Post-Quantum

Cryptography Conference

NIST Post-Quantum Cryptography Update

In August 2024, the National Institute of Standards and Technology (NIST) reached a pivotal moment by releasing the first three finalized Post-Quantum Cryptography (PQC) standards: FIPS 203, FIPS 204, and FIPS 205. These standards mark the beginning of a new era in cryptography, designed to protect against the future threat of quantum computing. In this presentation, Mr. Andrew Regenscheid, Manager Cryptographic Technology Group at NIST, will provide an in-depth update on the newly established FIPS PQC standards. He will also discuss the ongoing efforts to standardize additional cryptographic algorithms, ensuring preparedness for potential vulnerabilities in the current standards. Mr. Bill Newhouse, a cybersecurity engineer and Project Lead at the NIST National Cybersecurity Center of Excellence (NCCoE), will explain the urgency of transitioning to these new quantum-resistant cryptographic standards. He will also share practical strategies and best practices to facilitate the migration from existing public-key cryptographic systems to these next-generation standards.

Bill Newhouse
Cybersecurity Engineer & Project Lead, National Cybersecurity Center of Excellence (NCCoE) at NIST

Andrew Regenscheid
Manager Cryptographic Technology Group at NIST

January 15 and 16, 2025 - Austin, TX (US) | Online

Post-Quantum Cryptography

Andy Regenscheid, Manager
Cryptographic Technology Group, NIST

Tuesday, October 3rd, 2023

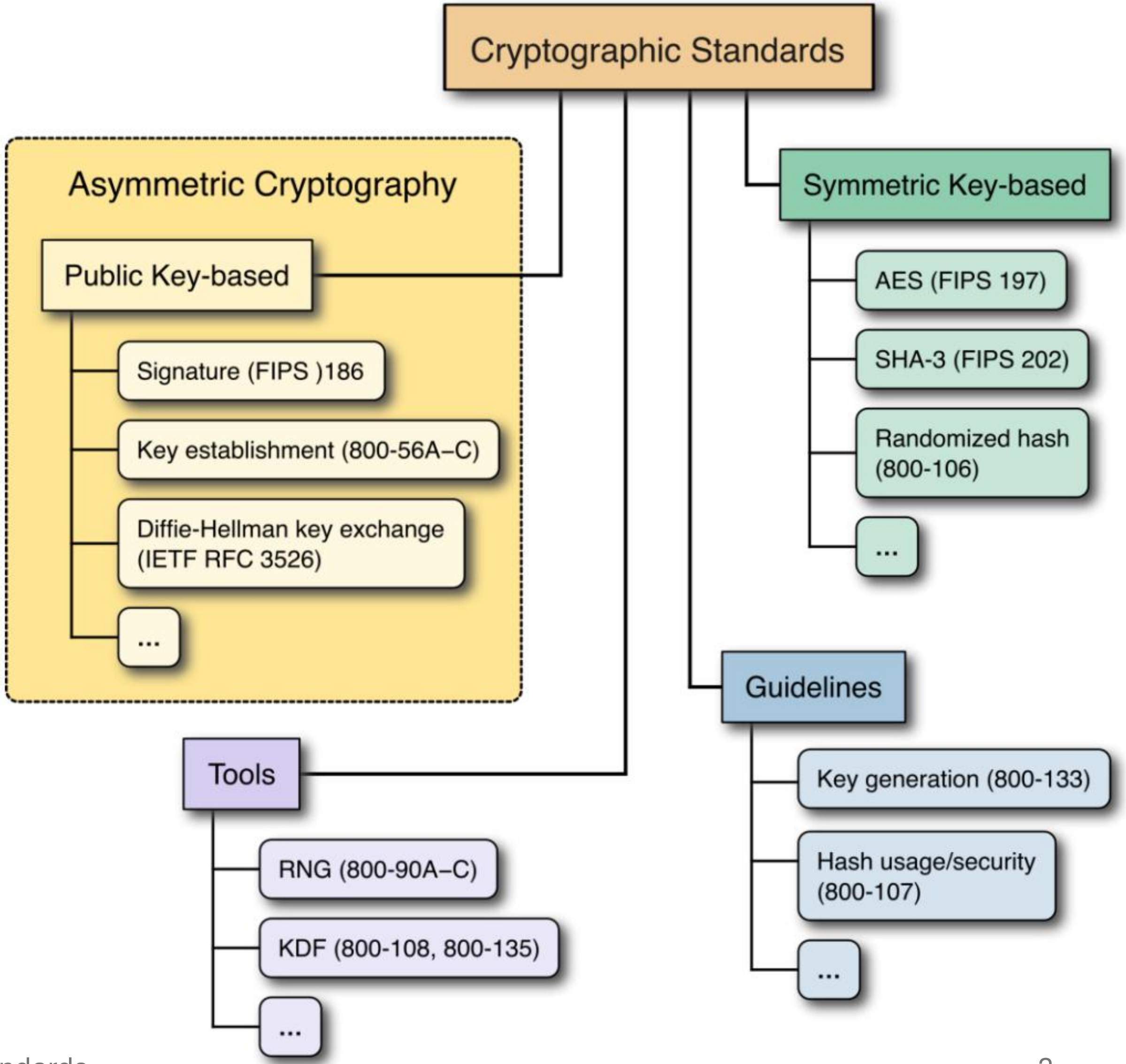
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Quantum Threat

- **Quantum computers threaten the security of current, widely-deployed public key cryptosystems**
    - *Signatures*– ECDSA, RSA
    - *Key Establishment*–Diffie-Hellman, RSA

- Quantum computers changed what we have believed about the hardness of mathematical problems that underpin cryptography
    - By Shor's algorithm, factorization and discrete logarithm problems can be solved by quantum computers in polynomial time

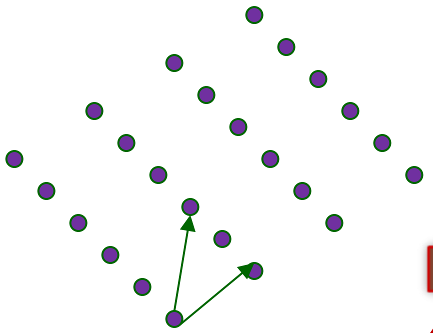
- Quantum computing also impacts security strength of symmetric key based cryptography algorithms – manageable by increasing key size
    - Grover's algorithm provides quadratic speedup

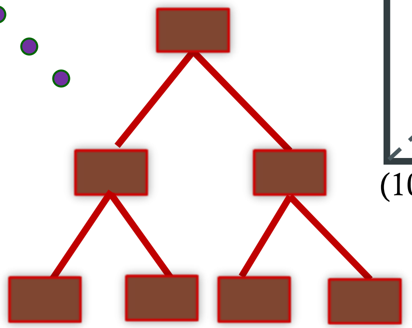


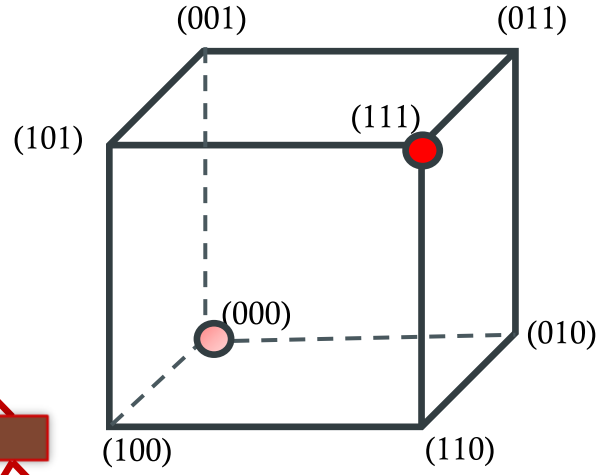
Post Quantum Cryptography (PQC)

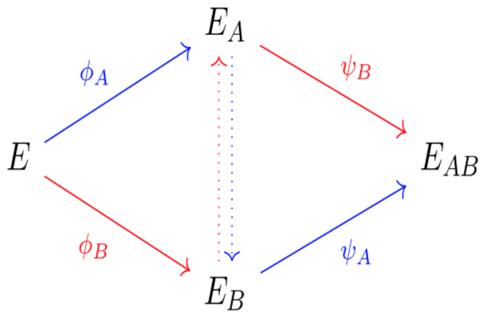
- PQC has been a very active research area in the past two decades

- Some actively researched PQC categories include
  - Lattice-based
  - Code-based
  - Multivariate
  - Hash/Symmetric key-based signatures
  - Elliptic curve isogeny-based









$$p^{(1)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$
$$p^{(2)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)}$$
$$\vdots$$
$$p^{(m)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}$$

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

PQC Process

NIST PQC Standards – Milestones and Timeline

2010-2015– NIST PQC project team builds & First PQC Conference

2016– Determined criteria and requirements, Call for proposals

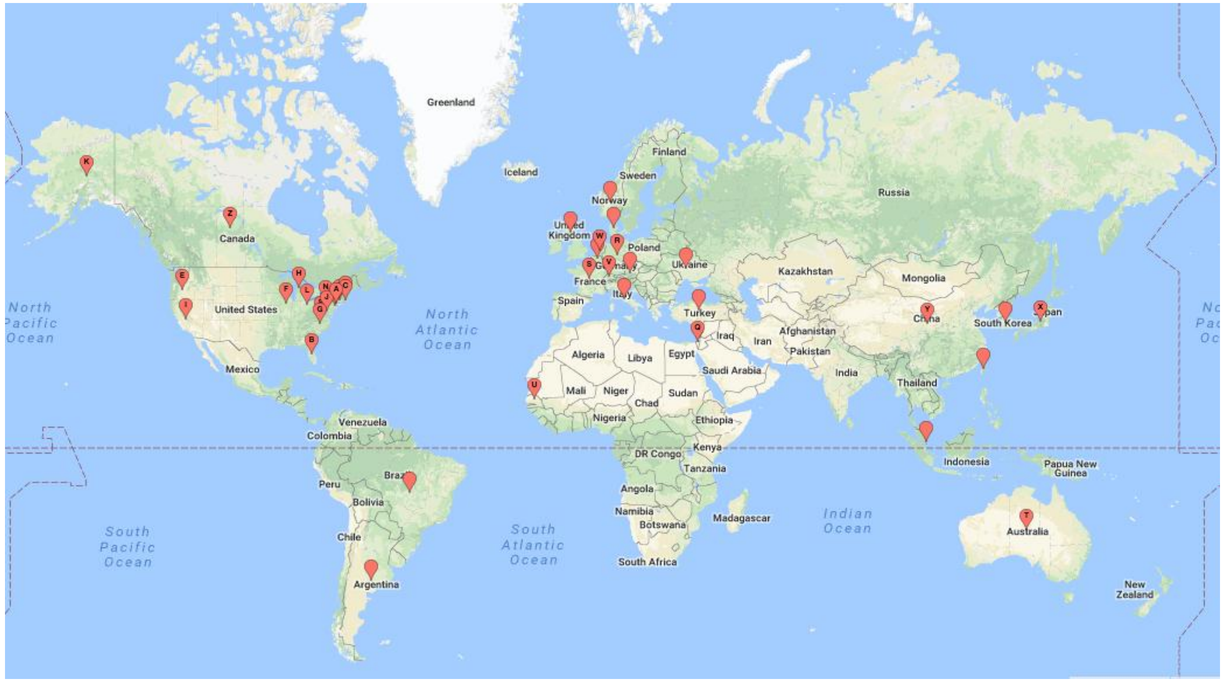
2017– Received 82 submissions, ***69 First Round candidates***

2018– 1st NIST PQC Standardization Conference

2019 – Announced ***26 Second Round candidates***
Released NISTIR 8240
Held the 2nd NIST PQC Standardization Conference

2020– Announced ***7 finalists & 8 alternate candidates***
Released NISTIR 8309

2021– Hold 3rd NIST PQC Standardization Conference



2022– ***Announced Initial Selections for Standardization & 4th Round Candidates***
Held 4th NIST PQC Standardization Conference

2023 Release draft standards and call for public comments

2024- Release Initial Final Standards

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Standards

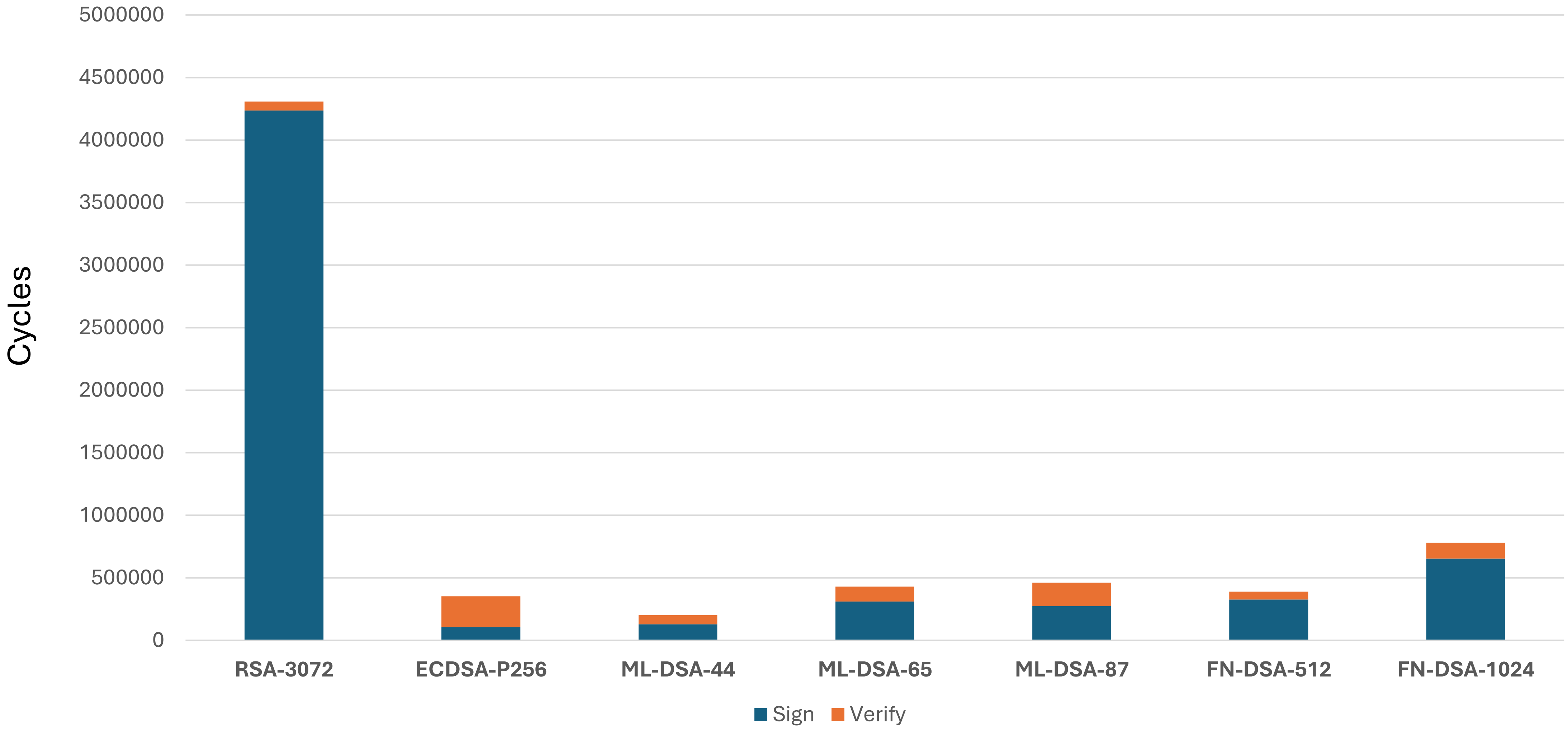
The first Set of NIST PQC Standards

NIST

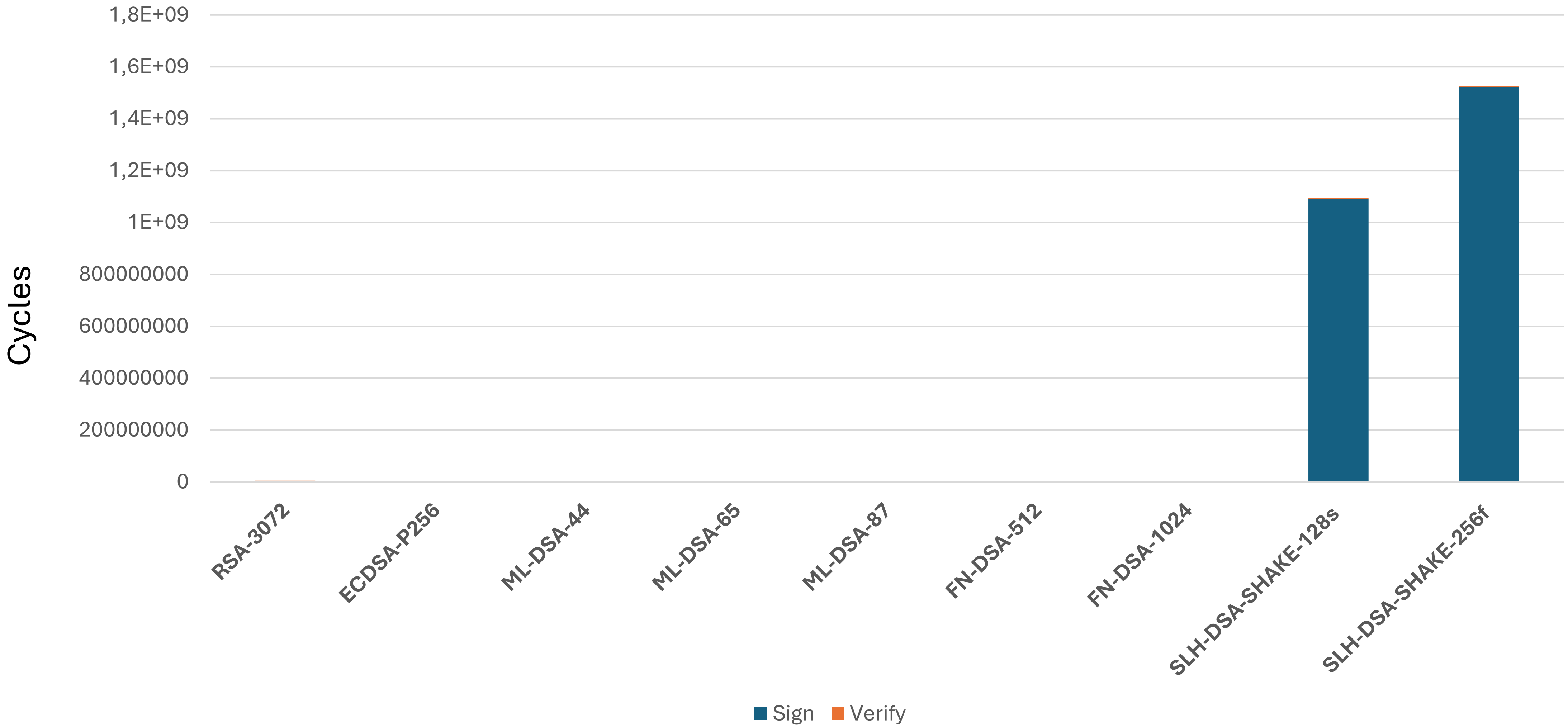
FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard (Based on CRYSTALS-Kyber)	FIPS 204 Module-Lattice-Based Digital Signature Standard (Based on CRYSTALS-Dilithium)	FIPS 205 Stateless Hash-Based Digital Signature Standard (Based on SPHINCS+)	FIPS 206 FFT-Over-NTRU-Lattice-Based Digital Signature Standard (Based on FALCON, ***under development***)
• A module learning with errors (MLWE)-based key encapsulation mechanism (KEM) • Good performance in different platforms • An algorithm for key establishment in security protocols	• A lattice-based digital signature algorithm based on the Fiat-Shamir paradigm • Good performance, simple implementation, moderate public-key and signature size, suitable for general applications	• Not require to keep track of any state between signatures • Solid security, signatures are longer compared with ML-DSA	• Hash and sign paradigm • Smaller bandwidth and fast verification but more complicated implementation

Published August 2024!

PQC Signatures– Performance



PQC Signatures– Performance- SLH-DSA



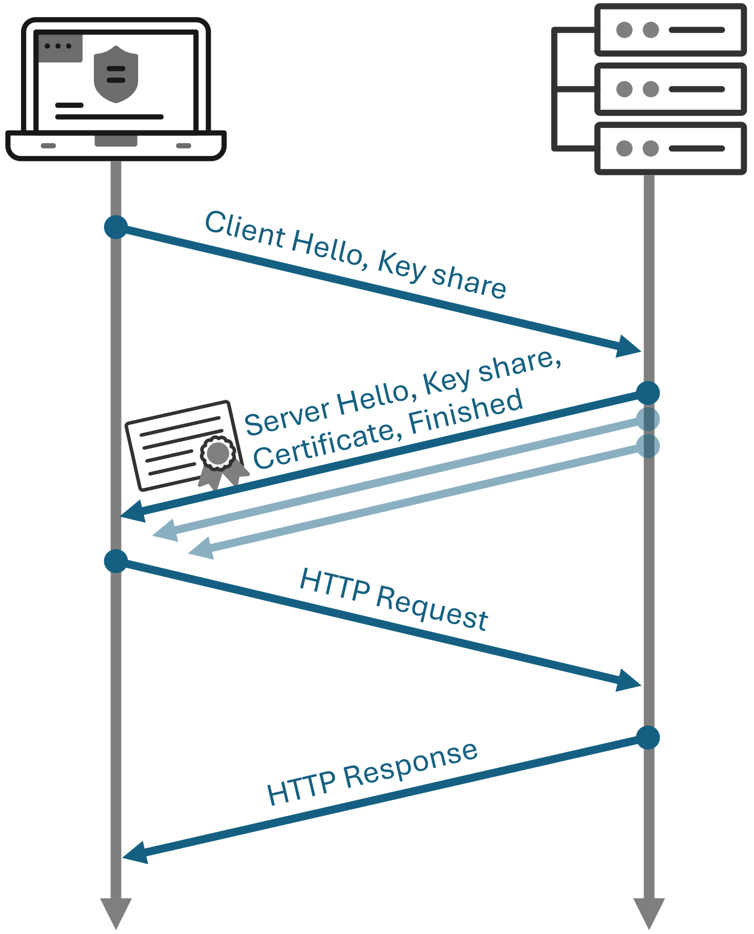
PQC Key and Signature Sizes

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)*

A bit much to chew?

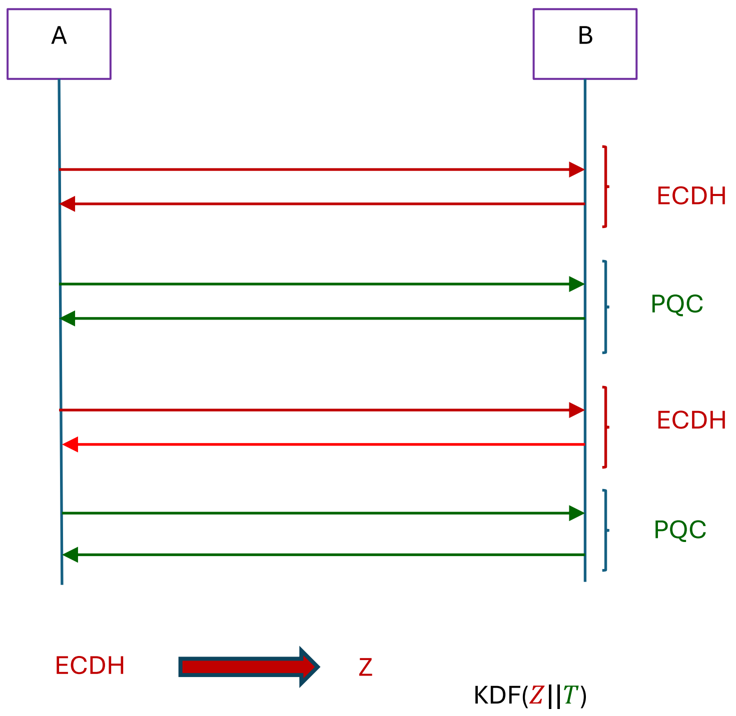
- TLS & WebPKI Certificate Signatures
  - *Server Certificate*: 1 public key and signature, 2 SCT signatures
  - *Intermediate CA Certificate*: 1 public key and signature
  - *TLS Handshake*: 1 signature
  - ML-DSA-44 → **14,724 bytes**
  - Current Quantum-Vulnerable → **1,248 bytes**
- ML-KEM-768 key shares
  - Client → Server: 1,184 bytes
  - Server → Client: **1,088 bytes**
- Why does this matter?
  - *TCP initial congestion window* limits the first wave of messages
  - Typical default: **~14,600 bytes**
- Without protocol/implementation changes, this could slow web connection establishment

TLS 1.3 Handshake



Hybrid Schemes

- **Hybrid**: using classical and PQC algorithms together
  - A hybrid mode combines a classical algorithm with a PQC algorithm
  - Reduces risks from uncertainty if either is broken
  - More complexity / slower performance
  - Can get FIPS 140 validation
  - More guidance to come in SP 800-227
- Several approaches to hybrid KEMs and certificates
  - Composite approaches
  - Non-composite hybrid approaches
- Use of hybrid will depend on community and application-specific needs
  - NIST does not intend to recommend for/against hybrid schemes
  - Implementers should consider complexity and migration issues
- Architectures /applications may support multiple algorithms



Migration

USG Migration

MAY 04, 2022

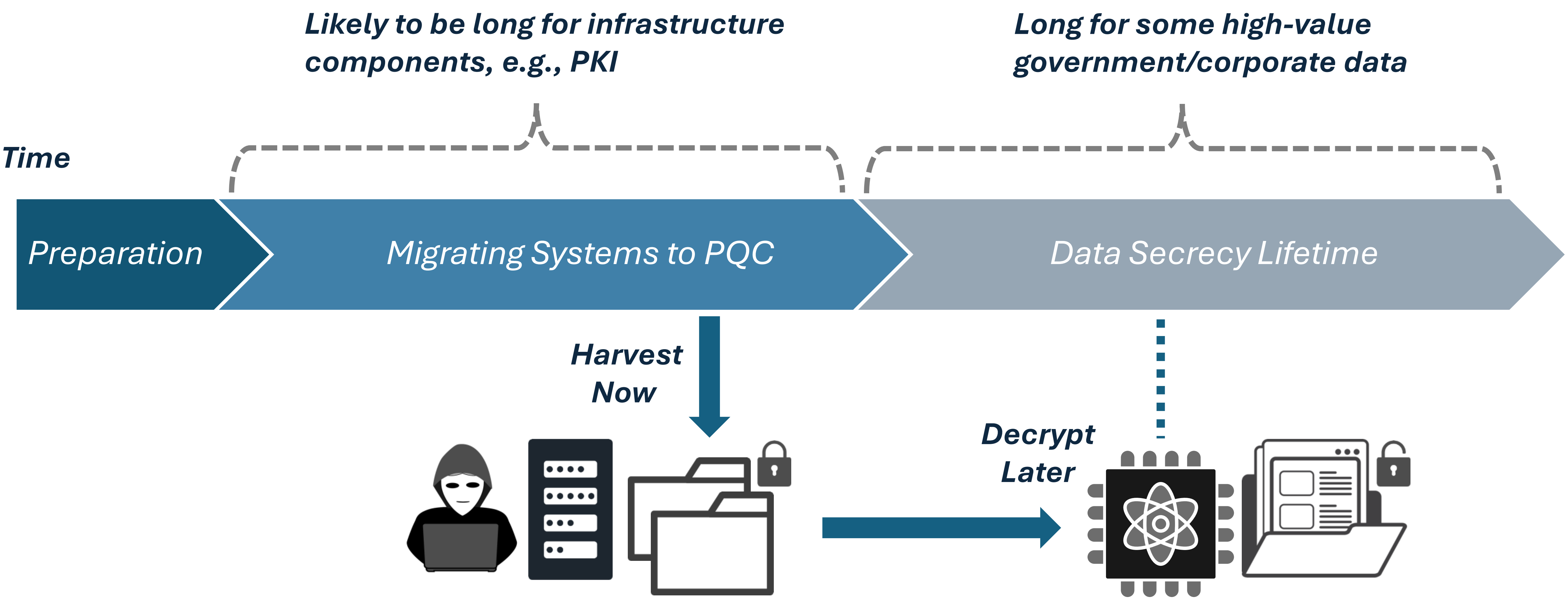
National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

BRIEFING ROOM ▸ STATEMENTS AND RELEASES

Excerpt from NSM-10:

"Mitigating the Risks to Encryption. ... To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, ***with the goal of mitigating as much of the quantum risk as is feasible by 2035."***

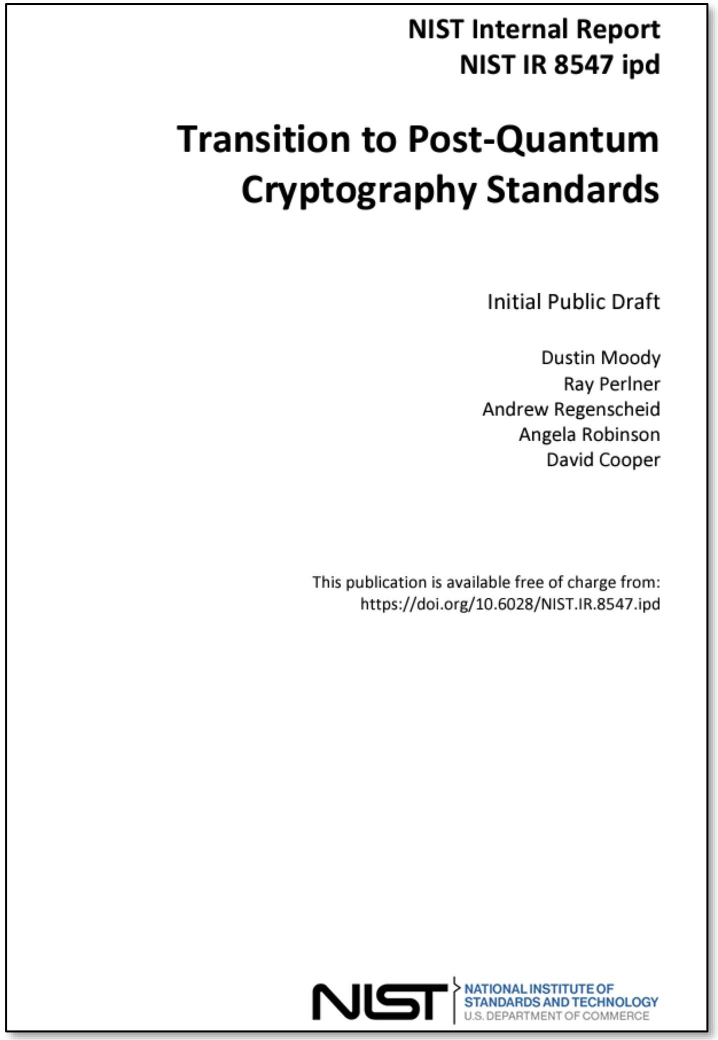
Migration Considerations



NIST IR 8547, Transition to PQC Standards

- Initial Public Draft released November 12th
  - Comment period ended ***January 10th***
- Identifies quantum-vulnerable standards
  - Key establishment based on Diffie-Hellman and MQV over finite field and elliptic curves (SP 800-56A)
  - Key establishment based on RSA (SP 800-56B)
  - Digital signatures include RSA, ECDSA, EdDSA (FIPS 186-4)
- Proposed transition timelines for quantum-vulnerable algorithms
  - 112-bit security strength – deprecated after 2030, disallowed after 2035
  - 128-bit and higher security strength – disallowed after 2035
- NIST-approved symmetric primitives providing at least 128 bits of classical security continue to be approved

Submit comments to: pqc-transition@nist.gov


NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8547.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Updates on the NIST NCCoE Migration to Post-Quantum Cryptography Project

Bill Newhouse –NCCoE Cybersecurity Engineer
william.newhouse@nist.gov

January 15, 2025

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Milestones and Timeline

NIST

NIST POST-QUANTUM CRYPTOGRAPHIC Standardization

2016 Criteria and requirements and call for proposals

2017 Received 82 submissions and announced 69 1st round candidates

2018 The 1st NIST PQC standardization Conference

2019 Announced 26 2nd round candidates. The 2nd NIST PQC Standardization Conference

2020 Announced 3rd round 7 finalists and 8 alternate candidate

2021 The 3rd NIST PQC Standardization Conference

2022 Announced the 3rd round selection and the 4th round candidates, the 4th NIST PQC conference

2023 Released draft standards for public comments

2024 5th NIST PQC standardization conference

2024 Published the 1st three PQC standards (Aug 2024)

2022 Called for additional signatures

2023 Received 50 signature submissions and 40 of them were selected as the first-round candidates

2024 14 Candidates to Advance to the Second Round of the Additional Digital Signatures for the PQC Standardization Process

2021 NCCoE begins Migration to Post-Quantum Cryptography Project calling for collaborators (Oct)

2022 Kickoff with 14 CRADA Collaborators (July)

2023 Published initial public drafts for discovery and interoperability/performance workstreams (Dec)

2024 Demonstrating how to use inventory for prioritization decisions, expanding interoperability and performance testing into additional communication protocols (over 40 collaborators)

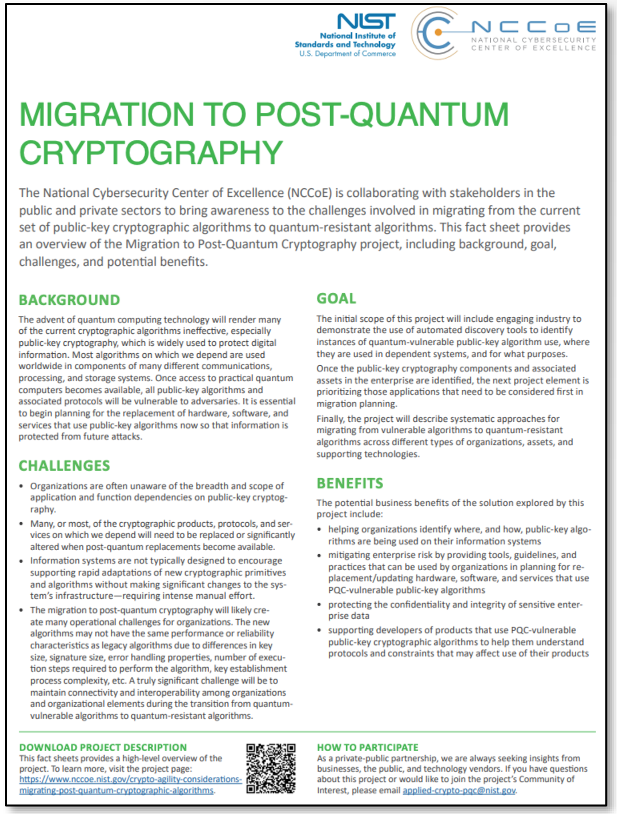
NCCoE Migration to Post Quantum Cryptography Project

Practices to ease migration from the current set of public-key cryptographic algorithms to NIST standardized PQC algorithms

The NCCoE – MIGRATION TO PQC - AN APPLIED RESEARCH PROJECT

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- Complement NIST PQC standardization effort
- Support/Inform US Government PQC initiatives (White House NSM-10, M-23-02)
- Tackle challenges with adoption, implementation, and deployment of PQC
- Engage with the community including industry collaborators and across government to bring awareness and education 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 migration to PQC algorithms
- 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.

Migration to PQC Project Collaborators

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- Amazon Web Services, Inc.
- ATIS
- Cisco Systems, Inc.
- Comcast
- Crypto4A Technologies, Inc.
- CryptoNext Security
- Federal: Cybersecurity and Infrastructure Security Agency (CISA)
- Data-Warehouse GbmH
- Dell Technologies
- DigiCert
- Entrust
- GDIT
- Gutsy
- HP, Inc.
- HSBC
- IDEMIA Secure Transactions
- IBM
- Information Security Corporation
- InfoSec Global
- ISARA Corporation
- JPMorgan Chase Bank, N.A.
- Keyfactor
- Kudelski IoT
- Microsoft
- M&T Bank
- Federal: National Security Agency (NSA)
- NXP Semiconductors
- Palo Alto Networks
- Post-Quantum
- PQShield
- QuantumXChange
- SafeLogic, Inc.
- Samsung SDS Co., Ltd.
- SandboxAQ
- Santander
- Siemens
- SSH Communications Security Corp
- Thales DIS CPL USA, Inc.
- Thales Trusted Cyber Technologies
- Utimaco
- Verizon
- wolfSSL

DRAFT NIST SPECIAL PUBLICATION 1800-38

Moving volumes into one NIST Special Publication 1800-38 to be hosted on pages.nist.gov

- Example: NIST SP 1800-35 https://pages.nist.gov/zero-trust-architecture/)

Initial Public Draft NIST SP 1800-38B (Dec 2023)

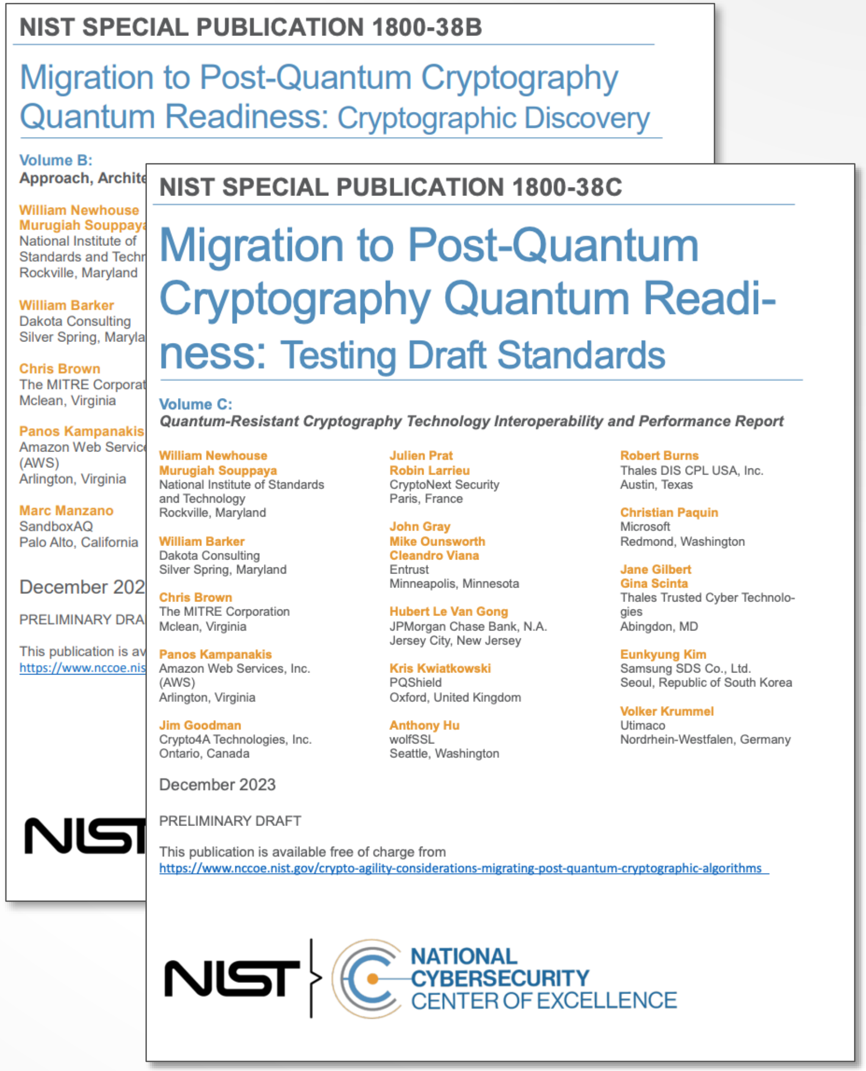
Quantum Readiness: Cryptographic Discovery

- Demonstration of collaborator cryptographic discovery and inventory tools

Initial Public Draft NIST SP 1800-38C (Dec 2023)

Quantum Readiness: Testing Draft and Final Standards for Interoperability and Performance

- Explore interoperability issues in a controlled, non-production environment
- Reduction of time spent by individual organizations performing similar interoperability testing for their own PQC migration efforts


NIST SPECIAL PUBLICATION 1800-38B

Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery

Volume B:
Approach, Archite

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

William Barker
Dakota Consulting
Silver Spring, Maryla

Chris Brown
The MITRE Corporat
Mclean, Virginia

Panos Kampanakis
Amazon Web Servic
(AWS)
Arlington, Virginia

Marc Manzano
SandboxAQ
Palo Alto, California

December 202

PRELIMINARY DRA

This publication is av
https://www.nccoe.nis

NIST SPECIAL PUBLICATION 1800-38C

Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standards

Volume C:
Quantum-Resistant Cryptography Technology Interoperability and Performance Report

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

Panos Kampanakis
Amazon Web Services, Inc. (AWS)
Arlington, Virginia

Jim Goodman
Crypto4A Technologies, Inc.
Ontario, Canada

Julien Prat
Robin Larrieu
CryptoNext Security
Paris, France

John Gray
Mike Ounsworth
Cleandro Viana
Entrust
Minneapolis, Minnesota

Hubert Le Van Gong
JPMorgan Chase Bank, N.A.
Jersey City, New Jersey

Kris Kwiatkowski
PQShield
Oxford, United Kingdom

Anthony Hu
wolfSSL
Seattle, Washington

Robert Burns
Thales DIS CPL USA, Inc.
Austin, Texas

Christian Paquin
Microsoft
Redmond, Washington

Jane Gilbert
Gina Scinta
Thales Trusted Cyber Technologies
Abingdon, MD

Eunkyung Kim
Samsung SDS Co., Ltd.
Seoul, Republic of South Korea

Volker Krummel
Utimaco
Nordrhein-Westfalen, Germany

December 2023

PRELIMINARY DRAFT

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

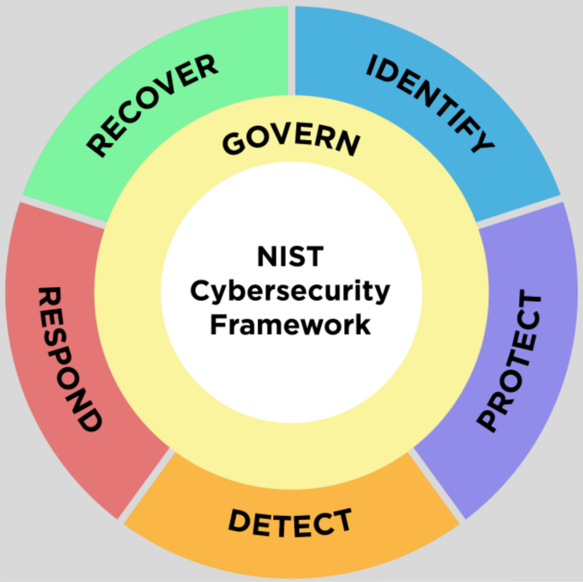
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

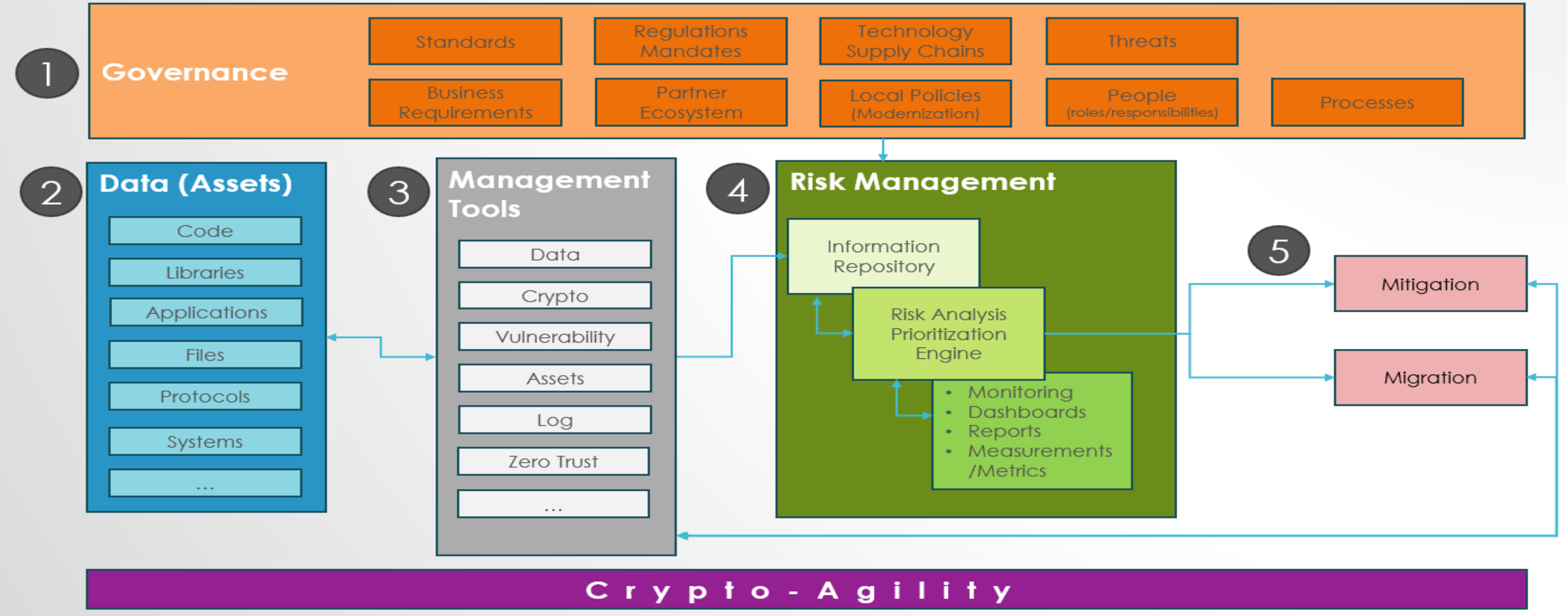
WORKSTREAMS

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- Update earlier tests with standardized PQC algorithms parameters (X.509, HSMs, TLS, SSH)
- VPN (PQC -only and hybrid modes of the IKEv2 Key Exchange
- IPsec
- DNSSEC
- Smart Card/PIV…

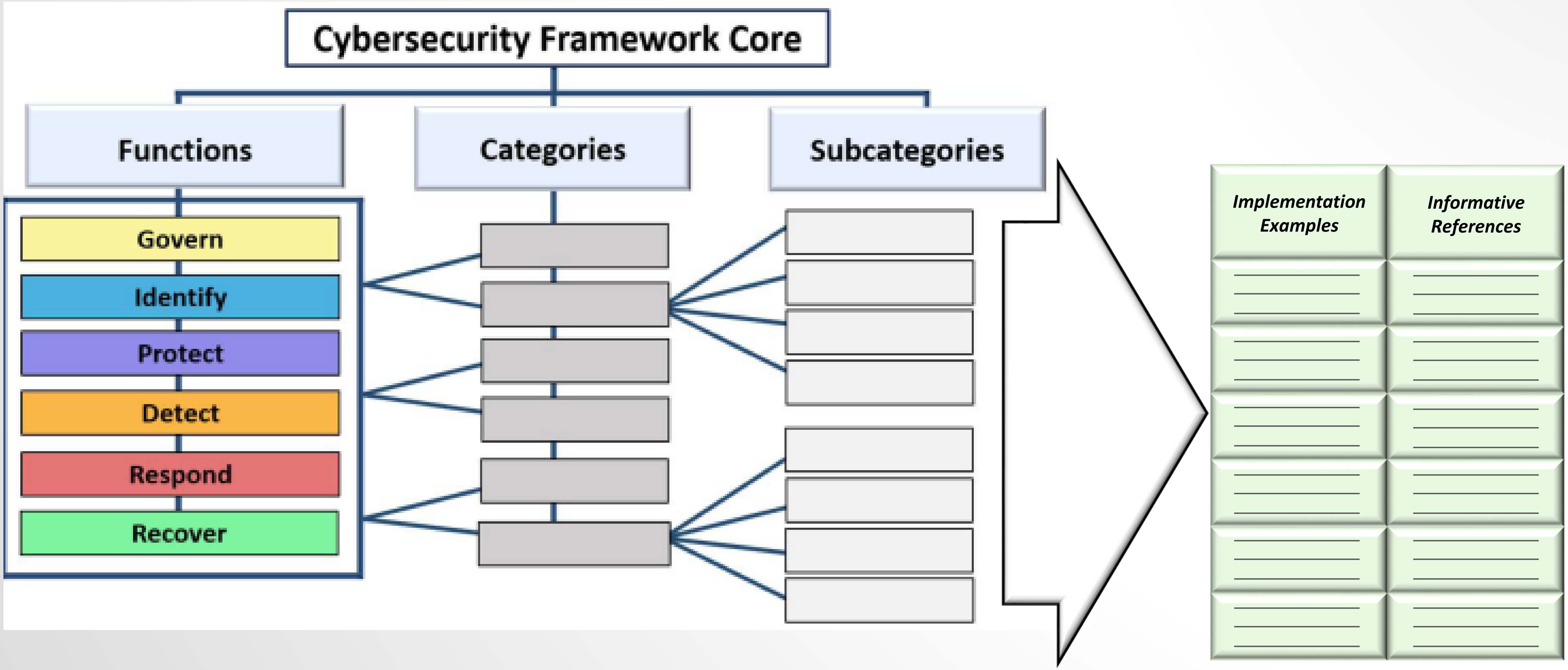
Data centric risk management to prioritize mitigation and migration with crypto agility





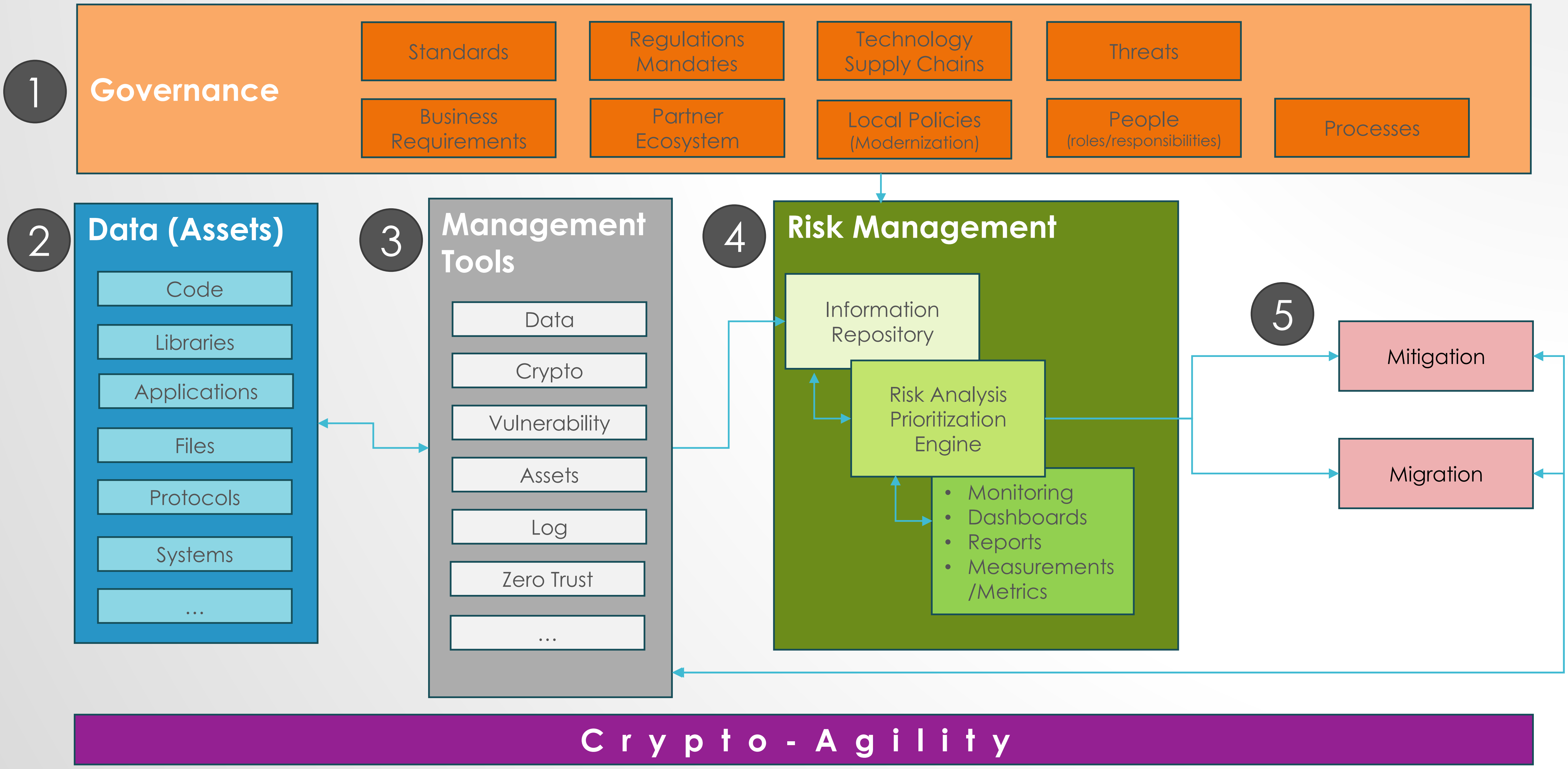
A RISK MANAGEMENT FRAMEWORK
CYBERSECURITY FRAMEWORK (CSF) 2.0

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



DATA CENTRIC CRYPTO RISK MANAGEMENT APPROACH

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

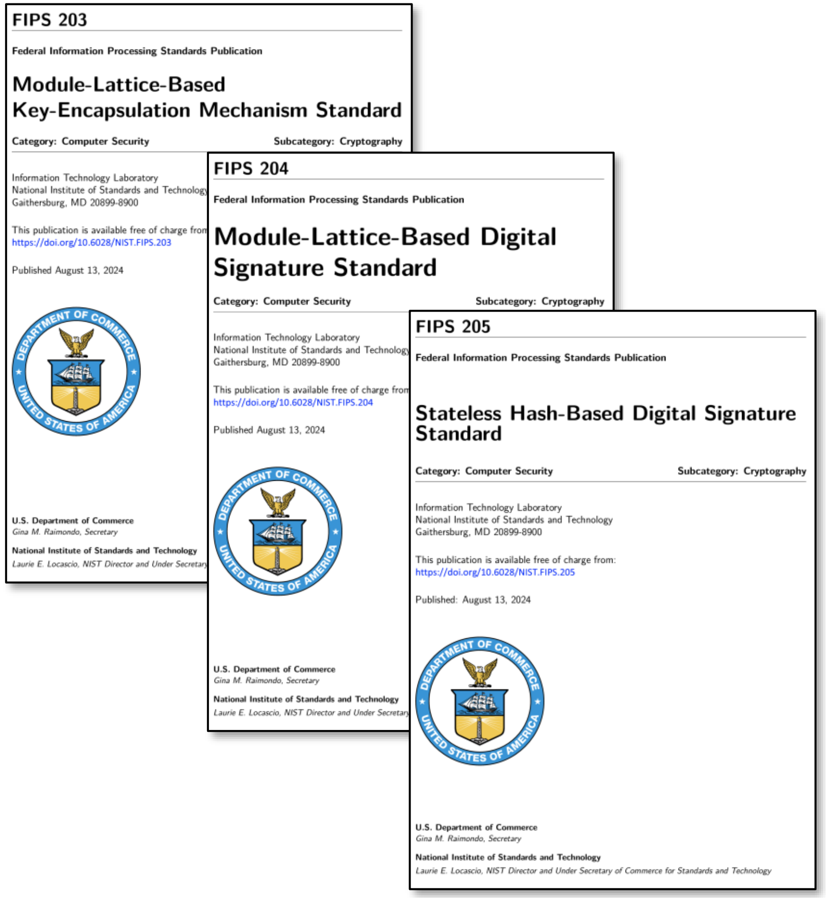


NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Next Steps

PQC Standards- Next Steps

- ***ML-KEM***, ***ML-DSA***, & ***SLH-DSA*** finalized on August 13
- Draft ***FN-DSA*** (Falcon) standard under development
- NIST plans to make 4th round KEM selection in 2024
  - Classic McEliece
  - BIKE
  - HQC
  - ~~SIKE~~
- NIST called for additional signatures in 2022 to evaluate general-purpose signatures based on diversified math problems
  - 14 algorithms were selected for a second round


FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from
https://doi.org/10.6028/NIST.FIPS.203

Published August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary

FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from
https://doi.org/10.6028/NIST.FIPS.204

Published August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary

FIPS 205

Federal Information Processing Standards Publication

Stateless Hash-Based Digital Signature Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.205

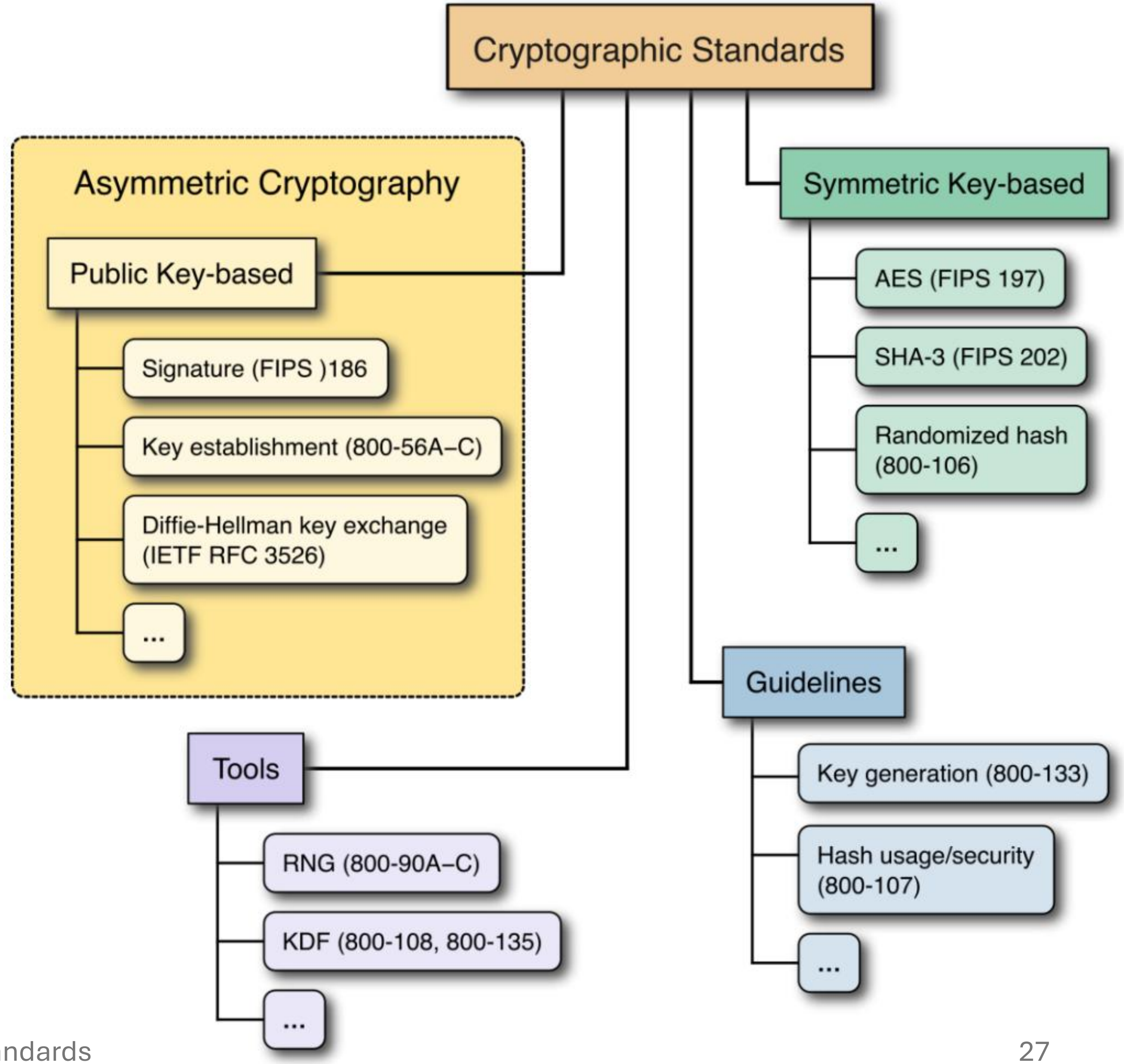
Published: August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Recommendations & FIPS 140 Testing

- NIST is actively working on Special Publications to provide recommendations for the usage of PQC standards in applications, e.g.,
  - SP 800-227 *Recommendations for key-encapsulation mechanisms* to use KEM in key establishment protocols
- NIST provided guidance for transition in the past (SP 800-131A) and will provide PQC transition guidance
- NIST CAVP is already testing new PQC algorithms for FIPS 140 validation



PQC– Much Work Remains

NIST

- Operations
- Infrastructure Modernization
- PQC Adoption in Software/Systems
- Hardware Acceleration/Support
- Implementation in Cryptographic Libraries
- Protocol/Application Standards
- $\mathbb{Z}_q[X]$ Algorithm Standards

Considerations for Achieving Crypto Agility

Initial Public Draft NIST Cybersecurity Whitepaper (CWSP 39) Considerations for Achieving Crypto Agility

Crypto agility refers to the capabilities needed to replace and adapt cryptographic schemes in protocols, applications, software, hardware, and infrastructures.

This white paper provides an in-depth survey of current approaches to achieving crypto agility. It discusses challenges and tradeoffs and identifies some approaches for providing operational mechanisms to achieve crypto agility while maintaining interoperability.

- Transition Challenges
- Crypto Agility for Security Protocols
- Crypto Agility in Systems for Applications
- Governance
- Discussions:
  - Resource Considerations
  - Agility Awareness Designs
  - Crypto Agility in the Cloud
  - Maturity Assessment for Crypto Agility
  - Strategic Planning
  - Security Policy Enforcement
  - Complexity and Security
  - Environment Specific Agility Requirements

Questions

Contact Information

Andrew Regenscheid, Cryptographic Technology Group

Email: Andrew.Regenscheid@nist.gov

Bill Newhouse, National Cybersecurity Center of Excellence

Email: William.Newhouse@nist.gov

NIST PQC standardization

www.nist.gov/pqcrypto
Sign up for ***pqc-forum*** mailing list
Email: pqc-comments@nist.gov

NCCoE PQC Migration Project

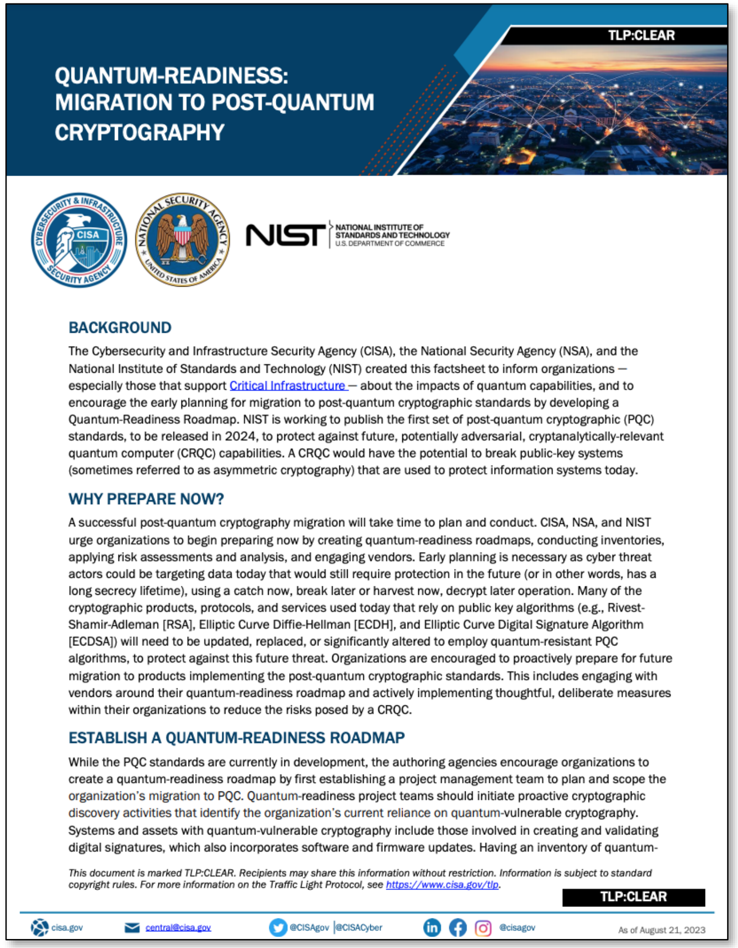
www.nccoe.nist.gov/applied-cryptography
Request to join Community of Interest
Email: applied-crypto-pqc@nist.gov

ML-KEM Sizes

Scheme	Public Key (bytes)	Private Key (bytes)	Ciphertext (bytes)	Security Level
RSA-3072	**384**	**384**	**384**	**Classical-128**
ECDH-P256	**64**	**32**	**---**	**Classical-128**
ML-KEM-512 (Kyber512)	**800**	**1632**	**768**	**PQC Category 1** *(AES-128)*
ML-KEM-768 (Kyber768)	**1184**	**2400**	**1088**	**PQC Category 3** *(AES-192)*
ML-KEM-1024 (Kyber1024)	**1568**	**3168**	**1568**	**PQC Category 5** *(AES-256)*

Migration– How Organizations Can Prepare

- **Establish a Quantum-Readiness Roadmap**
  - Project management team to plan and scope the migration to PQC
- **Prepare an Inventory of Cryptography and Assets**
  - Identity protocols/applications/devices that use vulnerable cryptography
  - Identify high-value data requiring long-term secrecy
- **Discuss PQC Roadmaps with Vendors**
- **Develop a Migration Strategy**
  - Prioritize high-impact systems, ICSs, and those requiring long-term secrecy
  - Integrate with technology modernization/refresh efforts
  - Prepare to rearchitect, rebuild, or replace legacy applications/systems
- **Validate and Test Systems**
- **Educate and Train Staff**



TLP:CLEAR

QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

BACKGROUND

The Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST) created this factsheet to inform organizations — especially those that support Critical Infrastructure — about the impacts of quantum capabilities, and to encourage the early planning for migration to post-quantum cryptographic standards by developing a Quantum-Readiness Roadmap. NIST is working to publish the first set of post-quantum cryptographic (PQC) standards, to be released in 2024, to protect against future, potentially adversarial, cryptanalytically-relevant quantum computer (CRQC) capabilities. A CRQC would have the potential to break public-key systems (sometimes referred to as asymmetric cryptography) that are used to protect information systems today.

WHY PREPARE NOW?

A successful post-quantum cryptography migration will take time to plan and conduct. CISA, NSA, and NIST urge organizations to begin preparing now by creating quantum-readiness roadmaps, conducting inventories, applying risk assessments and analysis, and engaging vendors. Early planning is necessary as cyber threat actors could be targeting data today that would still require protection in the future (or in other words, has a long secrecy lifetime), using a catch now, break later or harvest now, decrypt later operation. Many of the cryptographic products, protocols, and services used today that rely on public key algorithms (e.g., Rivest-Shamir-Adleman [RSA], Elliptic Curve Diffie-Hellman [ECDH], and Elliptic Curve Digital Signature Algorithm [ECDSA]) will need to be updated, replaced, or significantly altered to employ quantum-resistant PQC algorithms, to protect against this future threat. Organizations are encouraged to proactively prepare for future migration to products implementing the post-quantum cryptographic standards. This includes engaging with vendors around their quantum-readiness roadmap and actively implementing thoughtful, deliberate measures within their organizations to reduce the risks posed by a CRQC.

ESTABLISH A QUANTUM-READINESS ROADMAP

While the PQC standards are currently in development, the authoring agencies encourage organizations to create a quantum-readiness roadmap by first establishing a project management team to plan and scope the organization's migration to PQC. Quantum-readiness project teams should initiate proactive cryptographic discovery activities that identify the organization's current reliance on quantum-vulnerable cryptography. Systems and assets with quantum-vulnerable cryptography include those involved in creating and validating digital signatures, which also incorporates software and firmware updates. Having an inventory of quantum-

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

TLP:CLEAR

cisa.gov central@cisa.gov @CISAgov |@CISACyber @cisagov As of August 21, 2023

4^{th} Round KEMs

- **Classic McEliece**
  - Code-based KEM that uses a binary Goppa code
  - Solid security with confidence in the security of the 1978 scheme
  - Small ciphertext but very large public key and relatively slow key generation

- **HQC (Hamming Quasi-Cyclic)**
  - KEM based on QC-MDPC code
  - Offers strong security assurances and mature decryption failure rate analysis
  - Larger public keys and ciphertext sizes than BIKE

- **BIKE (Bit Flipping Key Encapsulation)**
  - KEM based on binary linear quasi-cyclic moderate density parity check (QC-MDPC) codes
  - Public-key and ciphertext comparable to lattice-based schemes
  - The most competitive performance among the non-lattice-based KEMs
  - Announced a new decoder in the 5^{th} NIST Conference
    - Reduce impact of new weak key classes in Crypto 2023 paper

- All the 4^{th} round candidates are code-based key encapsulation mechanisms (KEM)
- NIST plans to make selections soon

On-Ramp Signatures

- Why NIST called for additional post-quantum signatures?
  - NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices.
  - NIST may also be interested in signature schemes that have short signatures and fast verification.
  - Any lattice signature would need to significantly outperform CRYSTALS-Dilithium and FALCON and/or ensure substantial additional security properties.
- Received 50 submissions June 1, 2023 – 40 of them are accepted as the first-round candidates
- NIST announced 14 candidates to advance to the second round of the additional digital signatures for the PQC standardization process on October 24, 2024

Multivariate	MPC in-the-head				Lattice	Code	Symmetric	Isogeny
UOV	**MinRank**	**SD/Rank-SD**	**PKP**	**MQ**				
Mayo	**Mirath**	**Ryde**	**Perk**	**MQOM**	**Hawk**	**Cross**	**FAEST**	**SQIsign**
QR-UOV		**SDitH**				**LESS**		
SNOVA								
UOV								