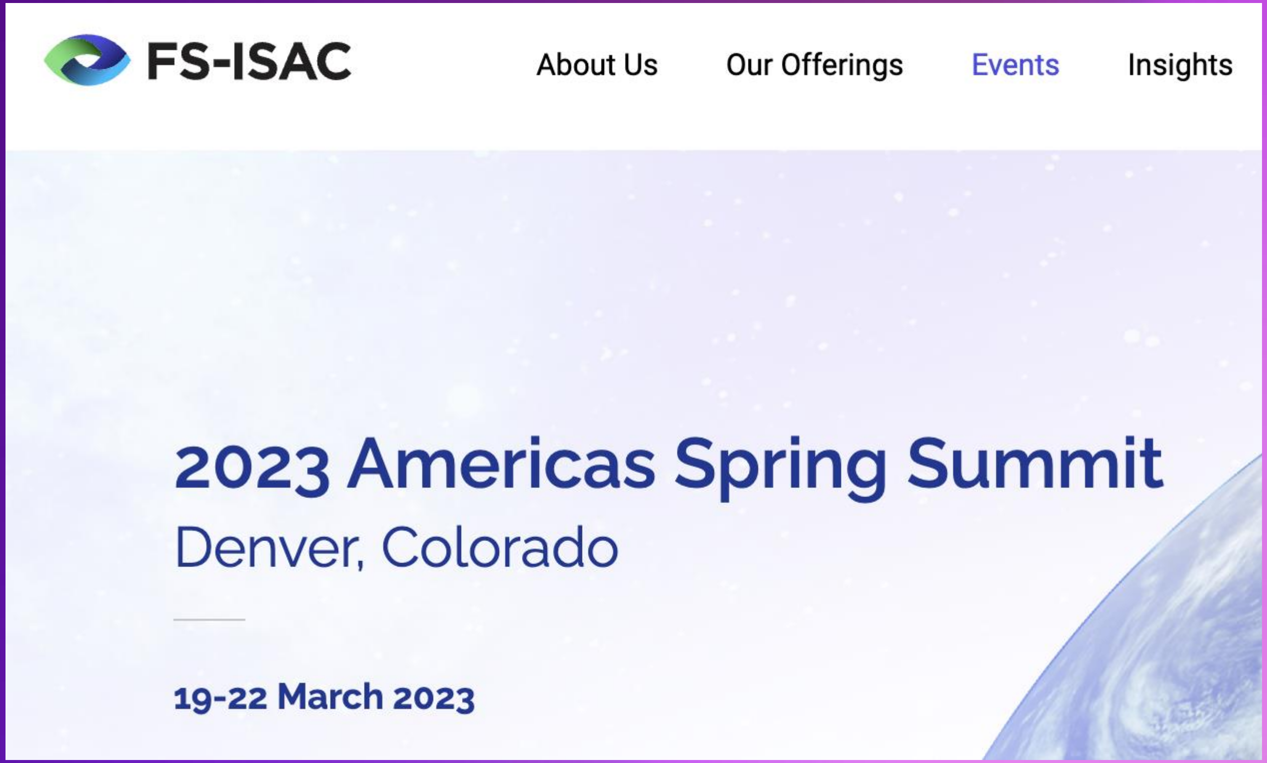
5. PQE Test Environment
Establish a test bed for seamless deployment and testing and gives visibility to interop, performance, and scale for crypto agility outcomes.

6. Limited Trials
Leverage tools and PoC, advanced crypto agility techniques, approaches, and technology tools to rapidly deploy solutions across selected client environments.

7. Roll Out
Migration integrates enterprise data and crypto into one platform, allowing end users with automated access to decision-ready information and accelerating time-to-insights.

8. Manage
Evergreen. New algorithms, new APIs, new automation orchestrated and managed recommend linking to Quantum Security Managed Services.

Report from FS/ISAC Denver March 2023 Roundtable



FS-ISAC

About Us Our Offerings Events Insights

2023 Americas Spring Summit

Denver, Colorado

19-22 March 2023

Summary of Discussions

from Roundtable Participants

Next Steps

Non-binding Show of Hands

WEF talk

Product Vendors

QUANTUM SECURITY GLOBAL LEAD

Tom Patterson | Accenture | Tom.Patterson@accenture.com

BACKGROUND

Tom is the Managing Director for Emerging Technology Security at Accenture, recently joining the leadership team to continue his mission to secure the world's critical infrastructure through the secure application of quantum, AI/ML, 5/6/g, and space technologies. His background in national policy, emerging technology, and as a CISO provides necessary perspective to defend and prosper with the technology used to compute, communicate, and make decisions.

EXPERIENCE (Selection)

Accenture Global Quantum Security Lead
Leads development and operations of global quantum security group, including quantum vendor database, post-quantum testbed, and quantum security strategy. Works with leading vendors of crypto discovery and crypto agility products and services.

Post-Quantum Crypto Agility
Project lead for a global 1000 company's post-quantum strategy, crypto discovery, crypto provenance, crypto agility architecture, and successful roll out to key applications. Implemented orchestrated crypto agility integrated with threat intelligence feeds for very critical operations.

Post-Quantum Encryption
Project lead for a communication (UCC) workspace platform's upgrade to integrate quantum resistant algorithms. Use of NIST candidates Crystals-Kyber and Crystals-Dilithium cryptographic algorithms, integrated into the messaging layer security encryption. Resulted in first commercial UCC product to fully implement PQE.

Post-Quantum Strategy and Discovery
Project executive for post-quantum security strategy and discovery at a large financial institution. Project scans, classifies and evaluates global networks and applications for quantum risk.

SKILLS and CERTIFICATIONS

- Post-Quantum Security
- Crypto Agility
- AI/ML Security
- 5/6/g Communications
- Space Security
- OT / SCADA
- Trust
- Resilience

INDUSTRIES

- Financial
- Energy
- Communications
- Manufacturing
- Technology
- Transportation
- Healthcare
- National Security
- Five Eyes

TOM
PATTERSON

QUANTUM SECURITY GLOBAL LEAD

Post-Quantum Cryptography Conference

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

01 COMMUNIQUE

amsterdam
convention
bureau

ascertia

亞洲誠信
TRUSTAsia

PKI
Consortium