Post-Quantum

Cryptography Conference

Building Your PQC Lab: Trust But Verify Your PQC Ecosystem

Blair Canavan

Director, Alliances at Thales

ENTRUST HID PKI Consortium

THALES
Building a future we can all trust

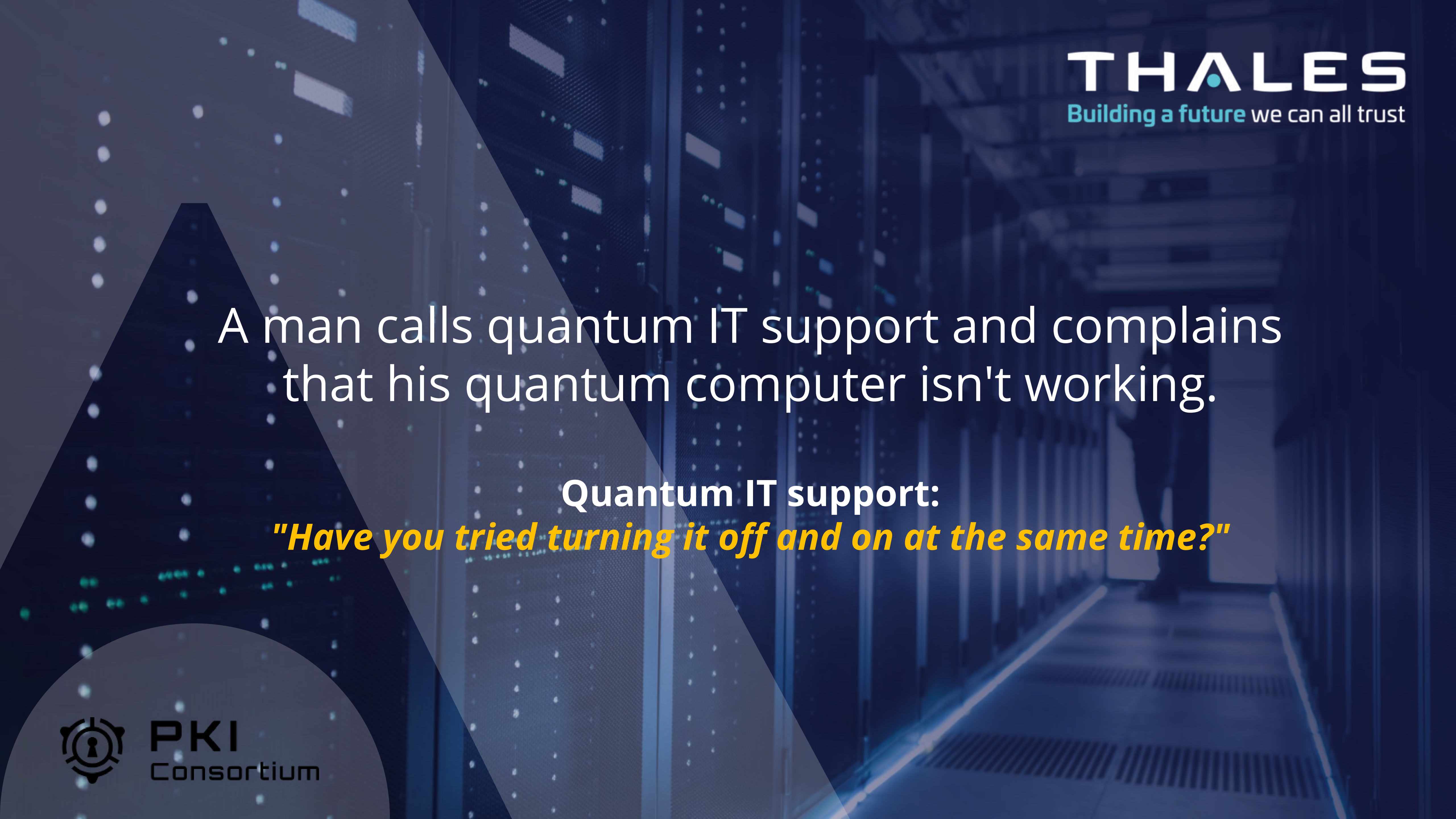
Building Your PQC Lab

Trust but verify your PQC ecosystem

Ensuring PQC-Agility

Nov 8, 2023
Blair Canavan
Director, Alliances, PQC Portfolio

PKI Consortium



THALES

Building a future we can all trust

A man calls quantum IT support and complains that his quantum computer isn't working.

Quantum IT support:

"Have you tried turning it off and on at the same time?"

PKI Consortium

Agenda

- Is there a problem here?
- Where do we start?
- Case study
- Take-aways
- Close

Is There a Problem Here?

Risk Management

"Quantum computing risk cannot be ignored. Without cryptography, we essentially need to "unplug" from the ICT infrastructure and stop using untrusted parties and media. This is simply not practical for the majority of applications, including anything involving a financial transaction that uses real-time communication (credit card purchases, Money Transfers, online banking, etc) online communication (e-mail, texting, social media, etc) online advertising, e-health and so on."

Dr. Michele Mosca, Institute for Quantum Computing, University of Waterloo.

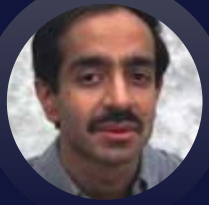
How a quantum computer impacts cryptography

PKI Consortium

CRYPTOGRAPHIC ALGORITHM TARGETED	TYPE	PURPOSE	IMPACT FROM LARGE SCALE QC
RSA	Public key	Signatures, Key establishment	No longer secure
Digital Signature Algorithm		Signatures, Key exchange	
ECDSA (Elliptic Curve DSA)			

Peter SHOR

CRYPTOGRAPHIC ALGORITHM TARGETED	TYPE	PURPOSE	IMPACT FROM LARGE SCALE QC
AES	Symmetric key	Encryption	Longer keys needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed

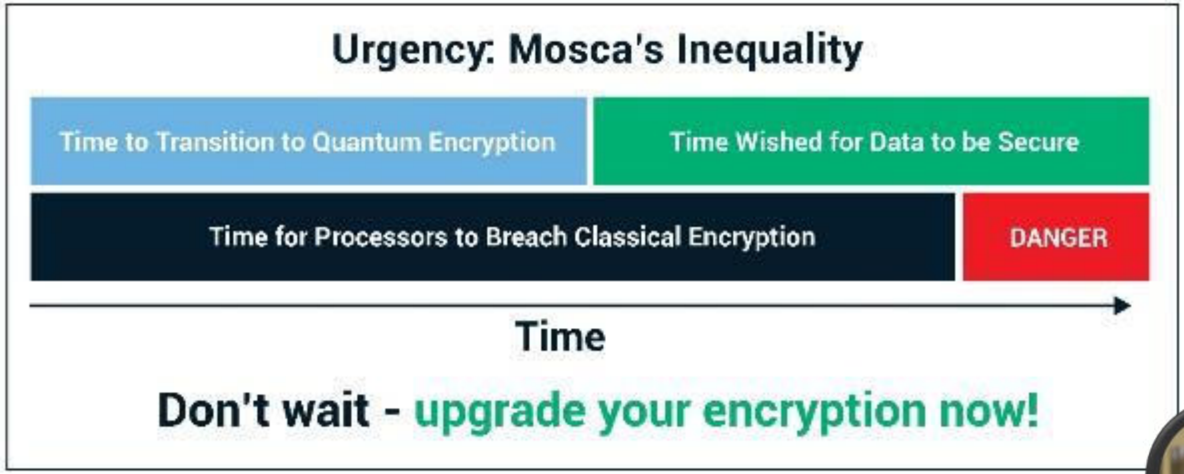


Lov GROVER

THALES

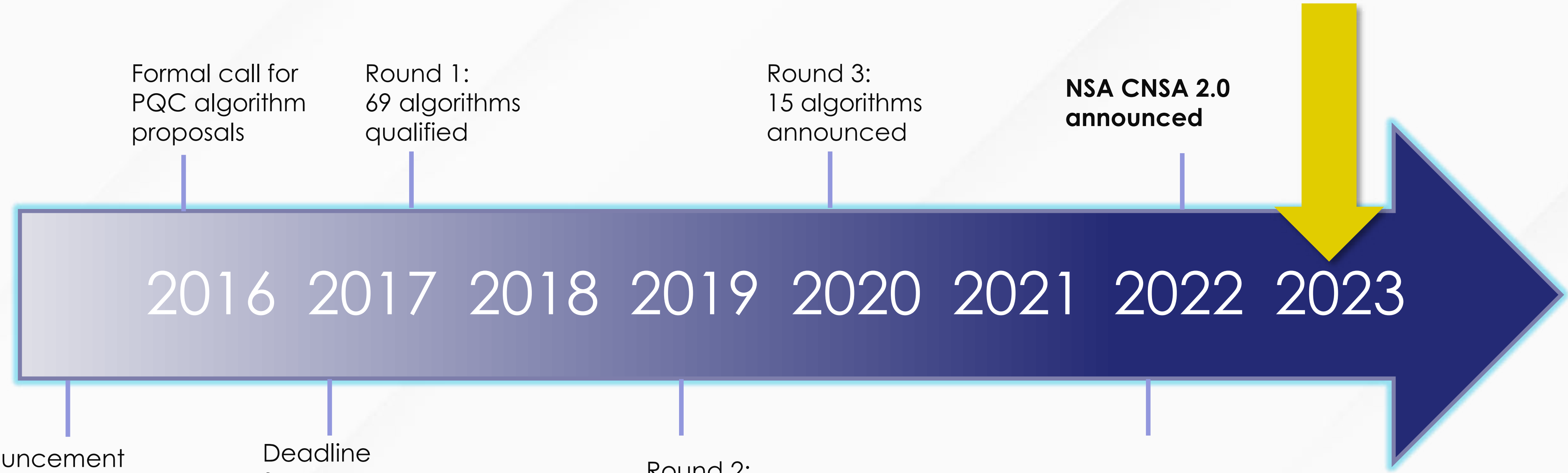
Mosca’s Theorem

“According to Dr. Mosca's Theorem (X+Y)>Z, if the amount of time that data must remain secure (X) plus the time it takes to upgrade cryptographic systems (Y) is greater than when quantum computers come online with enough power to break cryptography (Z), you have already run out of time”


Urgency: Mosca's Inequality
Time to Transition to Quantum Encryption
Time Wished for Data to be Secure
Time for Processors to Breach Classical Encryption
DANGER
Time

Don't wait - upgrade your encryption now!

The NIST Standardization Process



Announcement of Call for Submissions

Formal call for PQC algorithm proposals

Deadline for submission

Round 1: 69 algorithms qualified

Round 2: 26 algorithms announced

Round 3: 15 algorithms announced

NSA CNSA 2.0 announced

Standards expected in **2024**

CRYSTALS-KYBER	**ML-KEM (FIPS-203)**
CRYSTALS-DILITHIUM	**ML-DSA (FIPS-204)**
SPHINCS+	**SLH-DSA (FIPS-205)**
FALCON	**FN-DSA (PROPOSED NAME – RELEASED)**

NIST finalist FALCON was sponsored and co-developed by Thales along with academic and industrial partners from France (University of Rennes 1, PQShield SAS), Switzerland (IBM), Canada (NCC Group), and the US (Brown U, Qualcomm).

Threat Relevance

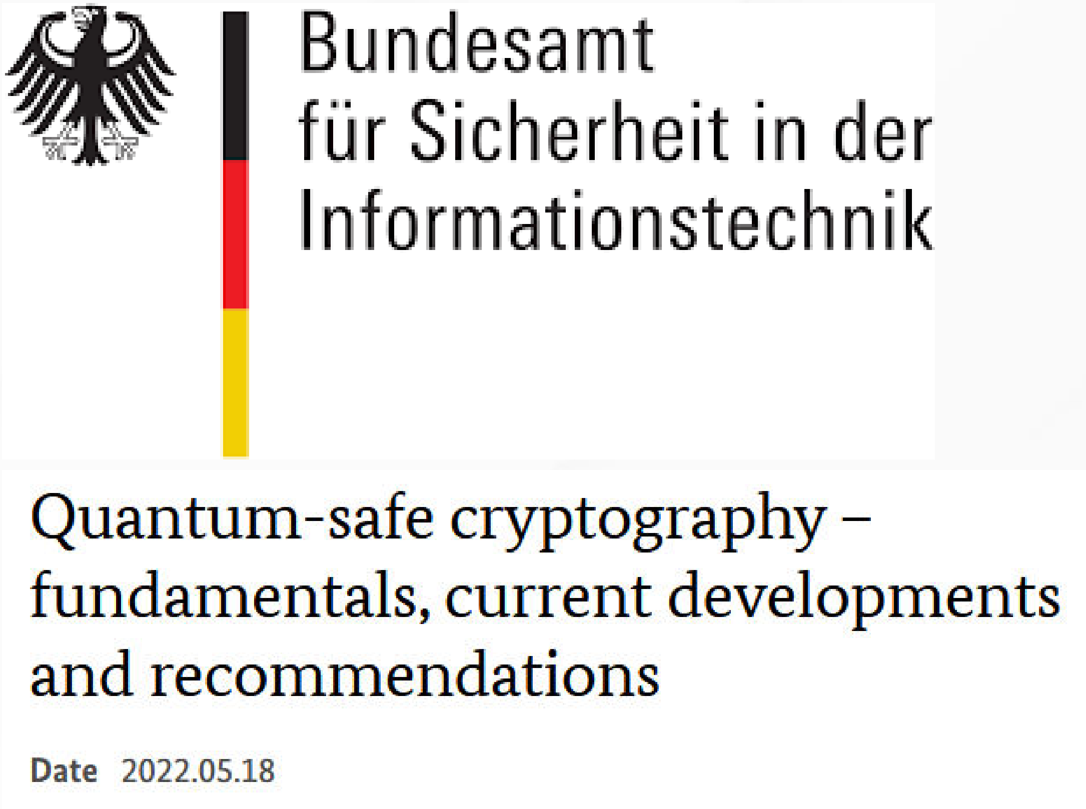
ANSSI | Agence nationale de la sécurité des systèmes d'information

For ANSSI, PQC represents the most promising avenue to thwart the quantum threat.

- « ANSSI encourages all industries to initiate [..] a **gradual overlap transition** in order to progressively increase trust on the **post-quantum algorithms** and their implementations »
- « The quantum threat makes **crypto agility particularly relevant** », and
- « ANSSI will **encourage** the initiation of progress towards **crypto agility** as much as possible for future products. »

Source:
https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/

Threat Relevance



Bundesamt für Sicherheit in der Informationstechnik

Quantum-safe cryptography – fundamentals, current developments and recommendations

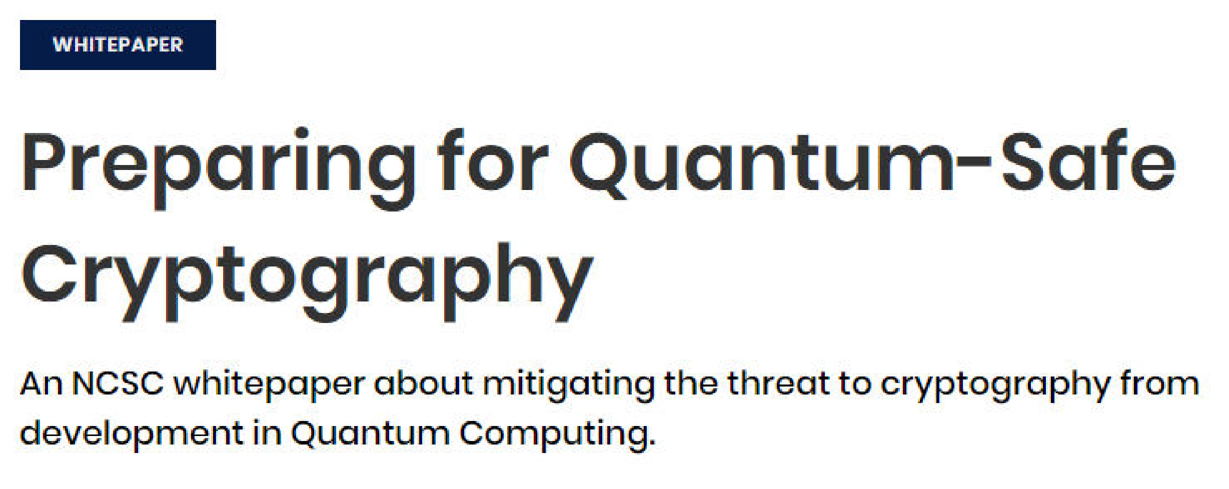
Date 2022.05.18

- « From BSI's point of view, the question of "if" or "when" there will be quantum computers is no longer in the foreground. **Post-quantum cryptography will become the standard in the long term**. »
- « Concerning further development [..] **particular attention** should be paid to making cryptographic mechanisms as flexible as possible in order to be able to react to [..] possibly replace algorithms in the future that no longer guarantee the desired level of security ("**cryptographic agility**"). »

