NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

MIGRATION TO POST-QUANTUM CRYPTOGRAPHY (PQC)

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 replacement algorithms that are resistant to cryptographically relevant quantum computer-based attacks. This fact sheet provides an overview of the Migration to Post-Quantum Cryptography project.

BACKGROUND

Once access to a cryptoanalytically-relevant quantum computer becomes available, all public-key algorithms and associated protocols which are widely used to protect digital information 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.

CHALLENGE

- Organizations are often unaware of the breadth and scope of application and function dependencies on public-key cryptography.
- Many 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 with agility to encourage supporting rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system’s infrastructure—requiring intense manual effort.
- 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

To Initiate the development of practices to ease migration from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to quantum computer-based attacks.

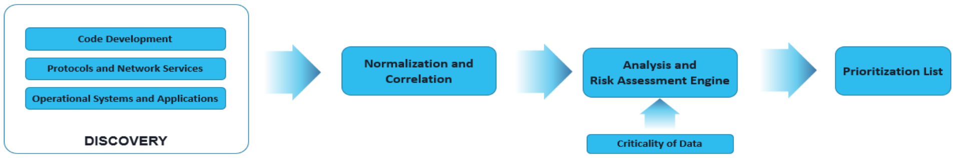
BENEFITS

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 with a renewed focus on how long it needs to be protected.
- 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.

PROJECT WORKSTREAMS

Discovery: Bringing together discovery tools to detect and report the presence and use of quantum vulnerable cryptography with enough detail and context to inform risk analysis and remediation.


Code Development
Protocols and Network Services
Operational Systems and Applications
DISCOVERY
Normalization and Correlation
Analysis and Risk Assessment Engine
Criticality of Data
Prioritization List

Interoperability: Identifying interoperability and performance challenges that applied cryptographers may face when implementing the first quantum-resistant algorithms NIST will standardize in 2024.

Performance: Compare algorithms, and not the implementation, by performing independent tests with each component. From these tests, document initial relative costs of using draft pure/hybrid PQC algorithms with baseline classical algorithms across various implementations.

Lessons learned from the workstreams, such as identifying gaps that exist between post-quantum algorithms and their integration into protocol implementations, will be shared with standards development organizations responsible for developing or updating standards that protect systems and related assets. Increased use of discovery tools will have the added benefit of detecting and reporting the use of cryptographic algorithms that are known vulnerable to non-quantum attacks.

TECHNOLOGY COLLABORATORS

The technology vendors participating in this project submitted their capabilities in response to an open call in the Federal Register. Companies with relevant security capabilities were invited to sign a Cooperative Research and Development Agreement with the National Institute of Standards and Technology (NIST), allowing them to participate in a consortium to build this example solution.

Amazon Web Services, Inc. (AWS)	CryptoNext Security	Information Security Corporation	National Security Agency (NSA)	Thales DIS CPL USA, Inc.
Cisco Systems, Inc.	Dell Technologies	InfoSec Global	PQShield	Thales Trusted Cyber Technologies
Cybersecurity and Infrastructure Security Agency (CISA)	DigiCert	ISARA Corporation	SafeLogic, Inc.	Utimaco
Cloudflare, Inc.	Entrust	JP Morgan Chase Bank	Samsung SDS Co., LTD	Verizon
Crypto4A Technologies, Inc.	IBM	Keyfactor	SandboxAQ	VMware, Inc.
		Microsoft	SSH Communications Security Corporation	wolfSSL

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or the NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

For more information about this project, visit:
www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms