Transition of Public Key Infrastructure (PKI) to Post Quantum Cryptograph (PQC): Plan for Next Five Years

12-07-2024

TABLE OF CONTENTS

Contents

1 Introduction

1.1 Background

Quantum computing is likely to become a reality. This is due to research efforts by the various Governments, Industries, and Academia. Companies such as Google, IBM, Nokia, have made progress in the development of the quantum computers.

In the Evolving context of Advances in the development of Quantum Computing it is important to ensure the traditional cryptosystems are resilient to adversaries from such environment.

While quantum computers exist today; they are not robust enough to solve practical problems. The current public key cryptography in use is based on the following algorithms: 2048-bit RSA; P-256 Elliptic Curve (EC); and SHA-256. These are being leveraged by various standards and protocols likeTLS/mTLS, MQTT, Mobile NFC, sFTP, FTPS, DNSSEC, DOH/DOT, SSH, RDP, DMARC, DKIM, SPF, Kerberos, LDAPS, EAP-TLS, WPA, SAML, Oauth, Open ID Connect, IPSec, IKE, PGP & S/MIME. It is foreseen that sometime in the future, quantum computers robust enough to break public key cryptography will become a reality. While exact year is hard to predict, this may happen sometime in 2035.

Most current public key cryptography and Public Key Infrastructure (PKI) in use today is based on computational complexity of integer factorization (RSA); of solving discrete logarithm problem in finite field (Diffie-Hellman or DH); or of solving discrete logarithm problem in EC field (EC). A sufficient large quantum computer can break many of these schemes using Shor's Algorithm. In order to enable the classical systems to be resilient against quantum adversaries the Unites States of America's (USA) National Institute for Standards and Technology (NIST) is in the process of standardizing the public key cryptographic algorithms that are likely to be secure against the threat of quantum computers. In this document, we call these algorithms as Post-Quantum Cryptography (PQC) algorithms.

While such robust quantum computer may impact present day asymmetric crypto scheme it may not likely to have as much of an impact to the present day symmetric key schemes such as AES encryption and SHA-2, SHA-3 hashing algorithms.

It is in this context this document is bringing out the overall transition strategy from classical computing environment to quantum resilient environment

1.2 Purpose

Controller of Certifying Authorities play a key role as trusted anchor for the digital transactions in the country. The purpose of this document is to bring out the overall strategy and five-year plan by the Controller of Certifying Authorities (CCA) towards transition to PQC based Quantum resilient environment.

This document also brings out summary of PQC algorithms that are in standardization process at global level and Commercial-Off-The-Shelf (COTS) available solutions.

The detailed discussion about the internal aspects of PQC schemes and quantum computing are beyond the scope of this document. It may also be noted that the said document shall get amended time to time depending on the advancements in the field of PQC.

The overall document is organized such a way that Section-2 brings out the current state of PQC standardization, Section-3 on strategy for transition to PQC, Section-4 on Recommendations & Transition in phases.

2 Post Quantum Cryptography

Challenge for Traditional Cryptosystems

In the Evolving context of Advances in the development of Quantum Computing it is important to ensure the traditional cryptosystems are resilient to adversaries from such environment. It is widely believed that a scalable quantum computer, capable of implementing algorithms like Shor's, can break the traditional public key cryptographic schemes [1]. The security of these schemes depends on the hardness of the underlying problems of factoring and finite field discrete log.

Current state of Quantum Computers is Noisy intermediate-scale quantum era where issues pertaining to sensitivity, decoherence, error correction, etc., are still in the areas of research. Hence, development of robust quantum computers is still an ongoing work and it may expected be available by end of this decade. Robust quantum computer is required to break the important cryptographic standards used today [2].

Post Quantum Cryptography (PQC)

To address the above challenge, it is required to device a stronger cryptosystem that can be resilient to attacks from quantum adversaries. Towards the same NIST of the USA is running a competition to finalize a portfolio of post quantum cryptosystems. These cryptosystems are expected to replace the corresponding, existing ones in various protocols, applications and devices. Two main aspects of the challenge include devising post quantum crypto system for (a) Digital Signatures and (b) Key Encapsulation/Encryption Mechanisms.

