FIX Information Xchange

Quantum Computing & Financial Messaging



FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

FIX Information Xchange

Quantum Computing & Financial Messaging



Jim Kaye
Executive Director
FIX Trading Community



Bill Poletti
Co-Chair, ASC X9 Financial PKI Operations Team, ASC X9 (Member Emeritus)
ASC X9



Ralph Spencer Poore
CISSP(Emeritus), CISA, CFE(Retired), CHS-III, PCIP
X9 PKI Financial Industry Forum Chair
X9 AI Study Group, Vice Chair
X9F1 Vice Chair
US Expert ISO TC68/SC2/WG 11 & 13
ISSA Distinguished Fellow
ACM Senior Member
ASC X9



Steve Stevens
Executive Director
ASC X9



Jeff Stapleton
Post-Quantum Cryptography (PQC) researcher & architect
Wells Fargo



Ivy Lyons
X9 PKI Operations
ASC X9

FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

Who is ASC X9

- Accredited Standards Committee X9 Financial Industry Standards https://x9.org
  - X9 is accredited by the American National Standards Institute (ANSI) to develop national standards for the financial industry
  - X9 is the US technical advisory group (TAG) to ISO Technical Committee 68 Financial Services (TC68)
  - X9 is the TC68 Secretariat
  - X9 membership includes over 100 companies
  - X9 manages subcommittees, workgroups, and public forums
  - X9 published over 100 X9 standards
  - X9 participates over 80 ISO standards

- ASC X9 also supports a number of research and technical groups for purposes on gaining information for their membership.
- Some of these groups include:
  - Post Quantum Risk Study Group
  - AI Study Group
  - Payments Study Group
  - Healthcare Services Payments
- Standards development and study groups are staffed by volunteers.

FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

What is Quantum Computing

- Classic computers use binary bits
  - Data (and code) encoded using binary (0, 1) bits
  - Code sequential (step-by-step) solution
  - Solves linear problems in polynomial time - more CPU faster result
  - Can only approximate hard business problems

- Quantum computers use qubits
  - Data encoded using super-position – one qubit is two binary bits
  - Code non-sequential using quantum entanglement
  - Solves non-polynomial (NP) in polynomial time
  - Quantum advantage: solve hard business problems

- The Quantum Threat
  - Breaks legacy asymmetric cryptography – RSA, DH, ECC
  - Shor's Algorithm derives private key from public key

FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

Quantum Threat Scenarios

- Harvest Now Decrypt Later (HNDL)
  - TLS sends encrypted data over open networks
  - TLS session keys established swapping public keys
  - TLS session recorded today can be decrypted tomorrow

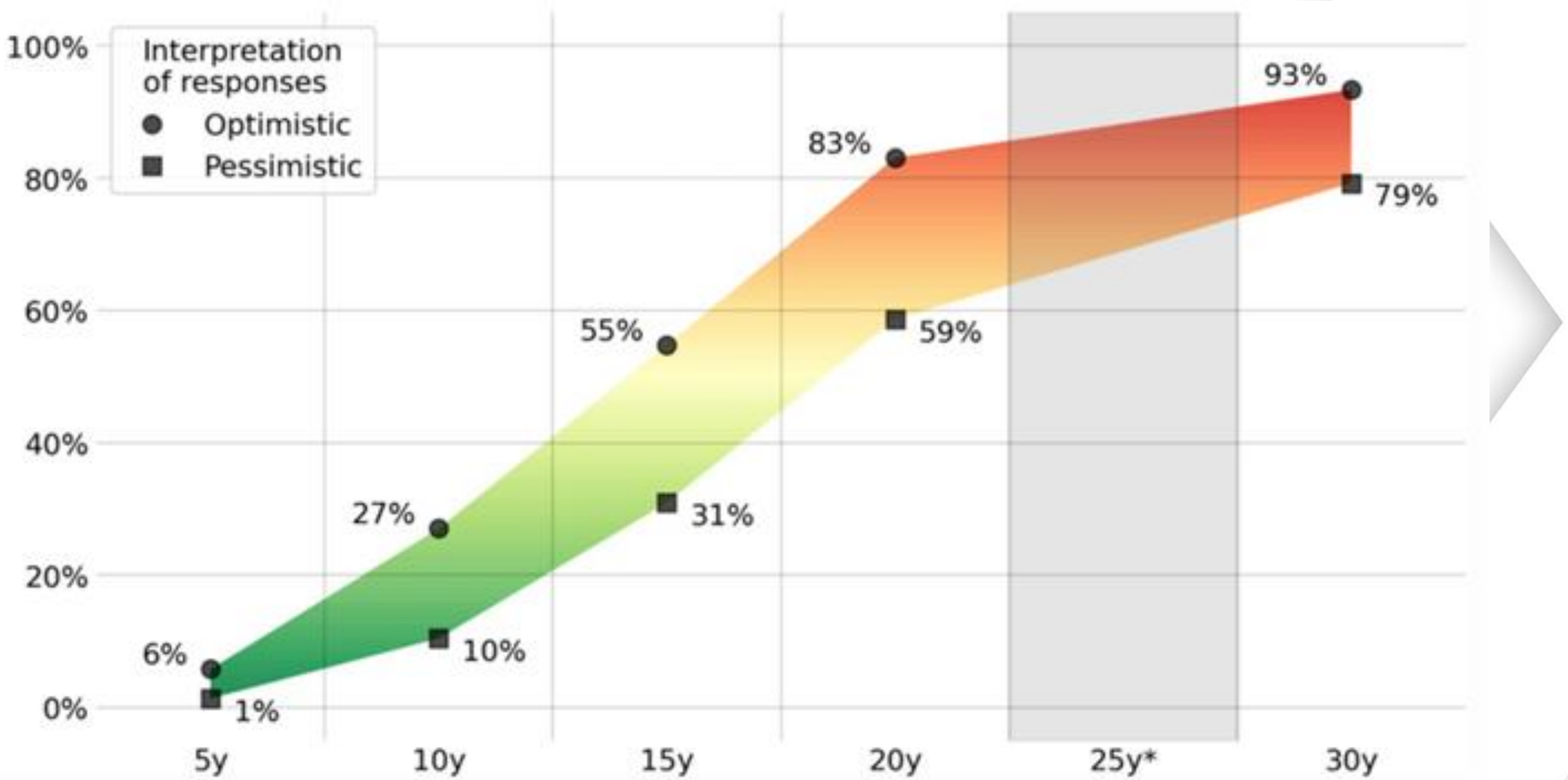
- Trust Now Fraud Later (TNFL)
  - Messages signed independent TLS connections
  - Message signatures verified using public key certificates
  - Messages modified or spoofed with “valid” signatures