Source:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html

Threat Relevance

National Cyber Security Centre



WHITEPAPER

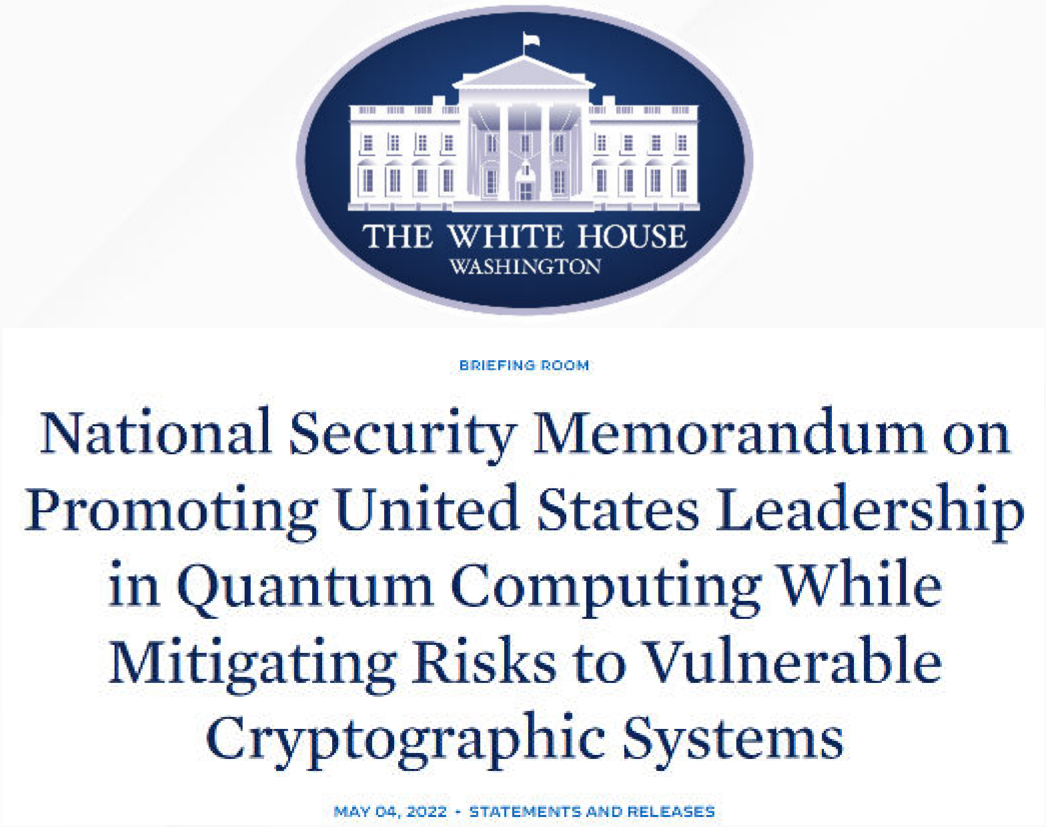
Preparing for Quantum-Safe Cryptography

An NCSC whitepaper about mitigating the threat to cryptography from development in Quantum Computing.

- «There is likely to be a period during which organisations will be required to operate both conventional and quantum-safe cryptography, in order to ease transition between the two.»
- «The NCSC cautions against early adoption of non-standardised QSC. », and
- «There is **unlikely** to be a **single quantum-safe algorithm** suitable for all applications.. »

Source: https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

Threat Relevance



THE WHITE HOUSE
WASHINGTON

BRIEFING ROOM

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

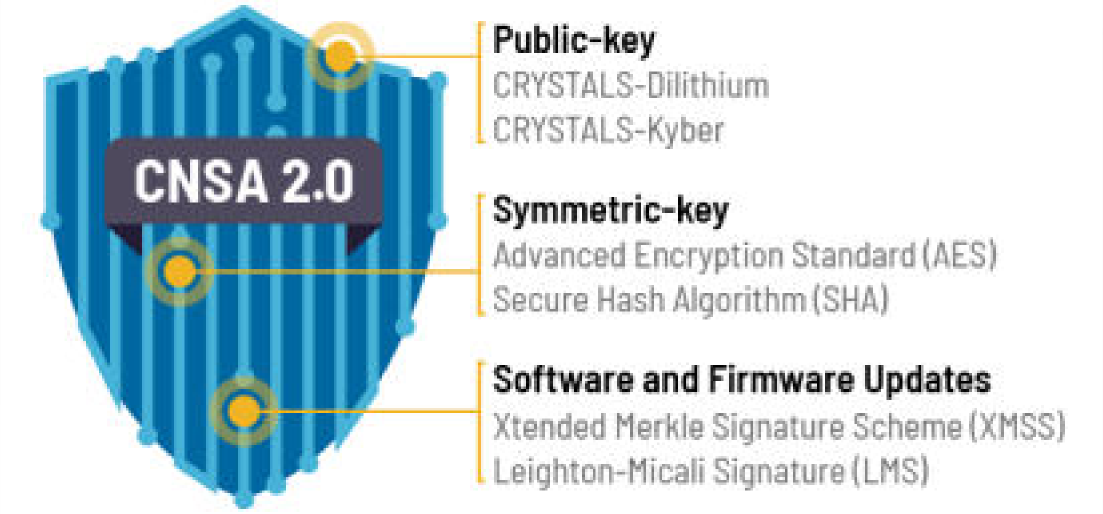
MAY 04, 2022 • STATEMENTS AND RELEASES

- « To mitigate this risk, the United States must **prioritize** the timely and equitable **transition** of cryptographic systems **to quantum-resistant cryptography**, with the goal of mitigating as much of the quantum risk as is feasible **by 2035**. »
- « Central to this migration effort will be an emphasis on **cryptographic agility**, both to reduce the time required to transition and to allow for seamless updates for future cryptographic standards. »

Source:
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

NSA CNSA 2.0 Recommendations

National Security Agency | Cybersecurity Advisory



Public-key
CRYSTALS-Dilithium
CRYSTALS-Kyber

Symmetric-key
Advanced Encryption Standard (AES)
Secure Hash Algorithm (SHA)

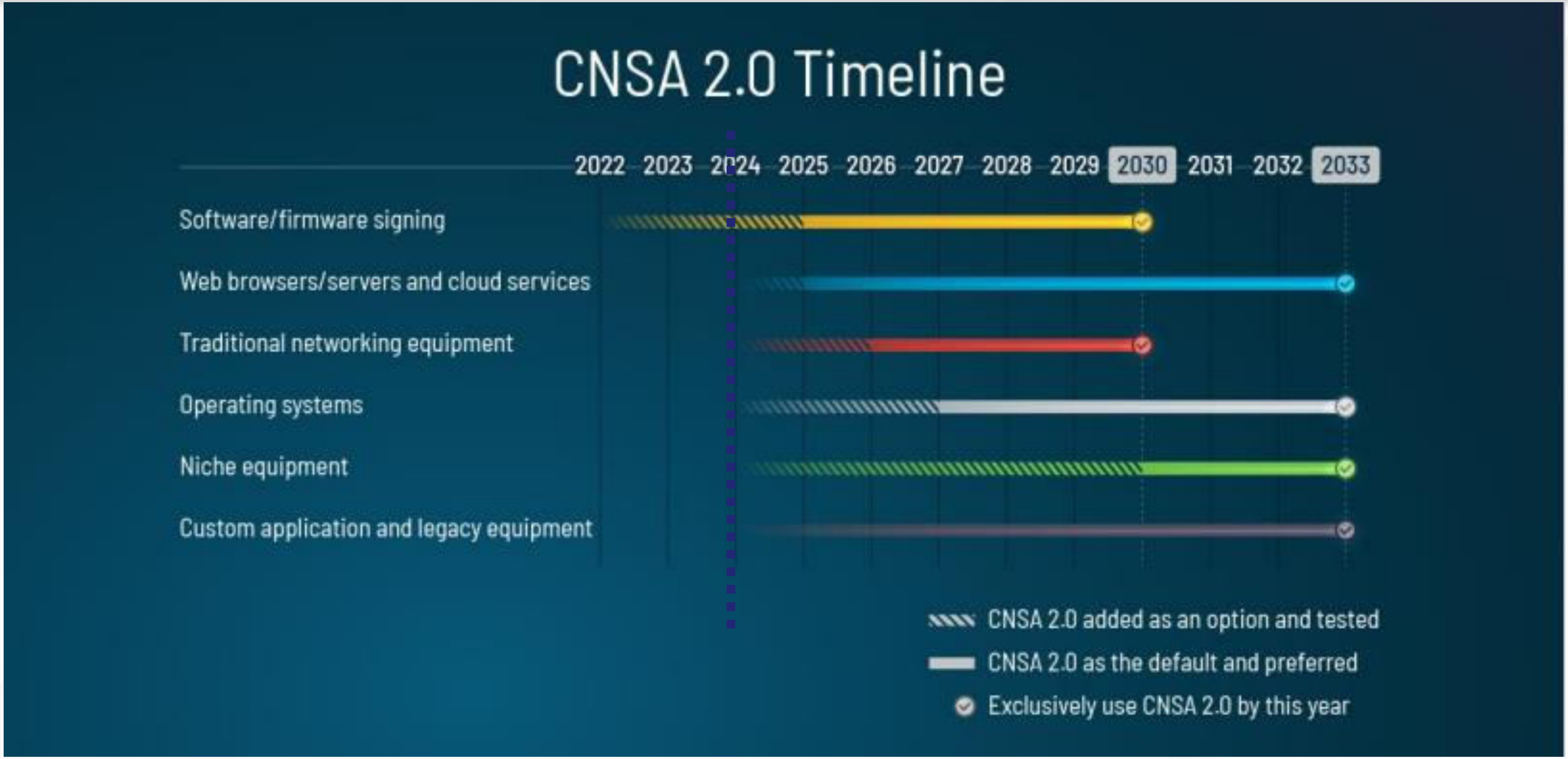
Software and Firmware Updates
Xtended Merkle Signature Scheme (XMSS)
Leighton-Micali Signature (LMS)

- SW/FW signing begin transition immediately
- New SW/FW signed using new algorithms by 2025
- Transition to be complete by 2035

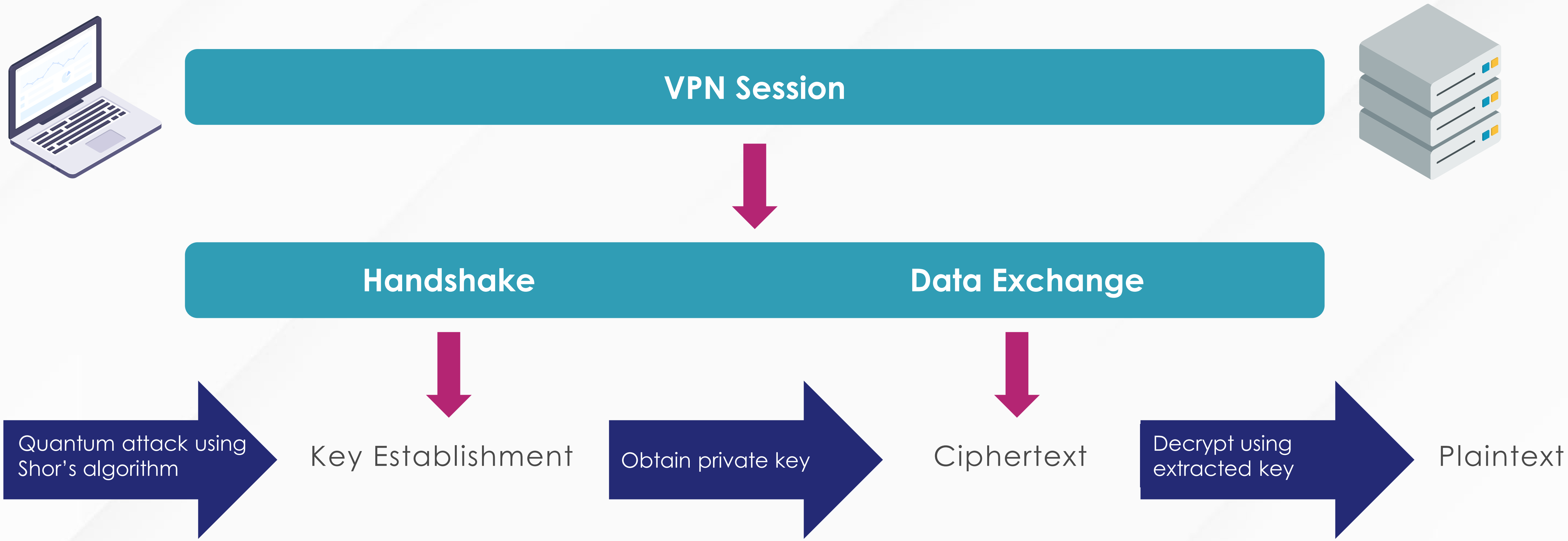
CRYSTALS-KYBER	**ML-KEM (FIPS-203)**
CRYSTALS-DILITHIUM	**ML-DSA (FIPS-204)**
SPHINCS+	**SLH-DSA (FIPS-205)**
FALCON	**FN-DSA (PROPOSED NAME – RELEASED)**

Source:
https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

Understanding implementation timelines by industry type



Area of high risk: Confidential Communications



VPN Session

Handshake

Data Exchange

Quantum attack using Shor's algorithm

Key Establishment

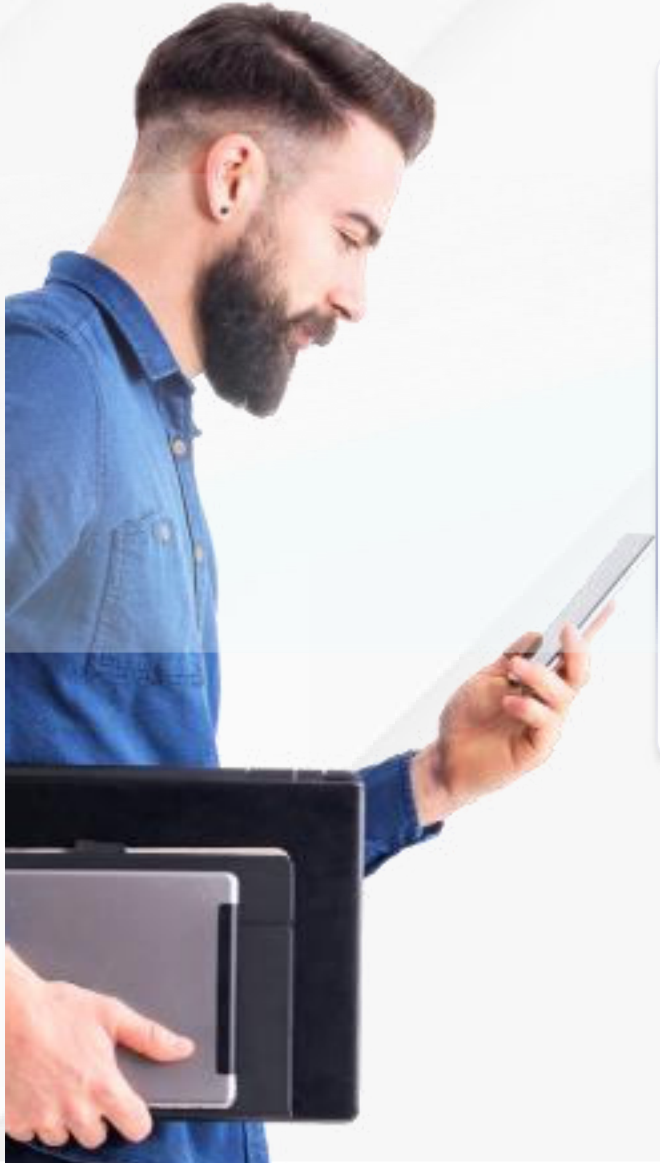
Obtain private key

Ciphertext

Decrypt using extracted key

Plaintext

Where Do We Start?



The ecosystem of technologies is already “on it”

The world relies on public key cryptography (e.g. RSA)

Today’s Asymmetric algorithms moving to PQC (NIST approved)

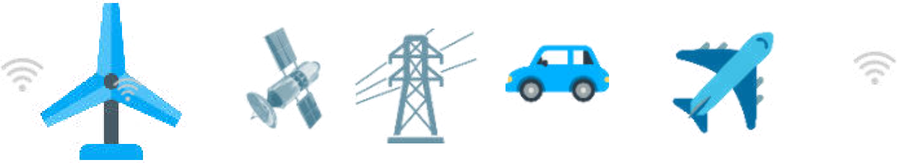
Planning is Essential: PQC Project Planning 101

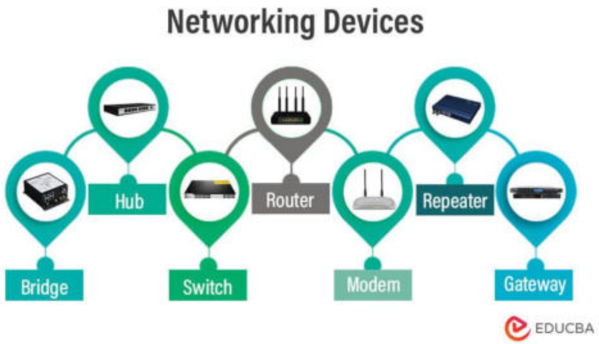
- Stakeholders & Staffing
  - Exec Sponsorship
  - Current staff expertise
  - External SMEs
  - Seek knowledge
- Budget for success
- Project Management
- Current vs. Desired State
- Crypto Discovery
  - Crypto Assets, vulnerabilities, priority-base approach
- Ecosystem support from vendors & industry

Area of high risk: Use Cases Vary

What's at risk?

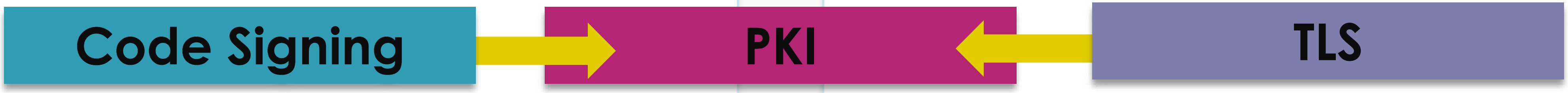
Durable connected devices (IoT) with **long in-field lives**





What's the attack?

Forged software updates by quantum-enabled adversaries



Code Signing → PKI ← TLS

A Collective Approach to Quantum Readiness

Work with your Technology Partners

- PKI certificate models
- Integrations, APIs

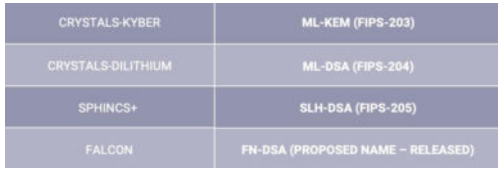
Work with standard bodies

- OASIS for PKCS#11
- IETF
- PKI Consortium
- NCCoE
- IEEE
- X9
- CA/Browser Forum

Focus on Code Signing

- Existing standard mechanisms (SP800-208)
- CNSA 2.0
- Firmware and S/W

Add NIST Finalists



CRYSTALS-KYBER	ML-KEM (FIPS-203)
CRYSTALS-DILITHIUM	ML-DSA (FIPS-204)
SPHINCS+	SLH-DSA (FIPS-205)
FALCON	FN-DSA (PROPOSED NAME – RELEASED)

Once standard, FIPS Certify

After all the work is done, important to remain **crypto agile**.

Running the Marathon

- Mainly dealing with ecosystems that are standards dependent
  - Today, time for PoCs, experimentation, announcements
    - QTLS, QPKI with Wells Fargo

- Changing algorithms, protocols, key formats…
  - Multi player ecosystem → not easy, costly, and takes time

- Quantum Risk Assessment
  - Preparation and migration strategy, with priority management
    - Key material that needs to be protected for a long time (PKI root keys, Digital signature keys…)
    - Key material that lives in products with a long shelf-life or difficult to upgrade ((I)IoT, SE, MIM..)

Case Study: Wells Fargo

Customer Challenge

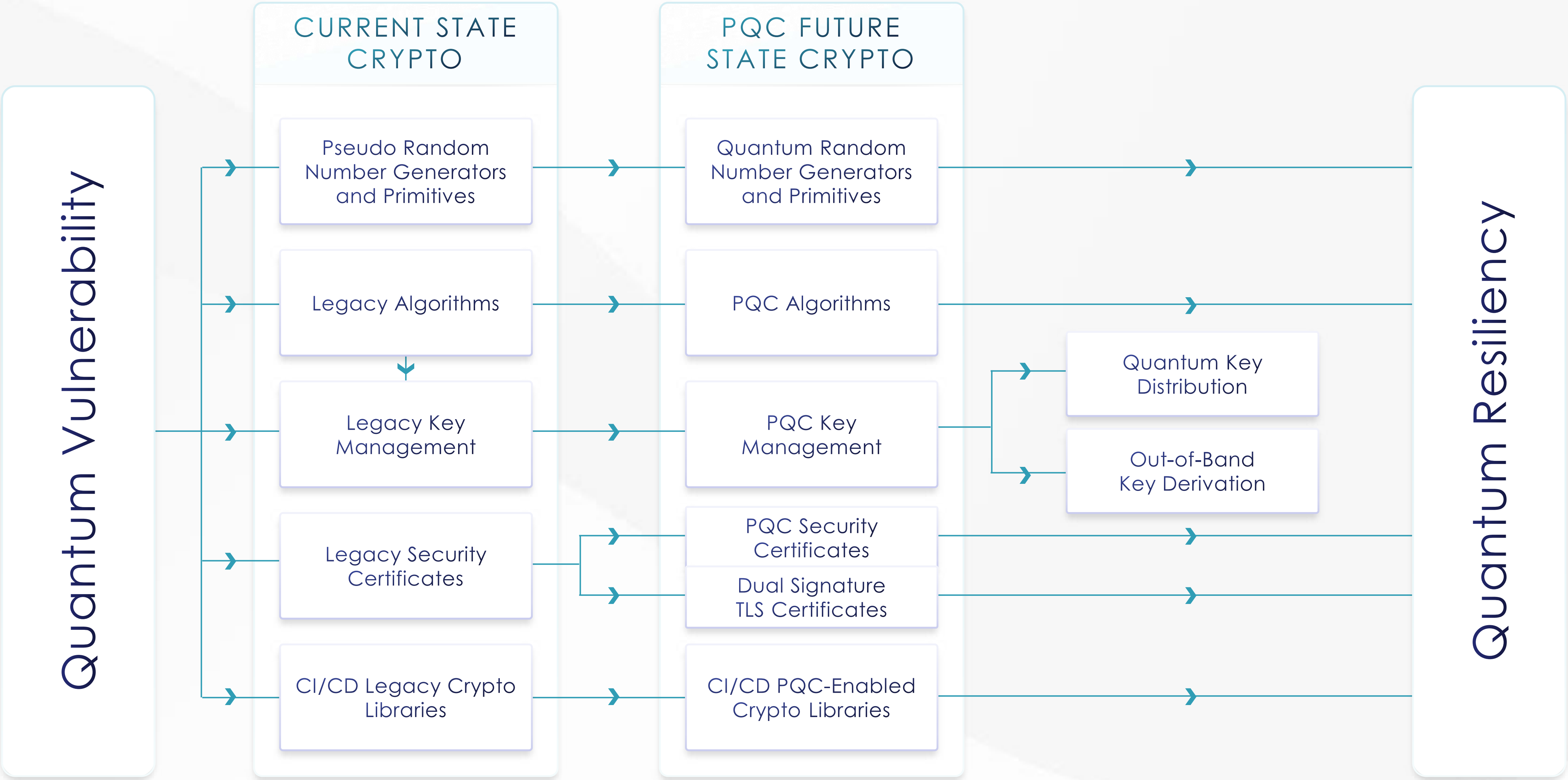
About Wells Fargo, about their team

What problems we were faced with	Protecting customer and WFC proprietary data while minimizing disruption to the Enterprise	Establishing crypto-agility as a foundation for PQC mitigation	Developing the foundational layer of the PQC solution tech stack
IT challenges	Integrating quantum entropy into an inherently heterogeneous architecture	Developing a scalable, agile PQC approach to leverage Entropy as a Service for banking innovations and workflows	
Other considerations	Ubiquity for the entire financial ecosystem	Operational costs, technical expertise, resource availability, multi-party cooperation.	Reputational risk – of doing nothing or doing it ineffectually

Customer Challenge – PQC Solution Stack

PKI Consortium

WELLS FARGO

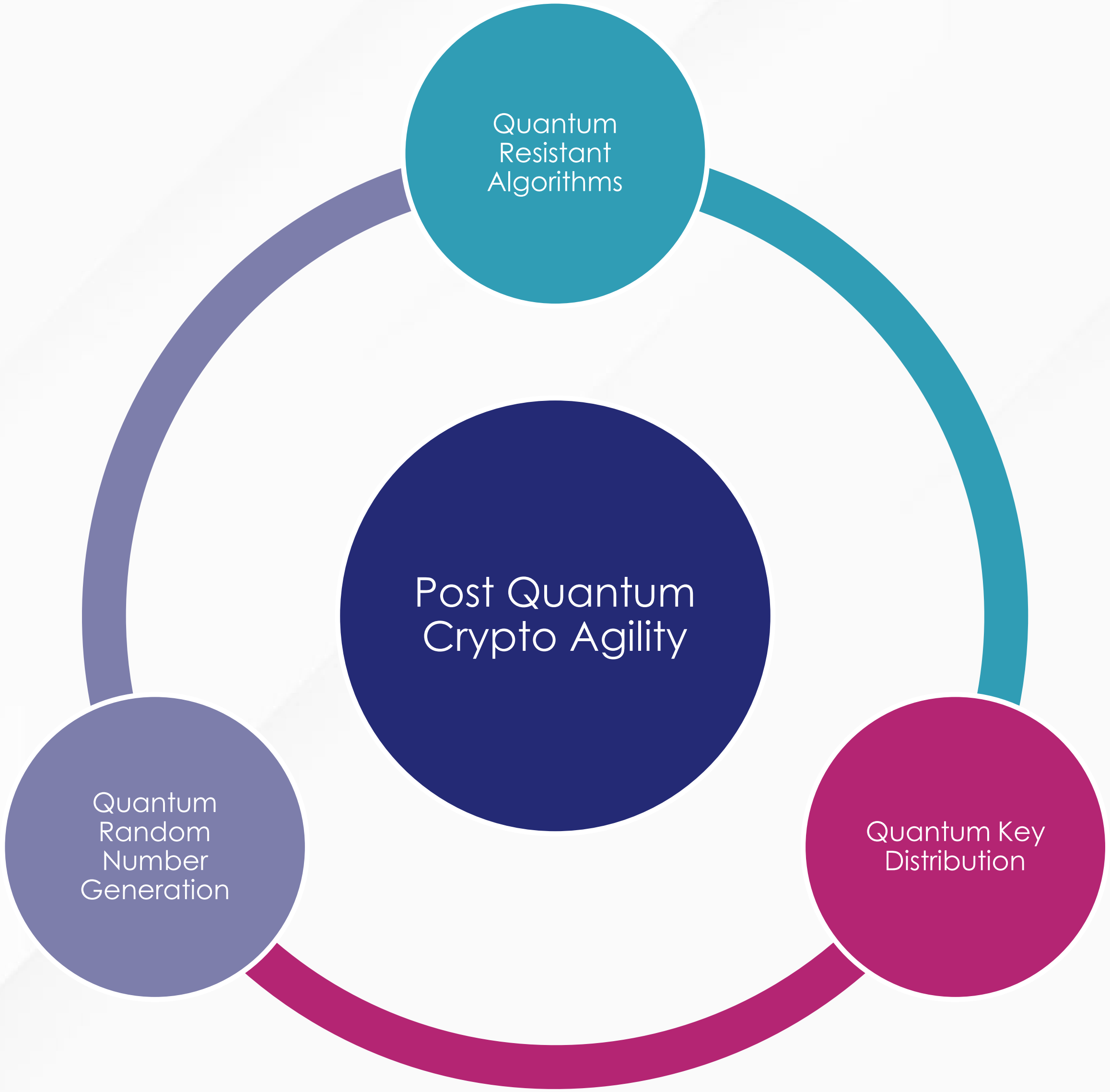


Quantum Vulnerability
CURRENT STATE CRYPTO
Pseudo Random Number Generators and Primitives
Legacy Algorithms
Legacy Key Management
Legacy Security Certificates
CI/CD Legacy Crypto Libraries
PQC FUTURE STATE CRYPTO
Quantum Random Number Generators and Primitives
PQC Algorithms
PQC Key Management
PQC Security Certificates
Dual Signature TLS Certificates
CI/CD PQC-Enabled Crypto Libraries
Quantum Key Distribution
Out-of-Band Key Derivation
Quantum Resiliency

THALES

Key Take-Aways

Building a future-proof Quantum strategy



Post Quantum Crypto Agility

Quantum Resistant Algorithms

Quantum Key Distribution

Quantum Random Number Generation

Standards

NIST

IETF

PKI Consortium

NCCoE National Cybersecurity Center of Excellence

ANSI

Accredited Standards Committee X9 Inc. Financial Industry Standards

ETSI World Class Standards

CAB CA/Browser Forum

CSA cloud security alliance®

Future-proof with crypto agility

PKI Consortium

Quantum is coming

Quantum capabilities are accelerating

NIST and others are finalizing quantum safe standards

PKI based crypto will become obsolete

Know your risks

Long term data is at risk, if using classic technologies

Consider that it is vulnerable to harvesting and early attacks

Focus on crypto agility

Crypto Agility is the best practice; requires supporting infrastructure

Take a hybrid approach by using classic & quantum-safe crypto solutions

Stronger Together

Assess your crypto agility maturity and readiness

Design a quantum safe architecture

Be ready for change, even after standards are established

Evaluate solutions and partnerships in place today to support your quantum safe initiatives

THALES

Trust but Verify

- Ecosystem support from vendors & industry
  - Reasonable verification
  - Vetted staff and technology
- Compare with external sources
- Audit – when available
- Assess, Review
- Communicate

Foundations of a Quantum-Safe solution

Key Generation

Provably Unpredictable Keys From Quantum Computers

Key Algorithms

NIST Post Quantum Algorithms

Key Management

Tamper-Proof Lifecycle Management

Taking a hybrid approach

PKI Consortium

Governing bodies recommend:

- A **Hybrid** approach utilizing **crypto agile** platforms for a smooth transition

Practice:

- Algorithms – Support for alternate modes with classical algorithms and QRA
- RNGs – Combine QRNGs with NIST certified RNGs

Transition:

- As Standards are approved, implement, and re-certify

3 phases proposed by ANSSI, towards full PQC:

- ✓ Phase #1: Preparation
- ✓ Phase #2: Hybridization
- ✓ Phase #3: Full PQC

THALES

Thank you

cpl.thalesgroup.com

THALES

Building a future we can all trust

Building Your PQC Lab

Trust but verify your PQC ecosystem

Ensuring PQC-Agility

Nov 8, 2023
Blair Canavan
Director, Alliances, PQC Portfolio

PKI Consortium

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