In a nutshell, PQC provides replacements for RSA / DH / DSA cryptosystems, for achieving the corresponding functionality, but providing extra guarantee in terms of security against quantum-enabled adversary. The focus of this document will dwell upon post quantum cryptography for digital signature purposes.

2.1 Current State of PQC Algorithms for Key Encapsulation Mechanism (KEM)

- **CRYSTALS-Kyber [3]:** Kyber is also Module Learning With Errors (MLWE) based scheme used for KEM. The details of the same is available in draft FIPS-203 [4].

2.2 Current State of PQC Algorithms for Digital Signature

The current state of PQC standardization under NIST for Digital Signature schemes is given below.

- **CRYSTALS-Dilithium [5]:** Dilithium is also Module Learning with Errors (MLWE) based scheme used for digital signatures. The details of the same is available in draft FIPS-204 [6].
- **Falcon [7]:** Falcon is also MLWE based digital signature scheme. Draft FIPS for Falcon has not yet been published. Falcon may not be suitable for all users since it requires the use of reliable and constant-time 64-bit floating-point operations.
- **SPHINCS+ [8]:** SPHINCS+ is stateless hash-based signature scheme. It is documented in draft FIPS-205 [9].

Type of Cryptography	KEM	Signature
Lattice	CRYSTALS-KYBER	CRYSTALS-DILITHIUM
		FALCON
Hash Based		SPHINCS+

2.3 New Call for Round-1 Additional Submissions

Considering the chosen PQC algorithms based on Lattice based, NIST is currently evaluating additional signature schemes based on other hard problems of multivariate, isogeny, code based, etc [10].

Type of Cryptography	PKE/KEM
Code Based	Classic McEliece BIKE HQC
Super Singular Elliptic Curve Isogeny	SIKE

2.4 Related Signature Schemes

The following stateful hash-based signature schemes are documents in NIST Special Publication (SP) SP800-208:

One is eXtended Merkle Signature Scheme (XMSS). It is also documented in Internet Research Task Force (IRTF) RFC 8391.

Another scheme documented in IRTF RFC 8554 is Leighton-Micali Signature (LMS). These schemes are not recommended for general use because they require careful state management and ensuring no reuse of the signature keys. They are recommended only when the need to implement the PQC signature scheme is now and it will be difficult to transition to new signature scheme (e.g., in firmware update signature verification for deployed constrained devices).

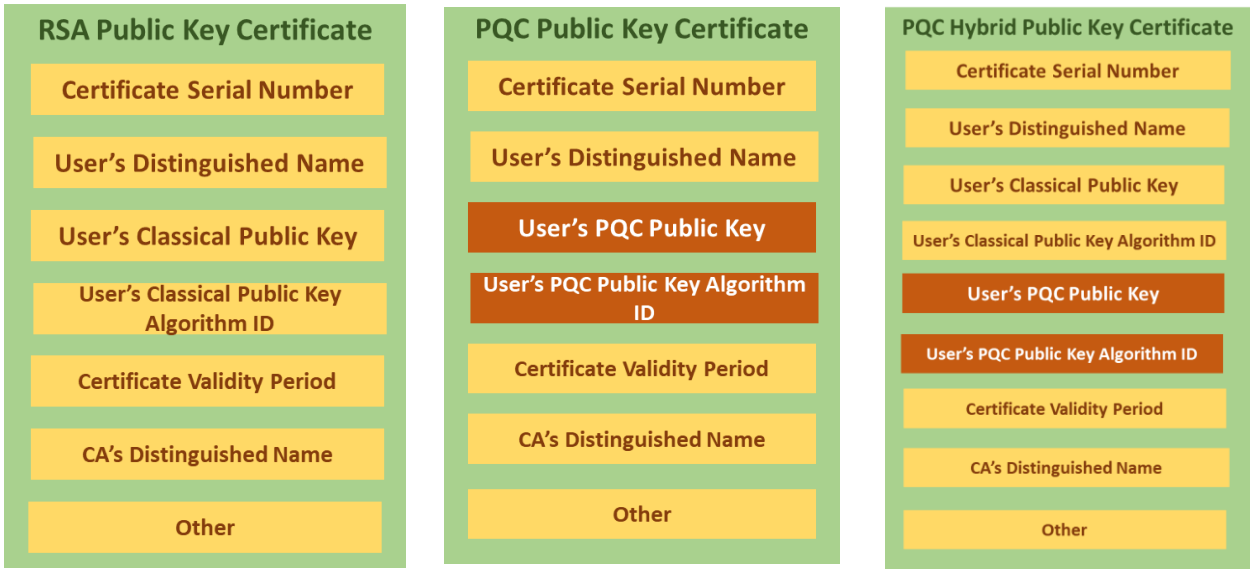
2.5 Current State of PQC in PKI

There are several ongoing efforts related to adoption of PQC for PKI & related use cases in various IETF forums such as LAMPS [11] and PQUIP [12].

Different approaches related to the PQC migration plan are being discussed and considered for standardization, some of the approaches are as given below are within X.509 certificate standards [13]:

2.5.1 Pure PQC

This entails issuing PQC certificates just like RSA or ECDSA certificates. The Subject Public Key Information (SPKI) and Signatures will be those suitable for applicable PQC certificate.



The details of this format can be found in the following documents

- RFC 5280 [14]
- draft-ietf-lamps-dilithium-certificates [15]
- draft-ietf-lamps-kyber-certificates [16]

2.5.2 Hybrid Concatenated

This X.509 certificate is a hybrid certificate. It basically concatenates the classic and post-quantum objects without changing the structure of the ASN.1 tree:

For the algorithm identifier, a specific OID for the selected combination of traditional + post-quantum algorithm is used.

Keys and signatures follow the usual ASN.1 syntax, except the byte string corresponds to the concatenation of a traditional and a post-quantum object.

2.5.3 Hybrid Bound

The details of this format can be found in the following:

- draft-becker-guthrie-cert-binding-for-multi-auth [17]

2.5.4 Hybrid Composite

The details of this format can be found in the following documents:

- draft-ounsworth-pq-composite-sigs [18]
- draft-ietf-lamps-pq-composite-kem [19]

2.5.5 Hybrid Delta Extensions (Chameleon)

The details of this format can be found in the following documents:

- draft-truskovsky-lamps-pq-hybrid-x509 [20]

- ITU-T X.509 (10/2019) [21]

2.5.6 Hybrid Using Extensions (Catalyst)

The details of this format can be found in the following:

- draft-bonnell-lamps-chameleon-certs [22]

2.6 Current State of PQC Protocols

Existing protocols such as, Transport Layer Security (TLS) and Cryptographic Message Syntax (CMS) based Secure/Multipurpose Internet Mail Extensions (S/MIME), might need to be modified to handle larger PQC certificates, signatures and key sizes.

How PQC will be retrofitted in TLS can be tracked via the IETF TLS working group located at https://datatracker.ietf.org/wg/tls/documents/

How S/MIME will be retrofitted with PQC can be tracked via IETF LAMPS working group located at https://datatracker.ietf.org/wg/lamps/documents/

Another useful resource is the IETF PQC working group located at https://datatracker.ietf.org/wg/pquip/documents/

CCA is encouraged to work through the vendors to ensure that their products incorporate secure, standard-compliant, interoperable PQC and attendant protocols.

3 Strategy for Transition

In this section we explore when the CCA should transition.

There are no known COTS deployments of PQC. CCA should work with the COTS vendors through the CCA approved Certification Authorities (CAs) to determine what their plans are for transition to PQC and using COTS software, Hardware Security Modules (HSM), and tokens that implement one or more of these algorithms.

Transition to PQC can be expected to happen in the coming years at global level. There are already ongoing efforts from browsers and applications to adopt PQC mechanisms for secure communication through PQC based KEM. Protocols like SSL and TLS use public key cryptography. Specialized protocols like VPN and 5GPP depend on them. The Certification Authority service (CA) depends on standards for public key cryptography like X.509. Dongles and Hardware Security Modules (HSM) are used for providing PKI- based authentication services. Trusted Execution Environment (TEE) too uses PKI for certificate management. Thus, migration to PQC would touch upon citizen-centric services, internet protocols, browser, OS security, IoT security, mobile security and hardware security.

3.1 Implications for CCA

CCA shall carryout stakeholder consultation regarding the overall transition to PQC to enable agencies get equipped for the same. CCA should wait until it needs to make a decision on transition to PQC before surveying the CAs and IT vendors used by the CA as to what approach to take. It is likely that by the time CCA needs to plan the transition to PQC, these issues will be sorted out through the standardization and product development process.

3.2 Potential Use cases & Certificates

In general, there are three security applications of cryptography: entity authentication; digital signature (source authentication, data integrity, and support for non-repudiation); and encryption to support confidentiality. We examine if they require any lead time to preserve security.

Generally, entity authentication applications do not require any lead time since entity authentication is done in real-time.

Generally, digital signature applications require some lead time since signature is verified at a later date. This can be on the order of days to years. CCA and its users should determine how long this lead time is. It should be noted that this is not a catastrophic situation since data can always be re-signed using more robust algorithms when a given algorithm is compromised, be it due to advent of practical quantum computers or otherwise.

Encryption/confidentiality applications are harder to deal with. Confidential data protected using encryption are vulnerable to an attacker or adversary via a simple capture now and decrypt later threat. Thus, if data needs to be confidentiality protected for "n" years after the creation of encrypted payload, and break of traditional algorithms is "m" years away, m always needs to be greater than n, which may not be possible if quantum computers become a reality. Given that the quantum computers are likely to become a reality, confidentiality protection requires transition to PQC algorithms to be completed by the year 2035-n, assuming 2035 as the start of the use of quantum computers to break traditional algorithms.

In the following subsections, we examine the nine types of certificates CCA PKI issues for the required lead time for PQC transition.

3.2.1 End User Certificate (issued for personal use)

These certificates are used for affixing individuals' Electronic Signature (E-Sign). We will assume that three-year lead time is sufficient to allow signers to re-sign the documents using stronger algorithms. Thus, starting in 2032, end users will need PQC certificates.

3.2.2 End User Certificate (issued for organization use)

These certificates are used for affixing individuals' Electronic Signature (E-Sign) on behalf of the organization. We will assume that three-year lead time is sufficient to allow signers to re-sign the documents using stronger algorithms. Thus, starting in 2032, end users will need PQC certificates.

3.2.3 System Certificate Machine to machine authentication

These certificates are used for real-time device authentication and can be issued as late as starting 2035.

3.2.4 Time Stamping Authority Certificate Generating Timestamp Token

Time stamps will need to be reapplied to objects. We assume Timestamp authority is centralized function. We also assume that the number time stamps that need to be transitioned are in hundreds of thousands to less than ten million. We think this can also occur in three years' time. Thus, starting in 2032, Time Stamp Authorities will need PQC certificates.

3.2.5 Code Signing Certificate Signing of software code

These certificates are used for affixing digital signatures. We also assume these do not include firmware or software that cannot be retrofitted with new signature verification firmware or software. We will assume that three-year lead time is sufficient to allow signers to re-sign the code using stronger algorithms. Thus, starting in 2032, code signers will need PQC certificates.

3.2.6 OCSP Responder Certificate OCSP response Signature

OCSP Signature certificates will transition to the stronger algorithms at the same time as the CAs.

3.2.7 Encryption Certificate Key Encryption

We assume that these certificates are needed to encrypt e-mail. The lead time required to preserve confidentiality of information is very much user and usage dependent. CCA may not be in a position to provide guidance in this area. Some form of user input is required to make an educated guess and estimated the time encryption certificates are required.

3.2.8 Document Signer Certificate Organizational application signature

These certificates are used for affixing digital signatures. We will assume that three-year lead time is sufficient to allow signers to re-sign the documents using stronger algorithms. Thus, starting in 2032, end users will need PQC certificates.

3.2.9 SSL Certificate Secure Communication

Server and client authentication aspects of TLS do not require much lead time since these actions are in real-time. The lead time required to preserve confidentiality of information is very much TLS application dependent. Some form of input from the electronic business industry like banks and e-commerce industry may be required to protect the data.

A possible scenario to protect against confidentiality breach is as follows:

1) The transition to TLS.
2) TLS Servers are advised to advise customers to change their password when the transition occurs obsoleting the harvesting of passwords sent using TLS communications protected using traditional algorithms.
3) Banking and other industry applications (e-commerce, insurance, etc.) are advised to change sensitive information such as user account numbers, credit and debit card numbers to protect against data harvesting. Note this need not result in physical card or account information to change. The change can only be for electronic transactions. Further thought and industry participation is required in this area.

The CAs, including the Root CAs, Intermediate CAs, and OCSP Responders, should start issuing PQC certificate and revocation information when the earliest of these applications requires. That could be as early as 2030.

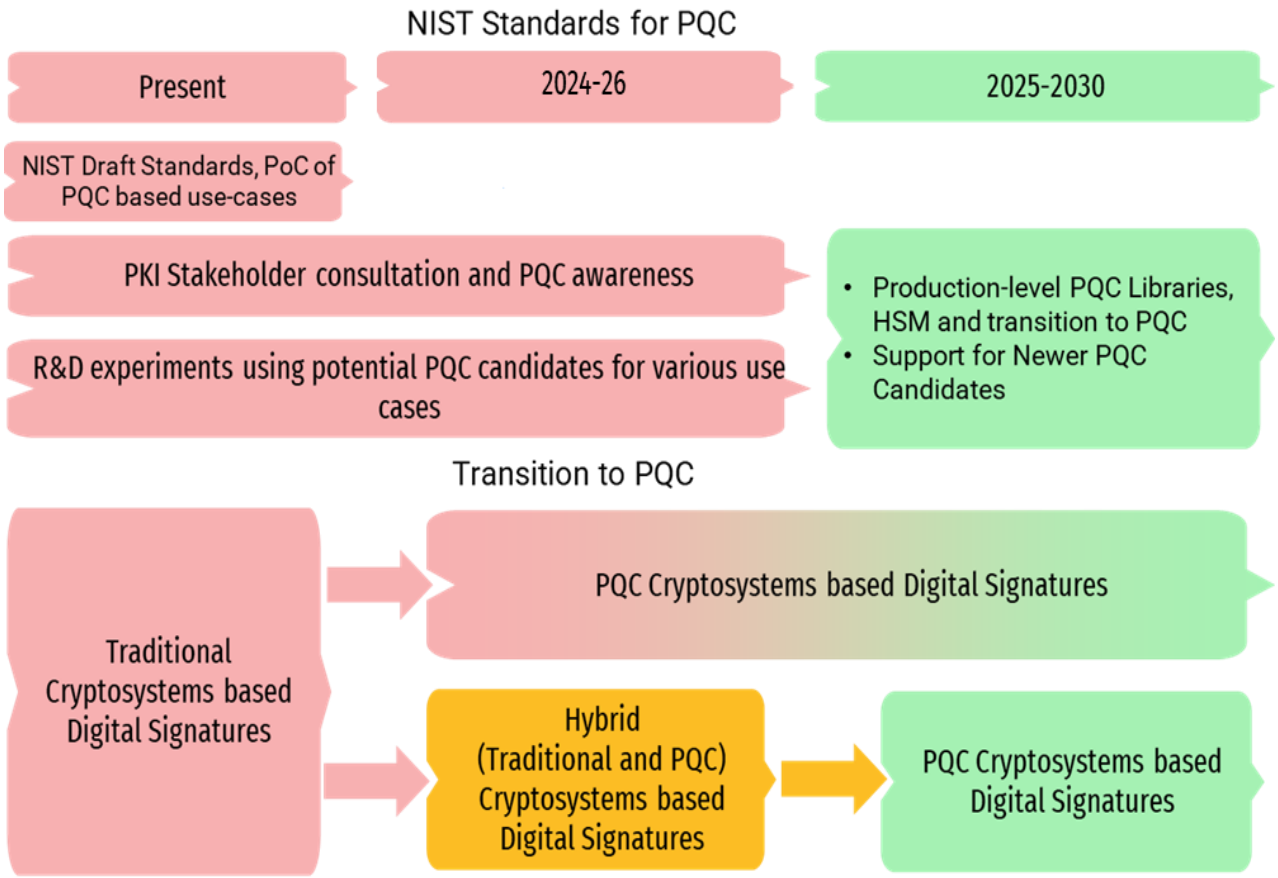
Hence, a PQC action plan should be drawn by India PKI, in consultation with Industry, Experts, User agencies & Academia towards evolving a viable solution for adoption of PQC in India.

Many formats are been proposed based on current X.509 certificate structure to PQC. Some of them are pure PQC - transporting only a PQC public key and signed by a PQC signature algorithm. There are also proposed hybrid approaches being considered that both traditional and PQC public keys and signed by both traditional and PQC signature algorithms.

NIST has published three documents outlining the need and plan for migration to PQC [23]. They are:

- Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography
- Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery
- Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standards

At national level there are similar efforts being carried out including proof of concepts implementations for specific use cases such as workflow automation & PKI applications. There are possible approaches such as direct migration to PQC or stepwise migration through hybrid model. Depending on the criticality of use-cases the overall transition plan needs to be firmed up in coming months. Indicative activities towards the same given in the Figure.



Approaches & Activities towards Transition to PQC

There are several ongoing efforts towards migration to PQC in the Internet in terms of PKI which can be tracked in the IETF LAMPS working group [11]. Similarly, Recommendation of ITU-T are available on Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. The ITU-T has already standardized hybrid (multiple-algorithms) certificates in Section 9.8 of [12].

Hybrid approaches are being discussed in several forms including IETF where drafts are being evolved. One of the key considerations is about the type and the internals of digital signature certificates used for various purposes. Accordingly, we see a lot of traction towards the following types of certificates.

Different approaches related to the PQC migration plan are being discussed and considered for standardization, some of the approaches are as given below are within X.509 certificate standards [9]:

- Pure PQC Certificate
- Hybrid Certificate

4 Recommendations

4.1 Phase-1 (2024-26)

Phase-1 recommendations are for the immediate actions

4.1.1 Stakeholder consultation & Capability Development

- **User Education**
  Educate the users that by the end of 2030, signature made using 2048-bit RSA cannot be trusted and E Sign, documents, code and time stamps must be re-signed using NIST standardized algorithms.

  Also, educate the users that by 2025-2030 time-frame, NIST standardized algorithms will be used. The users must keep their platforms up-to-date to ensure availability of the latest algorithms. The users must ensure home-grown applications can be retrofitted with latest algorithms and key sizes.

- **Awareness creation**
  Create awareness among the citizens about effect of Quantum computers on classical algorithms like RSA & ECC and need of migration of the cryptosystems towards NIST standardized algorithms.

- Protocol awareness with developers towards the transition

4.1.2 Contribution to Standardization Process

- Participation & Contribution in International & National PQC Standardization initiatives
- Evolve frameworks/algorithms for design, development and testing of PQC primitives
- Involvement in International meeting and discussions related to Post Quantum Cryptography (PQC) Migration Plan and Roadmap

4.1.3 R&D Experiments

- **PQ-VPN & PQ-Browser**
  R&D experiments can be carried out to migrate the classical crypto based Virtual Private Network (VPN) & Browser to Post Quantum Resilient VPN & Browser.
- **Post Quantum PKI Solutions**
- **PQC for IoT applications**
  - CCTV using lightweight CBOR encoded X.509 certificates
  - Vehicle to Everything (V2X)
  - Drone using post quantum algorithms like ASCON-80pq
- **Hardware Root of Trust attestation service**
  Integration of NIST PQC standardized algorithms in Hardware Root of Trust attestation service
- **Post Quantum in Protocols**
  Design and development of following PQC based protocols
  - Secure Shell (SSH)
  - Secure File Transfer Protocol (SFTP)
  - Cryptographic Message Syntax (CMS)
  - Hybrid Public Key Encryption in Transport Layer Security (TLS)
  - Quick UDP Internet Connections (QUIC)
  - Pretty Good Privacy (PGP)
  - Messaging Layer Security (MLS)
  - Datagram Transport Layer Security (DTLS)
  - Post-quantum XML and SAML Single Sign-On
- **PQ Library**
  Develop and implement NIST standardized algorithms by Academia, R&D & Industry

4.2 Phase-2 (2025-30)

Initiatives towards development of the following by Academia, R&D & Industry

- User Education, Awareness & Capability building towards migration to PQC standards
- **Trusted Execution Environment (TEE)**
  Implementation of the NIST standardized algorithms to ensure Quantum resistant TEE
- **Dongle**
  Dongles are external devices are used for signing-in on websites which relies on classical cryptography-based algorithms. Usage of PQ enabled dongles will make the signing process robust against quantum attacks
- **Hardware Security Module**
  HSM are to be designed in accordance NIST standards for PQC algorithms with firmware upgrades to add any other new PQC algorithms as soon as they are standardized and proven

- **Production level PQ Library**
  Develop and implement NIST standardized algorithms by Academia, R&D & Industry.

- **TLS Version**
  CA vendors, CCA website and TLS Server certificate subscribers and relying parties need to immediately start using the following:

  1) Only use TLS 1.2 and TLS 1.3
  2) For TLS 1.2, only use the TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 { 0xC0, 0x30 } cipher-suite (specified in RFC 8422)
  3) For TLS 1.3, only use the TLS_AES_256_GCM_SHA384 {0x13,0x02} cipher-suite (specified in RFC 8446)
  4) For TLS 1.3, use Supported group secp384r1(0x0018) for ephemeral Elliptic Curve Diffie-Hellman key exchange

  These recommendations are made in order to improve the security posture of TLS. Data exchanged using these configurations, even when using RSA 2048-bit certificates will be secure for decades beyond 2030 if the adversary does not have quantum computers at their disposal.

5 Document Updates

As and when the forum releases the updates related to PQC protocols this document will be updated.

6 References:

[1] Peter W. Shor (AT&T Research), *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J.Sci.Statist.Comput. 26 (1997) 1484 https://arxiv.org/abs/quant-ph/9508027

[2] The PQC Migration Handbook, Applied Cryptography And Quantum Algorithms Cryptology Group Netherlands National Communications Security Agency https://publications.tno.nl/publication/34641918/oicFLj/attema-2023-pqc.pdf

[3] CRYSTALS KYBER https://pq-crystals.org/kyber/

[4] FIPS 203 (Initial Public Draft): Module-Lattice-Based Key Encapsulation Mechanism https://csrc.nist.gov/pubs/fips/203/ipd

[5] CRYSTALS DILITHIUM https://pq-crystals.org/dilithium/

[6] FIPS 204 (Initial Public Draft): Module-Lattice-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/204/ipd

[7] Falcon (Fast-Fourier Lattice-based Compact Signature over NTRU) https://falcon-sign.info/

[8] SPHINCS$^+$: Stateless hash-based signatures https://sphincs.org/

[9] FIPS 205 (Initial Public Draft) Stateless Hash-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/205/ipd

[10] NIST Round 1 Additional Signatures https://csrc.nist.gov/projects/pqc-dig-sig/round-1-additional-signatures

[11] IETF Group: Limited Additional Mechanisms for PKIX and SMIME (LAMPS) https://datatracker.ietf.org/wg/lamps/documents/

[12] IETF Group: Post-Quantum Use In Protocols (PQUIP) https://datatracker.ietf.org/wg/pquip/about/

[13] NIST SPECIAL PUBLICATION 1800-38C: Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standards https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf

[14] RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile https://datatracker.ietf.org/doc/html/rfc5280

[15] Internet X.509 Public Key Infrastructure: Algorithm Identifiers for ML-DSA https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates/

[16] Internet X.509 Public Key Infrastructure - Algorithm Identifiers for Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) https://datatracker.ietf.org/doc/draft-ietf-lamps-kyber-certificates/

[17] Related Certificates for Use in Multiple Authentications within a Protocol https://datatracker.ietf.org/doc/draft-becker-guthrie-cert-binding-for-multi-auth/

[18] Composite ML-DSA for use in Internet PKI https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs/

[19] Composite ML-KEM for Use in the Internet X.509 Public Key Infrastructure and CMS https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-kem/

[20] Multiple Public-Key Algorithm X.509 Certificates https://datatracker.ietf.org/doc/html/draft-truskovsky-lamps-pq-hybrid-x509-02

[21] Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. Standard, ITU-T, Geneva, Switzerland, October 2019

[22] A Mechanism for Encoding Differences in Paired Certificates https://datatracker.ietf.org/doc/draft-bonnell-lamps-chameleon-certs/

[23] NIST Migration to Post-Quantum Cryptography https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms