NIST SPECIAL PUBLICATION 1800-38A

Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography

Volume A:
Executive Summary

William Newhouse
Murugiah Souppaya
National Institute of Standards and Technology
Rockville, Maryland

William Barker
Dakota Consulting
Silver Spring, Maryland

Chris Brown
The MITRE Corporation
Mclean, Virginia

April 2023

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

Executive Summary

Advances in quantum computing could compromise many of the current cryptographic algorithms being widely used to protect digital information, necessitating replacement of existing algorithms with quantum-resistant ones. Previous initiatives to update or replace installed cryptographic technologies have taken many years, so it is critical to begin planning for the replacement of hardware, software, and services that use affected algorithms now so that data and systems can be protected from future quantum computer-based attacks.

NIST has been soliciting, evaluating, and standardizing quantum-resistant public-key cryptographic algorithms (https://csrc.nist.gov/projects/post-quantum-cryptography). To complement this effort, the NIST National Cybersecurity Center of Excellence (NCCoE) is engaging with industry collaborators and regulated industry sectors and the U.S. Federal Government to bring awareness to the issues involved in migrating to post-quantum algorithms and to prepare the crypto community for migration.

As the project progresses, this preliminary draft will be updated, and additional volumes will also be released for comment.

CHALLENGE

Many of the cryptographic products, protocols, and services used today, in particular those using public-key algorithms like Rivest-Shamir-Adleman algorithm (RSA), Elliptic Curve Diffie Hellman (ECDH), and Elliptic Curve Digital Signature Algorithm (ECDSA), need to be updated, replaced, or significantly altered to use quantum-resistant algorithms. Many public-key algorithms and the protocols that use them will be vulnerable to attacks. A majority of today's information and communication technology systems are not designed to support rapid adaptations of new cryptographic algorithms without making significant changes to the systems' components.

Furthermore, organizations are often unaware of the breadth and scope of application and functional dependencies on public-key cryptography within their products, services, and operational environments. As a result, an organization may not have complete visibility into and a full inventory of the use of cryptography across their organization. Having a complete inventory of key partners (Software as a Service, software vendors, etc.), where cryptography is being used (on-premises, over public internet, etc.) and what data is associated with those relationships will be instrumental to understand how to prioritize migration.

The new algorithms will likely not be drop-in replacements for the quantum-vulnerable algorithms. They may not have the same performance or reliability characteristics due to differences in key size, signature size, error handling, number of execution steps required to perform the algorithm, key establishment process complexity, etc. Maintaining connectivity and interoperability among organizations and organizational elements during the transition from quantum-vulnerable algorithms to quantum-resistant algorithms will require careful planning. Furthermore, an organization may not have complete control over its cryptographic mechanisms and processes so that they can make accurate alterations to them without involving intense manual effort.

OUTCOME

This project will initially develop example implementations, guidance, and recommended practices. Next, the project will demonstrate these examples supporting various use case scenarios. The findings from the demonstrations will be published in this practice guide, a NIST 1800-series Special Publication that is composed of multiple volumes targeting different topics and audiences defined by workstreams. The initial workstreams are scoped to the following:

- Exploring the use of discovery tools to detect and report the presence and use of quantum-vulnerable cryptography in systems and services, and the use of output from the tools to inform risk analysis for prioritizing actions to move away from quantum-vulnerable cryptography.
- Identifying interoperability and performance challenges that applied cryptographers may face when implementing the first quantum-resistant algorithms NIST will standardize in 2024. Initial interoperability and performance testing will incorporate QUIC, Transport Layer Security (TLS), Secure Shell (SSH), X.509 post-quantum certificate hybrid profiles to support traditional and post-quantum algorithms, and post-quantum-related operations of next-generation Hardware Security Modules (HSMs).

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. Further, our strategy for future phases will build iteratively to produce recommended practices for algorithm replacement, where in some cases interim hybrid implementations are necessary to maintain interoperability during migration.

We invite feedback from the larger PQC community of interest to identify future workstreams that will accelerate the adoption and deployment of PQC.

This preliminary practice guide can help your organization:

- Identify where, and how, public-key algorithms are being used on information systems
- Mitigate enterprise risk by providing tools, guidelines, and practices that can be used by organizations in planning for replacement/update of hardware, software, and services that use quantum-vulnerable public-key algorithms
- Develop a risk-based playbook for migration involving people, processes, and technology

This preliminary practice guide can help product and service producers:

- Perform interoperability and performance testing for different classes of technology
- Strengthen cryptographic discovery tools to produce actionable reports
- Understand the potential impact that transitioning from quantum-vulnerable algorithms could have on their products and services

SOLUTION

The initial drafts for the Migration to Post-Quantum Cryptography project will demonstrate tools for the discovery of quantum-vulnerable algorithms in the following use case scenarios:

- Vulnerable algorithms used in cryptographic code or dependencies during a continuous integration/continuous delivery development pipeline
- Vulnerable algorithms used in network protocols, enabling traceability to specific systems using active scanning and historical traffic captures
- Vulnerable algorithms used in cryptographic assets on end user systems and servers, to include applications and associated libraries

The result will be a practical demonstration of technology and tools that can support organizations that use vulnerable public-key cryptography today in their planning of a migration roadmap using a risk-based approach.

In tandem, industry collaborators will publish results/observations/findings from the interoperability and performance workstream in the form of additional practice guide volumes, white papers, or NIST Internal Reports (IRs) to mitigate the gaps and accelerate the adoption of post-quantum algorithms into the products, protocols, and services.

The following is a list of the collaborating organizations:

Consortium Members	
Amazon Web Services, Inc. (AWS)	JPMorgan Chase Bank, N.A.
Cisco Systems, Inc.	Microsoft
Crypto4A Technologies, Inc.	National Security Agency (NSA)
CryptoNext Security	PQShield
Dell Technologies	Samsung SDS Co., Ltd.
DigiCert	SandboxAQ
Entrust	Thales DIS CPL USA, Inc.
IBM	Thales Trusted Cyber Technologies
Information Security Corporation	VMware, Inc.
InfoSec Global	wolfSSL
ISARA Corporation	

While the NCCoE is using a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief information security and technology officers can use this part of the guide, *NIST SP 1800-38a: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Future releases of this publication will include guidance to assist people in the following roles:

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-38b: Approach, Architecture, and Security Characteristics,* which describes what we built and why, including the risk analysis performed and the security/privacy control mappings.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-38c: How-To Guides*, which provide specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at applied-crypto-pqc@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order 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 NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.