ASC X9 Financial PKI

October 15, 2026

Bill Poletti bill.poletti@x9.org
Ivy Lyons ivy.lyons@x9.org
Ralph Poore ralph.poore@x9.org
Steve Stevens steve.stevens@x9.org
Jeff Stapleton Jeff.Stapleton@wellsfargo.c

Accredited Standards Committee X9 Inc.
Financial Industry Standards ®

Agenda

- Who is ASC X9
- What is the Quantum Computing Threat
- Quantum Computing Risk Mitigation and Planning
- Who is ASC X9 Financial PKI

Accredited Standards Committee X9 Inc.
Financial Industry Standards

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

Who is ASC X9

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

and others as necessary

Standards development and study groups are staffed by volunteers.

Accredited Standards Committee X9 Inc.
Financial Industry Standards

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

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)

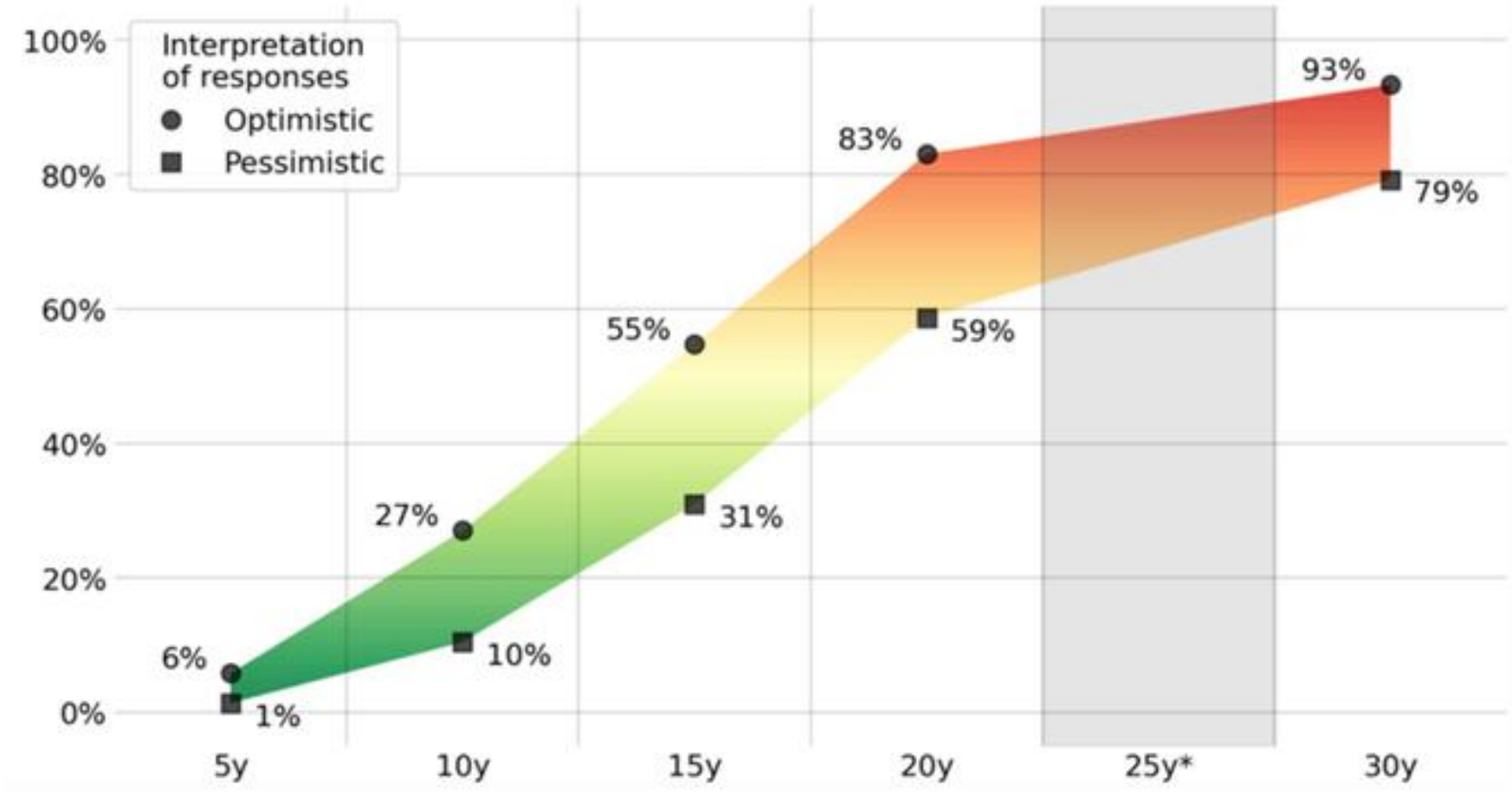
- Messages signed independent TLS connections
- Message signatures verified using public key certificates
- Messages modified or spoofed with “valid” signatures

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

Accredited Standards Committee X9 Inc.
Financial Industry Standards

Mosca's Global Risk Institute

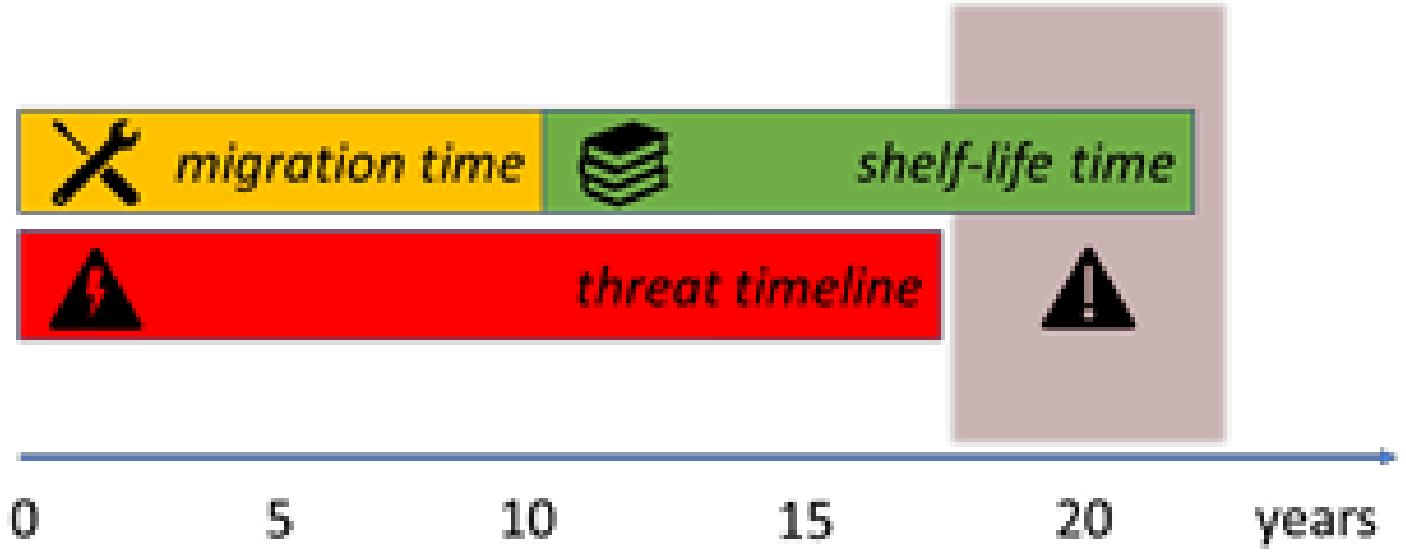
Quantum Threat Timeline Report 2022



Accredited Standards Committee X9 Inc.
Financial Industry Standards

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

Accredited Standards Committee X9 Inc.
Financial Industry Standards

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.

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.

Accredited Standards Committee X9 Inc.
Financial Industry Standards

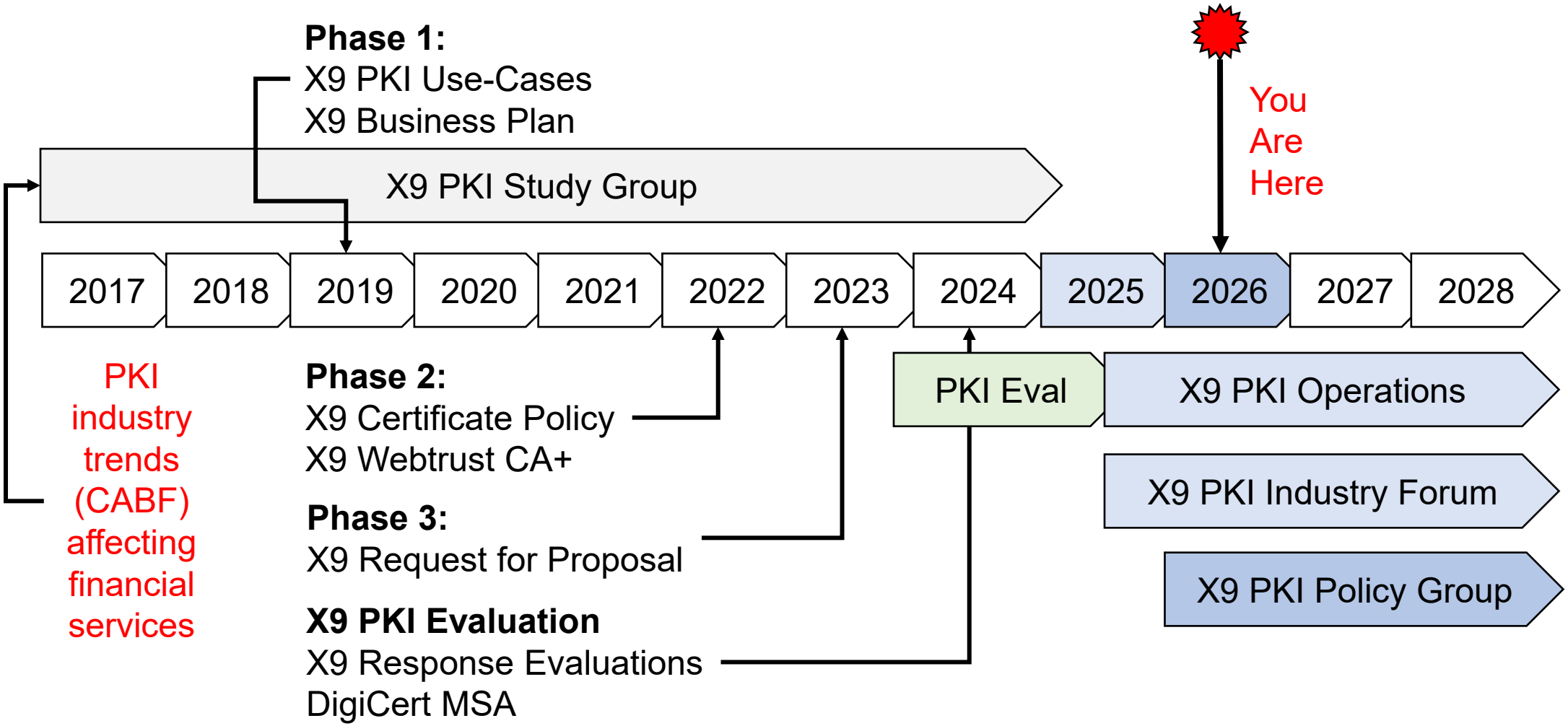
CA Browser Forum

CA Browser Forum (CAB Forum) scope is browsers and web services using X.509 certificates – *Public* PKI

- Specifically: TLS, S/MIME and Code Sign certificates
- Historically Forum and Financial Services differ but *only game in town*
- Financial Industry relied on Public PKI per CAB Forum – *until now*

- Apple Root Program
  - Short validity (47-day) TLS certificates
- Google Chrome Root Programs
  - Deprecate TLS client authentication
- Google Chrome Quantum-resistant Root Program
  - Merkle Tree Certificates (MTC)

X9 Financial PKI History



What is the X9 Financial PKI

- X9 Financial PKI is NOT a *Public* PKI per CAB Forum rules
- X9 Financial PKI is NOT a *Private* PKI
  - *Private* PKI is ascribed as single company
- X9 Financial PKI is a *Community* PKI
  - *Community* PKI is ascribed as collaboration of companies
  - *Community*: Global Financial Services Industry
- X9 Financial PKI is governed by ASC X9
  - Financial Institutions – large, medium, small banks
  - Financial Merchants
  - Financial Service Providers
  - Financial Product Manufactures

Accredited Standards Committee X9 Inc.
Financial Industry Standards

X9 Financial PKI Environments

- X9 Financial PKI DEV environment (X9 GitHub)
  - GitHub https://github.com/x9pki/ SDK
  - Dr. Massimiliano “Max” Pala Massimiliano.Pala@wellsfargo.com
- X9 Financial PKI UAT environment (DigiCert ONE)
  - X9 PKI Operations Team
  - X9 Preproduction Certificates
  - X9 Preproduction PQC Certificates
- X9 Financial PKI PROD environment (DigiCert CertCentral)
  - DigiCert with Webtrust CA+ audit
  - X9 Production mTLS Certificates
  - X9 Production ML-DSA Certificates *coming soon*

Accredited Standards Committee X9 Inc.
Financial Industry Standards

X9 Financial PKI Use-Cases

1. Financial TLS Web Services
2. Financial TLS Aggregator Services
3. **Financial TLS Host Services (mTLS)**
4. Financial TLS Message Queue (MQ) Services
5. Financial TLS Point-of-Interaction (POI) Services
6. Financial Virtual Private Cloud (VPC)
7. Financial File Transfer Protocol Secure (FTPS)
8. Financial Secure File Transfer Protocol (SFTP)
9. Financial SSH Services
10. Financial Device Remote Key Load (RKL)
11. Financial Device Authentication
12. Financial Device Component Authentication
13. Financial Device TLS Communications
14. Financial Manufacturer Code Sign
15. Financial Application Code Sign
16. **Financial ISO 20022 Messages**
17. Financial ID Certificates
18. Financial Distributed Ledger Technology (DLT)
19. Financial PSD2 Certificates
20. Financial Verified Mark Certificates
21. Financial SCD Authentication
22. Financial Application Communications
23. Financial ISO 17442 Legal Entity Identifier (LEI)
24. Financial X9.129 Legal Order Exchange (LOE)
25. Financial IPsec Host Services
26. Financial X9.100-187 Check21
27. Financial Software Bill of Materials (SBOM)
28. Financial Cryptographic Bill of Materials (CBOM)
29. Financial Time Stamp Token (TST) X9.95
30. **Financial QR Codes**
31. Digital Currencies
32. Digital Wallets and Vaults
33. Cryptographic Message Syntax (CMS)
34. **Financial TLS Content Delivery Network (CDN)**

Accredited Standards Committee X9 Inc.
Financial Industry Standards

X9 Financial PKI Industry Perspectives

Depository Trust & Clearing Corporation DTCC https://www.dtcc.com

- GOV2182-26 https://www.dtcc.com/-/media/Files/pdf/2026/7/8/DigiCert-X9---FICC-Important-Notice-GOV.pdf
- MBS1577-26 https://www.dtcc.com/-/media/Files/pdf/2026/7/8/DigiCert-X9---FICC-Important-Notice-MBSD.pdf
- A9791 https://www.dtcc.com/-/media/Files/pdf/2026/7/8/DigiCert-X9---NSCC-Important-Notice.pdf
- B24529-26 https://www.dtcc.com/-/media/Files/pdf/2026/7/8/DigiCert-X9---DTC-Important-Notice.pdf

Security Exchange Commission SEC https://www.sec.gov

- OMB Number: 3235-0045 https://www.dtcc.com/-/media/Files/Downloads/legal/rule-filings/2019/DTC/SR-DTC-2019-008.pdf

Accredited Standards Committee X9 Inc.
Financial Industry Standards

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

Accredited Standards Committee X9 Inc.
Financial Industry Standards

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

Accredited Standards Committee X9 Inc.
Financial Industry Standards

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

Accredited Standards Committee X9 Inc.
Financial Industry Standards

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

Accredited Standards Committee X9 Inc.
Financial Industry Standards

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

Accredited Standards Committee X9 Inc.
Financial Industry Standards

ASC X9 Financial PKI Architecture (Conventional Cryptography)

Production mTLS certificates

- X9 Financial PKI ECC P-256 Root
- X9 Financial PKI RSA-2048 Root
- X9 Financial PKI RSA-4096 Root
  - X9 Financial PKI RSA-4096 ICA
  - X9 Financial PKI RSA-4096 ICA EU

User Acceptance Test

- X9 Financial PKI ECC P-256 Root
- X9 Financial PKI RSA-2048 Root
  - QR Code ICA RSA-2048
  - CDN / VFD ICA RSA-2048
  - ISO 20022 ICA RSAS-2048
- X9 Financial PKI RSA-4096 Root
  - CDN / VFD ICA RSA-2048

Accredited Standards Committee X9 Inc.
Financial Industry Standards

ASC X9 Financial PKI Architecture (PQC)

User Acceptance Test

- X9 Financial PKI MLDSA-87 Root
  - ICAs for MLDSA-87, -65, -44 by use case
- X9 Financial PKI MLDSA-65 Root
  - ICAs for MLDSA-65, -44 by use case
- X9 Financial PKI MLDSA-44 Root
  - ICAs for MLDSA-44, by use case

PQC Production PKI Roots

- X9 Financial PKI MLDSA-87 Root
  - ICAs for MLDSA-87, -65, 44
- X9 Financial PKI MLDSA-65 Root
  - ICAs for MLDSA-65 and -44
- X9 Financial PKI MLDSA-44 Root
  - ICA for MLDSA-44

Currently negotiating for Key Ceremony date. Expecting 4Q2026 with full production PQC support late 2026 or early 2027.

Accredited Standards Committee X9 Inc.
Financial Industry Standards

FIX Discussion, Questions

How can ASC X9 Financial PKI work with FIX and / or its members?

Would it be beneficial to hold regular ASC X9 Financial PKI / FIX meetings?

ASC X9 Financial PKI includes an X9 PKI Industry Forum the second Monday of each month. Everyone is welcome to join the Industry Forum and attend the Forum Meetings.

Accredited Standards Committee X9 Inc.
Financial Industry Standards

References and Links

- ASC X9 https://x9.org
- ANSI https://www.ansi.org
- ISO TC68 https://www.iso.org/committee/49650.html
- X9 Financial PKI https://x9.org/pki-home/
- X9 PKI certificates – DigiCert

  https://knowledge.digicert.com/general-information/community-root-authority-certificates#X9Certificates
- CA Browser Forum https://cabforum.org/

Accredited Standards Committee X9 Inc.
Financial Industry Standards