ETSI/IQC Quantum Safe Cryptography Event

NIST NCCoE MIGRATION TO POST-QUANTUM CRYPTOGRAPHY PROJECT

Murugiah Souppaya

14/02/22

Agenda

- Introduction the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE)
- NCCoE Migration to PQC project
  - Discovery Workstream
  - Interoperability and Performance Workstream

NCCoE OVERVIEW

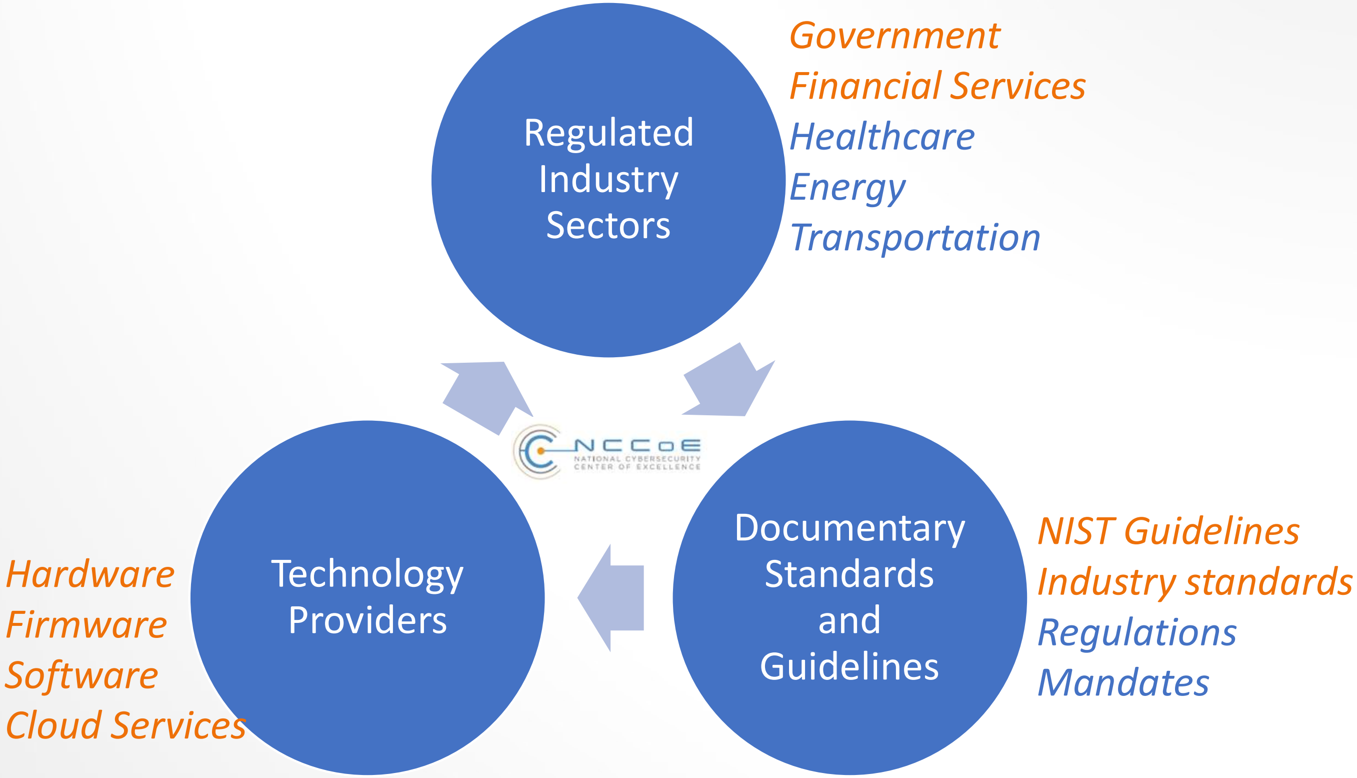
National Cybersecurity Center of Excellence (NCCoE)

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

- DEFINE
- ASSEMBLE
- BUILD
- ADVOCATE

Practice Guide SP 1800

Engagement Model



PROJECT DELIVERABLES

NIST Special Publication 1800 – Practice Guide

- **C-Suite**: executive summary
- **Architects and Infosec**: reference architecture, demonstration use cases, and security documentation
- **Operators and enginee**rs: implementation guide, bills of material, scripts, codes, tools, etc.

Other documents

- Playbooks
- Cybersecurity papers
- Update existing standards, guidelines, protocols, etc.

Open-source code

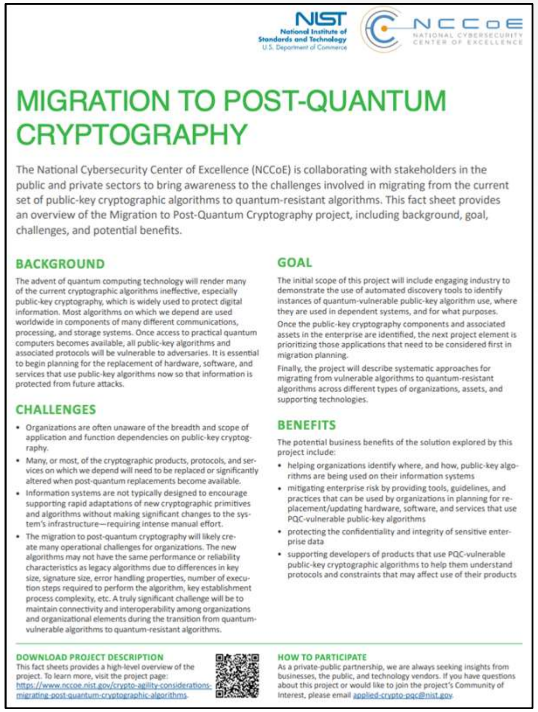
- Proof of concept code
- Infrastructure as code
- Sample applications

Outreach and Engagement

- Community of interest
- Webinars
- Public events

NCCoE– MIGRATION TO PQC PROJECT

- Complement NIST PQC standardization effort
- Support US Government PQC initiatives (White House NSM-10, DHS, etc.)
- 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
- Leverage automated tools to discover use of quantum vulnerable cryptography within an organization in hardware, firmware, software, protocols, and services and use a risk-based approach to prioritize their replacement
- Perform interoperability and performance demonstrations across different technology and protocols to include TLS, QUIC, SSH, code signing, public key certificates, hardware security modules, 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

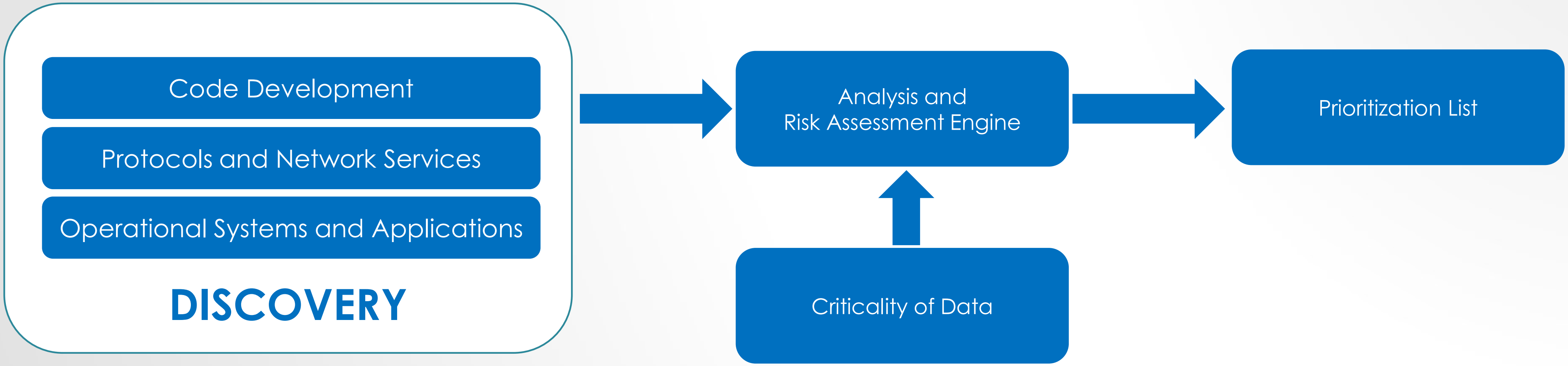
The potential business benefits of the solution explored by this project include:

- 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.

DISCOVERY WORKSTREAM

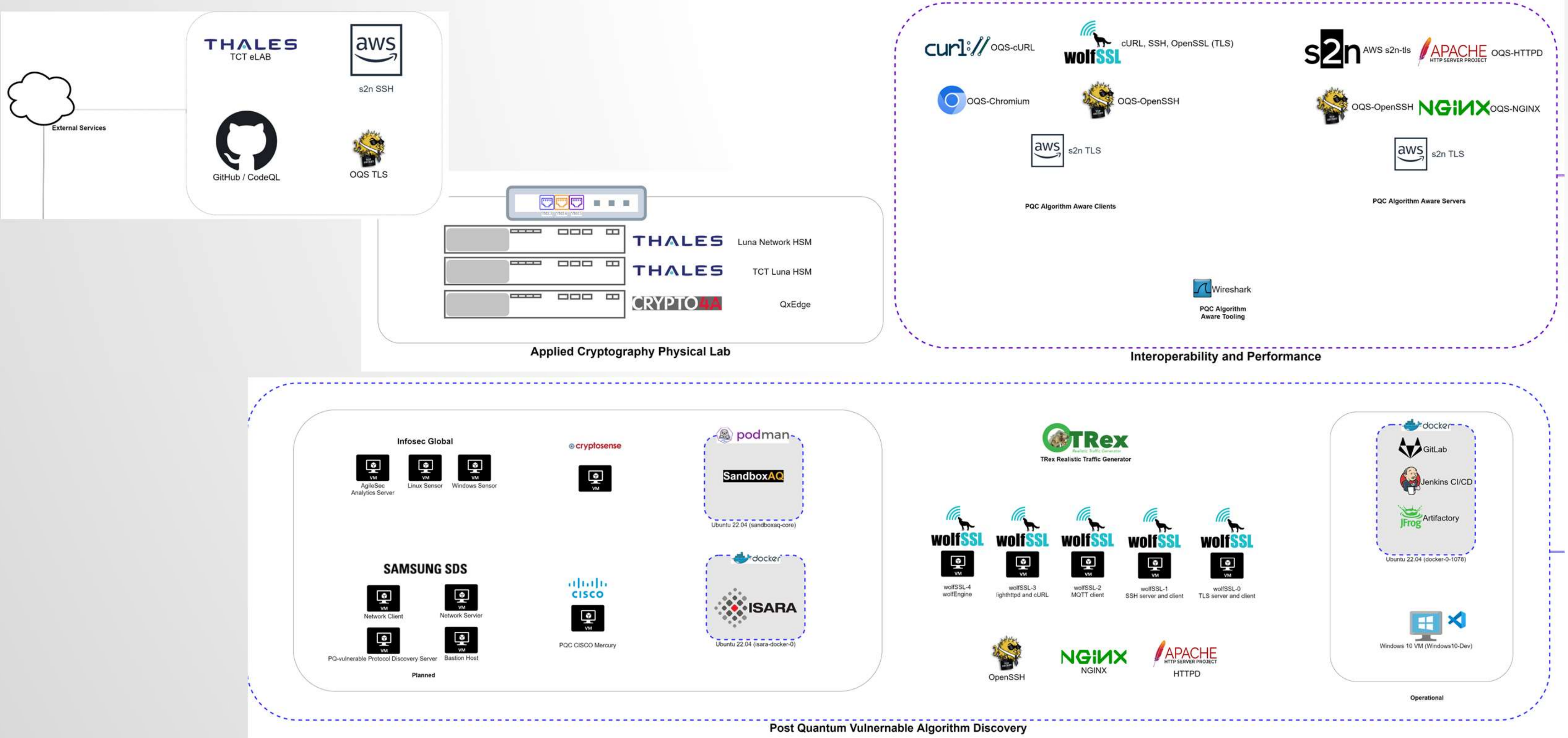

Code Development
Protocols and Network Services
Operational Systems and Applications
DISCOVERY
Analysis and Risk Assessment Engine
Prioritization List
Criticality of Data

- **Work in progress**
  - Define common data elements to describe quantum vulnerable cryptography such as
    - The Static Analysis Results Interchange Format (SARIF) is an industry standard format for the output of static analysis tools https://sarifweb.azurewebsites.net
    - Proposal of developing a cryptography bill of materials (CBOM) https://github.com/IBM/CBOM
  - Build the NCCoE lab environment with classical and quantum resistant systems and applications
  - Start deployment of the collaborators' contributed discovery tools and collect the assessment reports

INTEROPERABILITY AND PERFORMANCE WORKSTREAM

- **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
- **Work in progress**
  - Develop interop and performance demonstration plan for TLS, SSH, HSM, and X.509 certificate format (coordination with IETF hackathon PQC certificates)
  - Document issues and gaps to report back to the developers' standards and protocols to resolve the problems
  - Share our findings with the community
  - Leverage the NCCoE lab environment to initiate demonstrations starting with TLS protocol

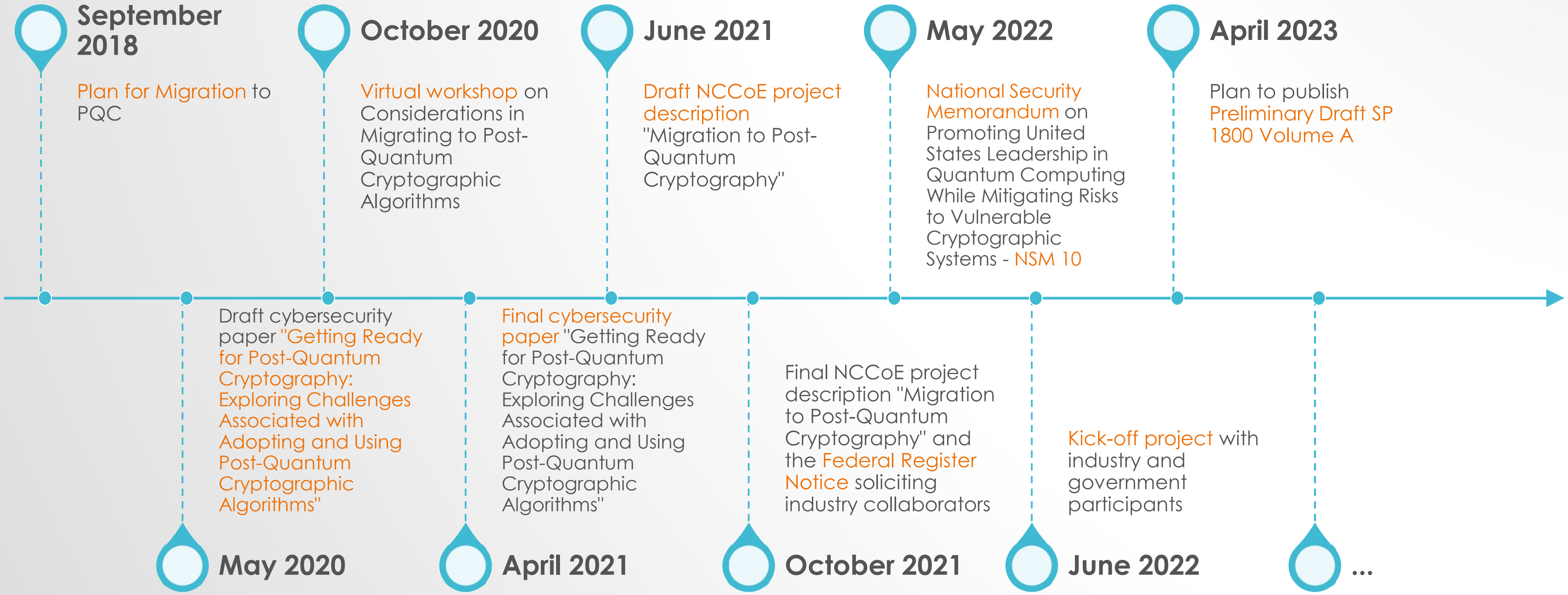
NCCoE DEMONSTRATION LAB (FEB 2023)



COLLABORATORS’ CONTRIBUTED COMPONENTS (FEB 2023)

COLLABORATORS	CONTRIBUTED COMPONENTS	DESCRIPTION
wolfSSL	wolfEngine	PQC-capable engine for openSSL project.
	wolfSSH	PQC-capable SSH library. Leveraging example client and server.
	wolfSSL	PQC-capable TLS library for cloud and embedded. Leveraging example client and server.
	MQTT implemention	PQC-capable MQTT protocol implementation.
	lighthttpd	PQC-capable web server.
	cURL	PQC-capable HTTP client.
Microsoft	Open Quantum Safe - Chromium	Patched PQC-enabled Chromium browser
	Open Quantum Safe - openSSL	PQC-enabled provider for openSSL.
	Open Quantum Safe - cURL	PQC-enabled HTTP client.
	Open Quantum Safe - httpd	PQC-enabled HTTP server.
	Open Quantum Safe - nginx	PQC-enabled HTTP server.
	Open Quantum Safe - OpenSSH	PQC-enabled SSH demonstration forked from openSSH project.
	Open Quantum Safe - liboqs	Core PQC library used in demonstration applications.
	CodeQL***	Automated vulnerable cloud-based code discovery service via GitHub.
Amazon	s2n-TLS	PQC-capable client and server implementations of the TLS protocol.
	s2n-SSH	PQC-capable client and server implementations of the SSH protocol. Not public
Infosec Global	Analytic Server	Core engine that discovers cryptographic assets, analyze threat levels and prioritize actions.
	Sensors	Host scanning agents for Linux and Windows systems.
Cryptosense (SanboxAQ)	Analyzer Platform	Automated host discovery and reporting platform.
SandboxAQ	AQ Analyzer	Automated network discovery and reporting platform.
Isara	Network Analyzer Platform	Automated network discovery and reporting platform.
Cisco	Mercury	Reads network packets, identifies metadata of interest, and writes out the metadata in JSON format.
Samsung SDS	BlueMax NG Firewall*	Automated network discovery and reporting platform.
IBM**	Integrated Cryptographic Service Facility	Dynamic usage tracking of ICSF crypto calls to chip based hardware, HSMs and software
	CP Assist for Cryptographic Functions Usage Tracking	Dynamic usage tracking of chip based hardware usage
	Application Discovery and Delivery Intelligence	Static analysis tool for COBOL applications using ICSF crypto or other IBM or non-IBM crypto providers
	z/OS Encryption Readiness Technology	Network crypto reporting and analysis including current and historical data
	Crypto Analytics Tool	Tooling which analyzes crypto settings like enabled functions, key repositories, certificates and other related metadata.
Crypto4A Technologies, Inc.	crypto4a QxEDGE	PQC-enabled network hardware security module.
Thales Trusted Cyber Technologies	Thales TCT	Network hardware security module with Quantum Number Generator.
Thales DIS CPL USA, Inc.	Thales CPT	Luna network hardware security module.
	Thales CPT e-lab	PQC-enabled network hardware security module. (cloud based)

PQC MIGRATION TIMELINE



September 2018

Plan for Migration to PQC

May 2020

Draft cybersecurity paper "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms"

October 2020

Virtual workshop on Considerations in Migrating to Post-Quantum Cryptographic Algorithms

April 2021

Final cybersecurity paper "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms"

June 2021

Draft NCCoE project description "Migration to Post-Quantum Cryptography"

October 2021

Final NCCoE project description "Migration to Post-Quantum Cryptography" and the Federal Register Notice soliciting industry collaborators

May 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems - NSM 10

June 2022

Kick-off project with industry and government participants

April 2023

Plan to publish Preliminary Draft SP 1800 Volume A

...

Migration to PQC Project Team

NIST

Project Leads & Points of Contact

- *Bill Newhouse*
- *Murugiah Souppaya*

Subject Matter Experts

- *Curt Barker*
- *Lily Chen*
- *David Cooper*
- *Dustin Moody*
- *Andy Regenscheid*

Lab Task Leads

- *Chris Brown*
- *Neil McNab*

Outreach & Engagement

- *Daniel Eliot*

Collaborating Organizations

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

REFERENCES

- **Project Website**
  - https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

- **Project Community of Interest (COI)**
  - Request to Join Email: applied-crypto-pqc@nist.gov

- **Contact the Project team**
  - applied-crypto-pqc@nist.gov