- NIST published post-quantum cryptography (PQC) algorithms
  - FIPS 204 Module-Lattice Digital Signature (ML-DSA)
  - FIPS 203 Module-Lattice Key-Encapsulation Mechanism (ML-KEM)

FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

Mosca's Global Risk Institute

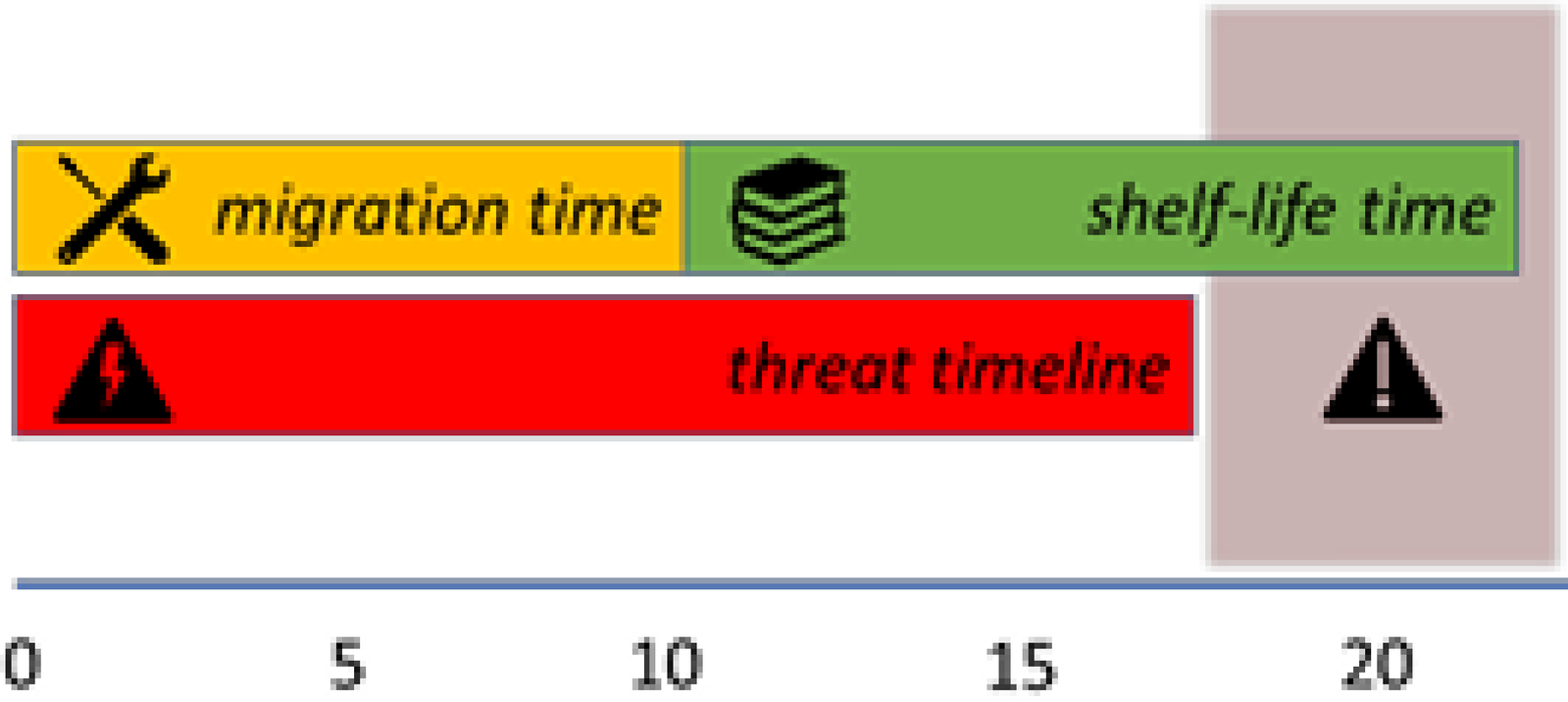
Quantum Threat Timeline Report 2022



FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

Mosca's Inequality Equation

Migration Time + Shelf-Life Time > Threat Timeline



- **Shelf-life time:** the number of years the data should be protected;
- **Migration time:** the number of years needed to safely migrate the systems protecting that information;
- **Threat timeline:** the number of years before relevant threat actors can potentially access cryptographically-relevant quantum computers

FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

Quantum Reality

- Quantum computing has the potential for significant advancements in medicine and medical analysis, agriculture planning, economic planning, meteorological forecasting and other advanced computer activities.

- So far, nothing has materialized.

- An October 8 announcement of an Executive Order to fund development of an Operational Quantum Computer by 2028.

- We still must modernize our systems since even if Quantum Computers are slow to be developed, ***we might not be aware of them for years after their deployment***.

FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

Who is the X9 Financial PKI

- In 2016, concerned members of the financial sector started having concerns over the browser community changing traditional certificate usage.

- A kitchen table discussion resulted in the formation of the initial Financial PKI team consisting of Jeff Stapleton, Ralph Poore and Bill Poletti. Their goal was to develop a PKI solution to address the needs of the financial sector independent of the browser community.

- In 2018, X9 established the X9 Financia PKI study initiative, the X9 PKI Study Group. Dean Coclin from Digicert, accepted the Chair position of the study group.

FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

PQC Transition – From the FIX Perspective

1. Analyze message contents and risk sensitivity

2. Independent of cryptographic implementations, determine whether changes in protection options may be desirable:
    1. Certificate validity period
    2. Extended Key Usage
    3. Segregation of Risk for certain messages, data and communication

3. Consult with X9 Financial PKI for suggestions and / or options

4. Request UAT system set-up for FIX participants to use for internal and interoperability testing

5. If necessary, make modifications to UAT system and repeat testing

6. Document results to include specification updates

FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

PQC Transition – Suggested User Planning

1. Make management commitment to update system protection to resist PQC attacks

2. Set up test system for new environment

3. Work with service providers, portals and other interacting organization to develop a plan for cooperative conversion efforts

4. Test and update systems to latest software and, if necessary, hardware

5. Analyze new system environment for any changes needed for PQC production

6. Work with service providers to develop a plan for cooperative conversion efforts

FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

PQC Transition – Suggested User Testing

1. Acquire PQC test certificates (X9 Financial PKI UAT certificates are now available)

2. Test system for internal operation

3. Establish plan for “dual” interoperability transition in system with both conventional and PQC certificates in circulation

4. Participate in external testing with other organizations for successful interoperability

FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

PQC Transition – Suggested User Implementation

1. Acquire PQC Production certificates (X9 Financial PKI PQC certificates available 4Q2026)

2. Install and test operation

3. Publish implementation date to alert other participants of PQC implementation

4. Observe and document results / issues that need attention

FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

TLS Action Plan

1. Upgrade all TLS instances to TLS 1.3
   - Talk to your vendors, engineers, business clients

2. Enable TLS 1.3 with PQC algorithms
   - TLS ephemeral public keys

     Replace Diffie-Hellman or Elliptic Curve (ECDH) with ML-KEM or Hybrid
     Hybrid: Edwards x2219 EdDH + ML-KEM
   - TLS public key certificates for Server authentication

     Replace RSA or ECDSA with ML-DSA or Hybrid
     Hybrid: Edwards x448 EdDSA + ML-DSA

3. Replace RSA or ECC TLS certificates with certificates based on PQC algorithms
   - X9 Financial PKI PQC enabled early 2027
   - Supports TLS for Server and/or Client authentication

FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

Questions?

FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL

Thank you for joining

Questions?

Please direct any follow-up questions to fix@fixtrading.org

Webinar Recording

A recording will be available soon on our **website** and **YouTube channel**

Not a Member Yet?

Contact us to discuss benefits of membership – fix@fixtrading.org

FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL