NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Migration to Post-Quantum Cryptography Project

Session XI – Panel – Interoperability and Performance

April 2024

SESSION XI – INTEROPERABILITY AND PERFORMANCE PANEL

Moderator:

Christian Paquin - Principal Research Engineer at Microsoft

Panelists:

Jim Goodman, Co-Founder, CTO at Crypto4A Technologies

John Gray, Software Developer (Architect) at Entrust

Volker Krummel, Chapter Lead PQC at Utimaco

Migration to Post-Quantum Cryptography (PQC)
Project Goal

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Initiating the development of practices to ease migration from the current set of public-key cryptographic algorithms to new standardized algorithms published by NIST that are resistant to quantum computer-based attacks

Migration to PQC Project CRADA Collaborators

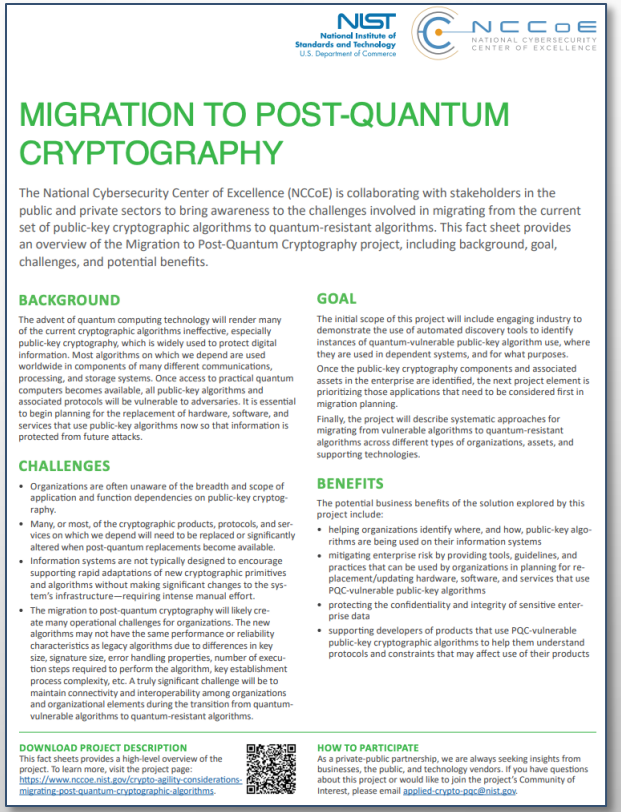
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- Amazon Web Services, Inc. (AWS)
- Cisco Systems, Inc.
- Cybersecurity and Infrastructure Security Agency (CISA)
- Cloudflare, Inc.
- Crypto4A Technologies, Inc.
- CryptoNext Security
- Dell Technologies
- DigiCert
- Entrust
- HP, Inc.
- HSBC
- IBM
- Information Security Corporation
- InfoSec Global
- ISARA Corporation
- JPMorgan Chase Bank, N.A.
- Keyfactor
- *Kudelski IoT*
- *Microsoft*
- *National Security Agency (NSA)*
- *NXP Seminconductors*
- *Palo Alto Networks*
- *PQShield*
- *QuantumXChange*
- *SafeLogic, Inc.*
- *Samsung SDS Co., Ltd.*
- *SandboxAQ*
- *Santander*
- *SSH Communications Security Corp*
- *Thales DIS CPL USA, Inc.*
- *Thales Trusted Cyber Technologies*
- *Utimaco*
- *Verizon*
- *VMware, Inc.*
- *wolfSSL*

MIGRATION TO PQC PROJECT FOCUS

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- **Complement NIST PQC standardization effort**
- Tackle challenges with adoption, implementation, and deployment of PQC
- Engage with the community including industry collaborators and across government to bring awareness to the issues involved in migrating to post-quantum algorithms
- Coordinate with standard developing organizations and government and industry sectors community to develop guidance to accelerate the migration
- Support US Government PQC initiatives (White House NSM-10 (M-23-02), CISA, NSA CNSA 2.0, etc.)



NIST National Institute of Standards and Technology U.S. Department of Commerce | NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

The National Cybersecurity Center of Excellence (NCCoE) is collaborating with stakeholders in the public and private sectors to bring awareness to the challenges involved in migrating from the current set of public-key cryptographic algorithms to quantum-resistant algorithms. This fact sheet provides an overview of the Migration to Post-Quantum Cryptography project, including background, goal, challenges, and potential benefits.

BACKGROUND

The advent of quantum computing technology will render many of the current cryptographic algorithms ineffective, especially public-key cryptography, which is widely used to protect digital information. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. Once access to practical quantum computers becomes available, all public-key algorithms and associated protocols will be vulnerable to adversaries. It is essential to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks.

CHALLENGES

- Organizations are often unaware of the breadth and scope of application and function dependencies on public-key cryptography.
- Many, or most, of the cryptographic products, protocols, and services on which we depend will need to be replaced or significantly altered when post-quantum replacements become available.
- Information systems are not typically designed to encourage supporting rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure—requiring intense manual effort.
- The migration to post-quantum cryptography will likely create many operational challenges for organizations. The new algorithms may not have the same performance or reliability characteristics as legacy algorithms due to differences in key size, signature size, error handling properties, number of execution steps required to perform the algorithm, key establishment process complexity, etc. A truly significant challenge will be to maintain connectivity and interoperability among organizations and organizational elements during the transition from quantum-vulnerable algorithms to quantum-resistant algorithms.

GOAL

The initial scope of this project will include engaging industry to demonstrate the use of automated discovery tools to identify instances of quantum-vulnerable public-key algorithm use, where they are used in dependent systems, and for what purposes.

Once the public-key cryptography components and associated assets in the enterprise are identified, the next project element is prioritizing those applications that need to be considered first in migration planning.

Finally, the project will describe systematic approaches for migrating from vulnerable algorithms to quantum-resistant algorithms across different types of organizations, assets, and supporting technologies.

BENEFITS

The potential business benefits of the solution explored by this project include:

- helping organizations identify where, and how, public-key algorithms are being used on their information systems
- mitigating enterprise risk by providing tools, guidelines, and practices that can be used by organizations in planning for replacement/updating hardware, software, and services that use PQC-vulnerable public-key algorithms
- protecting the confidentiality and integrity of sensitive enterprise data
- supporting developers of products that use PQC-vulnerable public-key cryptographic algorithms to help them understand protocols and constraints that may affect use of their products

DOWNLOAD PROJECT DESCRIPTION

This fact sheets provides a high-level overview of the project. To learn more, visit the project page: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project or would like to join the project's Community of Interest, please email applied-crypto-pqc@nist.gov.

MIGRATION TO PQC PRELIMINARY DRAFTS
PUBLIC COMMENT PERIOD ENDED FEBRUARY 20, 2024

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- **NIST SP 1800-38B, Quantum Readiness: Cryptographic Discovery**
  - (1) a functional test plan that exercises the cryptographic discovery tools to determine baseline capabilities;
  - (2) a use case scenario to provide context and scope our demonstration;
  - (3) an examination of the threats addressed in this demonstration;
  - (4) a multifaceted approach to start the discovery process that most organizations can start today; and (5) a high-level architecture based on our use case that integrates contributed discovery tools in our lab.

- **NIST SP 1800-38C, Quantum Readiness: Testing Draft Standards for Interoperability and Performance**
  - (1) identification of compatibility issues between quantum ready algorithms,
  - (2) resolution of compatibility issues in a controlled, non-production environment, and
  - (3) reduction of time spent by individual organizations performing similar interoperability testing for their own PQC migration efforts.

MIGRATION TO POST-QUANTUM CRYPTOGRAPHY INTEROPERABILITY & PERFORMANCE

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- Identifying interoperability and performance challenges that applied cryptographers face as they implement quantum-resistant algorithms.
  - QUIC, Transport Layer Security (TLS)
  - Secure Shell (SSH)
  - X.509 post-quantum certificate hybrid profiles to support traditional and post-quantum algorithms
  - post-quantum-related operations of next-generation Hardware Security Modules (HSMs).

INTEROPERABILITY AND PERFORMANCE WORKSTREAM WORKSTREAM

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- **INTEROPERABILITY**
  - DEMONSTRATE INTEROPERABILITY BETWEEN COLLABORATORS' SOFTWARE AND HARDWARE COMPONENTS IMPLEMENTING THE SAME ALGORITHM OR STANDARD
  - DEVELOP AND DEMONSTRATE KNOWN ANSWER TESTS (KATS) AND TEST VECTORS FOR THE NIST STANDARDIZED ALGORITHMS
- **PERFORMANCE**
  - IDENTIFY METRICS TO MEASURE (TIME, MEMORY, ETC.)
  - VARY THE DEMONSTRATION CONDITIONS (OPERATIONAL ENVIRONMENT SUCH AS ON-PREM, CLOUDS, DEVICES, VIRTUAL MACHINES, CONTAINERS, ETC.)
  - VARY THE DEMONSTRATION CRYPTO MODES SUCH AS PQC-ONLY AND HYBRID

PQC KEY AND SIGNATURE SIZES

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Scheme	Public Key (bytes)	Private Key (bytes)	Signature (bytes)	Security Level
RSA-3072	**384**	**384**	**384**	**Classical-128**
ECDSA-P256	**64**	**32**	**256**	**Classical-128**
ML-DSA-44 (Dilithium2)	**1312**	**2528**	**2420**	**PQC Category 2** *(SHA3-256)*
ML-DSA-65 (Dilithium3)	**1952**	**4000**	**3293**	**PQC Category 3** *(AES-192)*
ML-DSA-87 (Dilithium5)	**2592**	**4864**	**4595**	**PQC Category 5** *(AES-256)*
FN-DSA-512 (Falcon512)	**897**	**7553**	**666**	**PQC Category 1** *(AES-128)*
FN-DSA-1024 (Falcon1024)	**1793**	**13953**	**1280**	**PQC Category 5** *(AES-256)*

REFERENCES

- **PROJECT WEBSITE**
  - HTTPS://WWW.NCCOE.NIST.GOV/CRYPTO-AGILITY-CONSIDERATIONS-MIGRATING-POST-QUANTUM-CRYPTOGRAPHIC-ALGORITHMS
- **PROJECT COMMUNITY OF INTEREST (COI)**
  - WHO SHOULD BE IN OUR COMMUNITY OF INTEREST?
  - REQUEST TO JOIN EMAIL: APPLIED-CRYPTO-PQC@NIST.GOV
- **CONTACT THE PQC PROJECT TEAM**
  - APPLIED-CRYPTO-PQC@NIST.GOV
- **BILL NEWHOUSE**
  - WILLIAM.NEWHOUSE@NIST.GOV