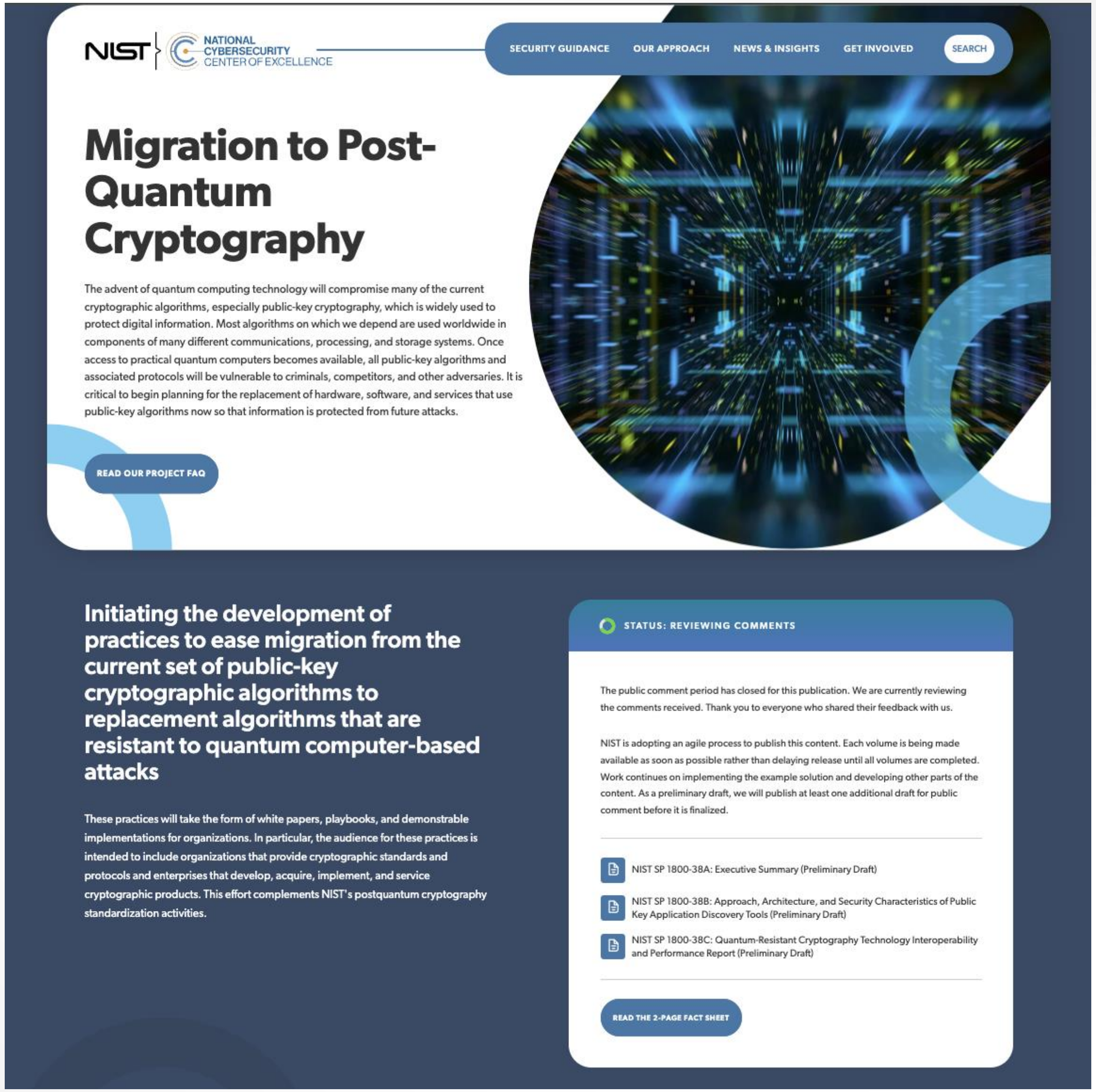
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE MIGRATION TO POST-QUANTUM CRYPTOGRAPHY PROJECT

Staying Ahead of the Curve: Planning for the Migration to Post-Quantum
June 18, 2024

Bill Newhouse, NIST National Cybersecurity Center of Excellence

WEBINAR AGENDA

- NCCoE Migration to Post-Quantum Cryptography (PQC) project
- Draft Special Publication 1800-38
  - Discovery of Quantum Vulnerable Cryptography Workstream
  - Interoperability and Performance PQC Implementations Workstream
- Current Status of FIPS 140 Validation Program
- Data Centric Risk Management to Prioritize Mitigation and Migration with Crypto Agility



ALGORITHMS FOR QUANTUM COMPUTATION: DISCRETE LOGARITHMS AND FACTORING, A 1994 PAPER

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Proceedings 35th Annual Symposium on Foundations of Computer Science

Algorithms for quantum computation: discrete logarithms and factoring

Year: 1994, Pages: 124-134 , DOI Bookmark: 10.1109/SFCS.1994.365700

Author: P.W. Shor, AT&T Bell Labs., Murray Hill, NJ, USA

Abstract (subdivided into bullets for emphasis):

- A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor: It is not clear whether this is still true when quantum mechanics is taken into consideration.

- Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties.

- This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems.

- We thus give the first examples of quantum cryptanalysis.

WHY MIGRATE TO POST-QUANTUM CRYPTOGRAPHY?

- **Threat:**
  - **Implementation of Shor's Algorithm on quantum computers** will defeat the current public-key algorithms that are currently employed in supporting confidence in the integrity of information and the security of **keys** that are essential to protecting its confidentiality (e.g., digital signatures and key establishment).
  - **Harvest Now, Decrypt Later -**Adversaries are already archiving key establishment and other quantum-vulnerable information for exploitation whenever implementation of Shor's Algorithm on quantum computers becomes practical.
- **Response:**
  - **Standardized post-quantum cryptography (also called quantum-resistant cryptography) is designed to be secure against attacks from both quantum and classical computers.**
  - **Standards that leverage digital signatures and key exchange and establishment will need to be updated to support post-quantum cryptography.**
- **Challenges:**
  - **In most cases, organizations have an incomplete picture of how dependent they are on public-key cryptography.**
  - **Urgency, cryptographic migrations take a long time.**

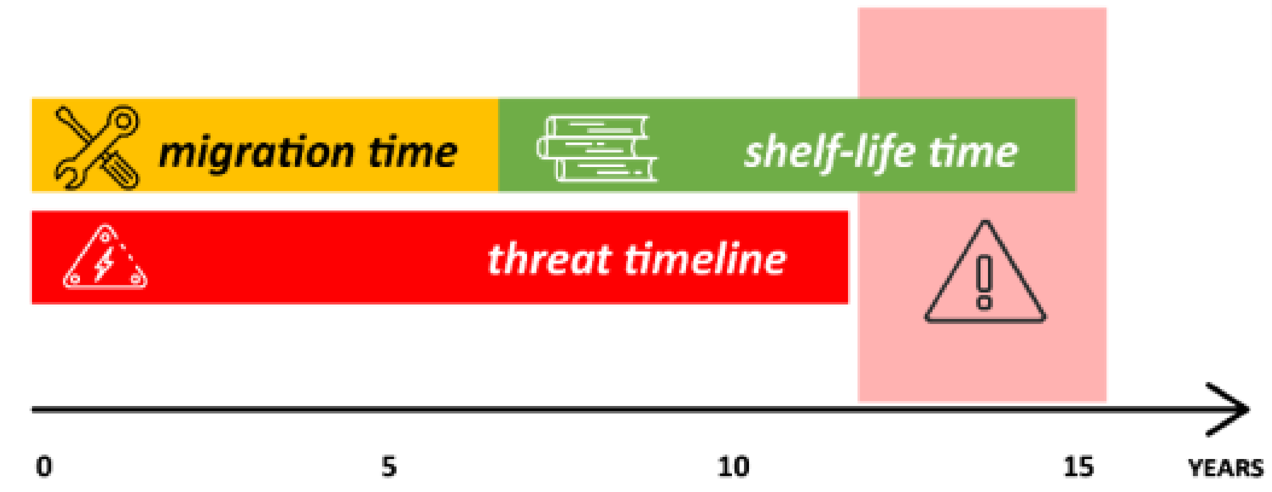
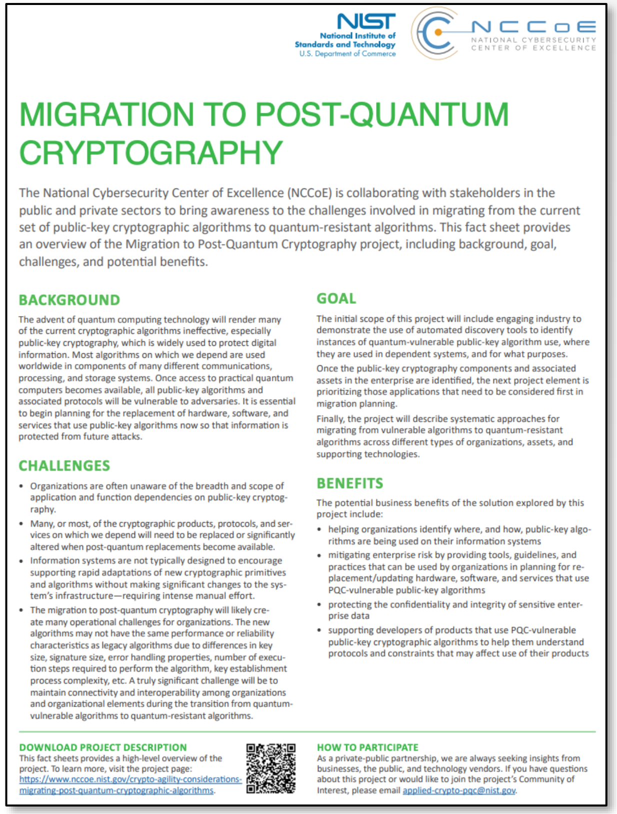


Image Source: https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/cfdir-quantum-readiness-best-practices-v03.pdf

NCCoE – MIGRATION TO PQC
AN APPLIED RESEARCH PROJECT

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

- 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 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 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.

Migration to PQC Project Collaborators

- Amazon Web Services, Inc. (AWS)
- Cisco Systems, Inc.
- Federal: Cybersecurity and Infrastructure Security Agency (CISA)
- Comcast
- 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
- Federal: National Security Agency (NSA)
- NXP Seminconductors
- Palo Alto Networks
- Post-Quantum
- 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
- wolfSSL

MIGRATION TO PQC PROJECT TIMELINE

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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
Published Preliminary Draft SP 1800-38 Volume A

December 2023
Published Preliminary Draft SP 1800-38 Volume B and C

March-June 2024
FIPS 140 Cryptographic Algorithm Validation Program Demo Server

ML-KEM
ML-DSA
SLH-DSA

2024
Continue interoperability and performance testing

Risk-Based Approach to Manage Quantum Threat to Crypto with a Focus on Crypto Agility

DRAFT NIST SPECIAL PUBLICATION 1800-38

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

December 2023

Published Preliminary Draft SP 1800-38 Volume B and C

Draft NIST SP 1800-38B

Quantum Readiness: Cryptographic Discovery

- Functional test plan that exercises the cryptographic discovery tools to determine baseline capabilities
- Describes a use case to provide context and scope
- Identifies threats addressed in this demonstration
- Provides a multifaceted approach to start the discovery process
- Describes the high-level architecture that integrates contributed discovery tools in our lab

Draft NIST SP 1800-38C

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

- Identification of compatibility issues between quantum-ready algorithms
- 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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

FIPS 140 VALIDATION PROGRAM (CURRENT STATUS)

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

March - June 2024

Cryptographic Algorithm Validation Program Demo Server

ML-KEM
ML-DSA
SLH-DSA

- **Cryptographic Algorithm Validation Program**
  - Automated Cryptographic Validation Testing System (ACVTS) https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/how-to-access-acvts
  - Demo testing for draft algorithm standards to enable production/official testing once the standards are finalized https://github.com/usnistgov/ACVP-Server
- FIPS 140 implementation guidance on self-test requirements are developed in collaboration with the Cryptographic Module User Forum

- **DRAFT FIPS 203 ML-KEM** (March 2024)
  - Key Generation, Encapsulation, Decapsulation
- **DRAFT FIPS 204 ML-DSA** (March 2024)
  - Key Generation, Signature Generation, Signature Verification
- **DRAFT FIPS 205 SLH-DSA** (May/June 2024)
  - Key Generation, Signature Generation, Signature Verification

https://pages.nist.gov/ACVP/#module-lattice-algorithms

WORK IN PROGRESS

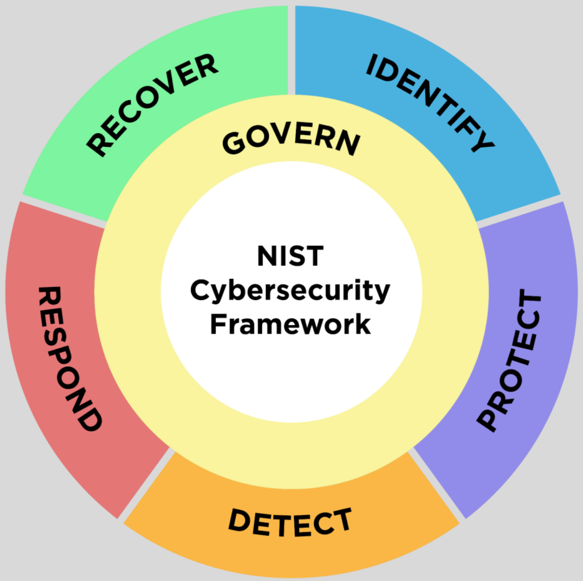
2024

Continue interoperability and performance testing

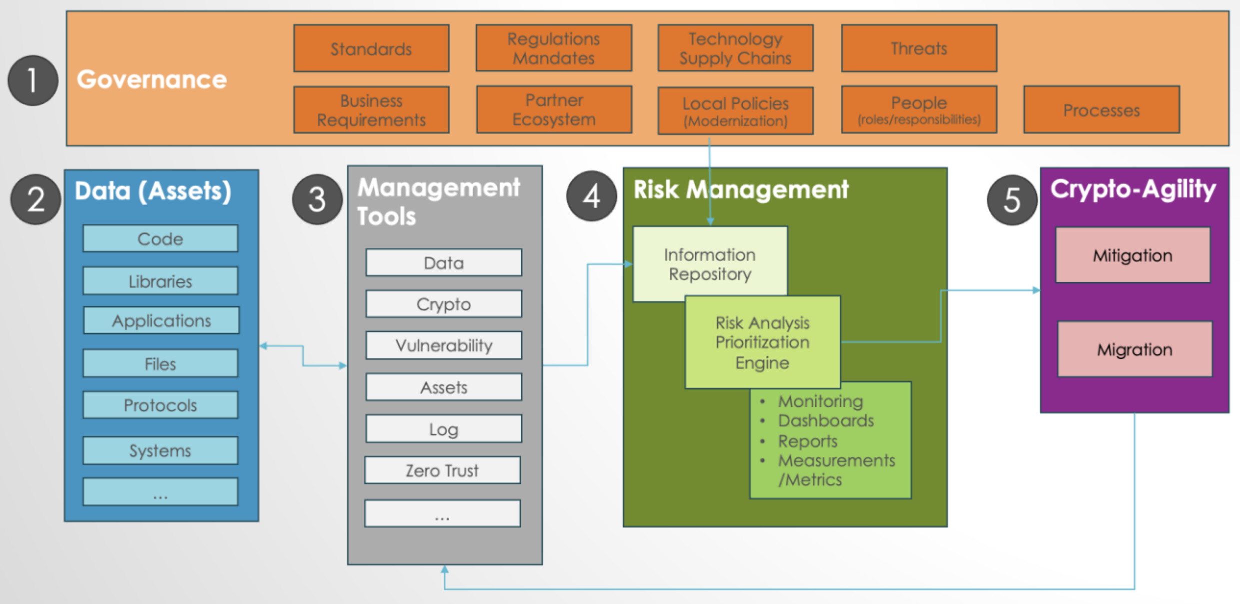
Risk-Based Approach to Manage Quantum Threat to Crypto with a Focus on Crypto Agility

- **IPsec**
- **DNSSEC**
- **Smart Card/PIV**
- **…**

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

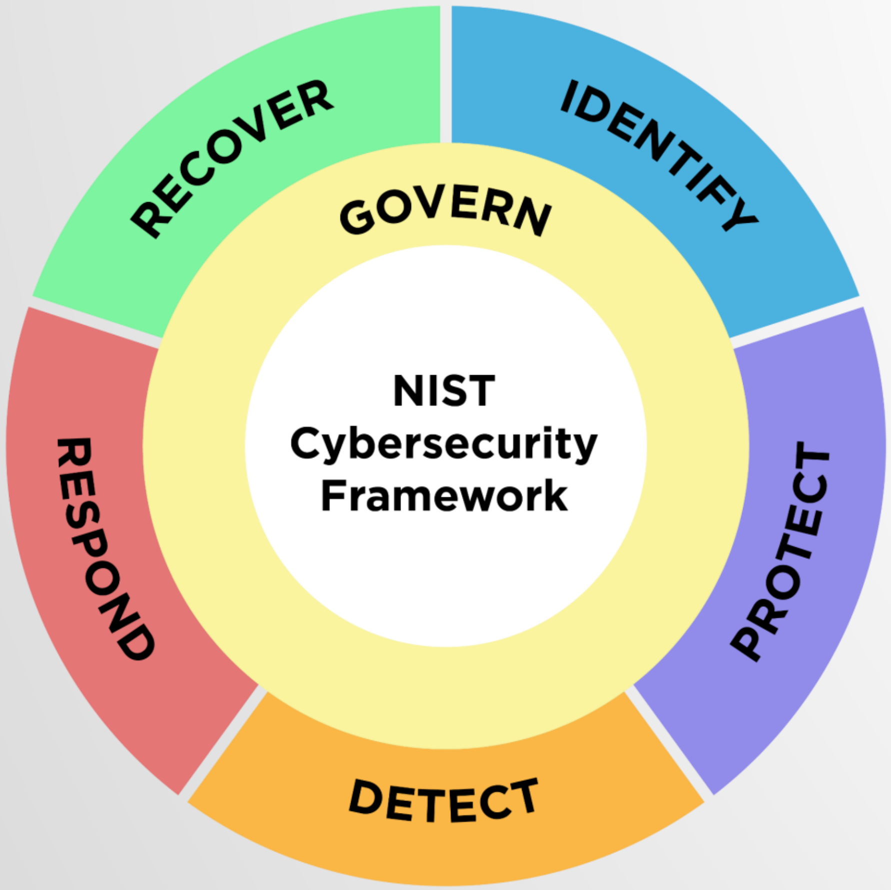


+



A RISK MANAGEMENT FRAMEWORK
CYBERSECURITY FRAMEWORK (CSF) 2.0

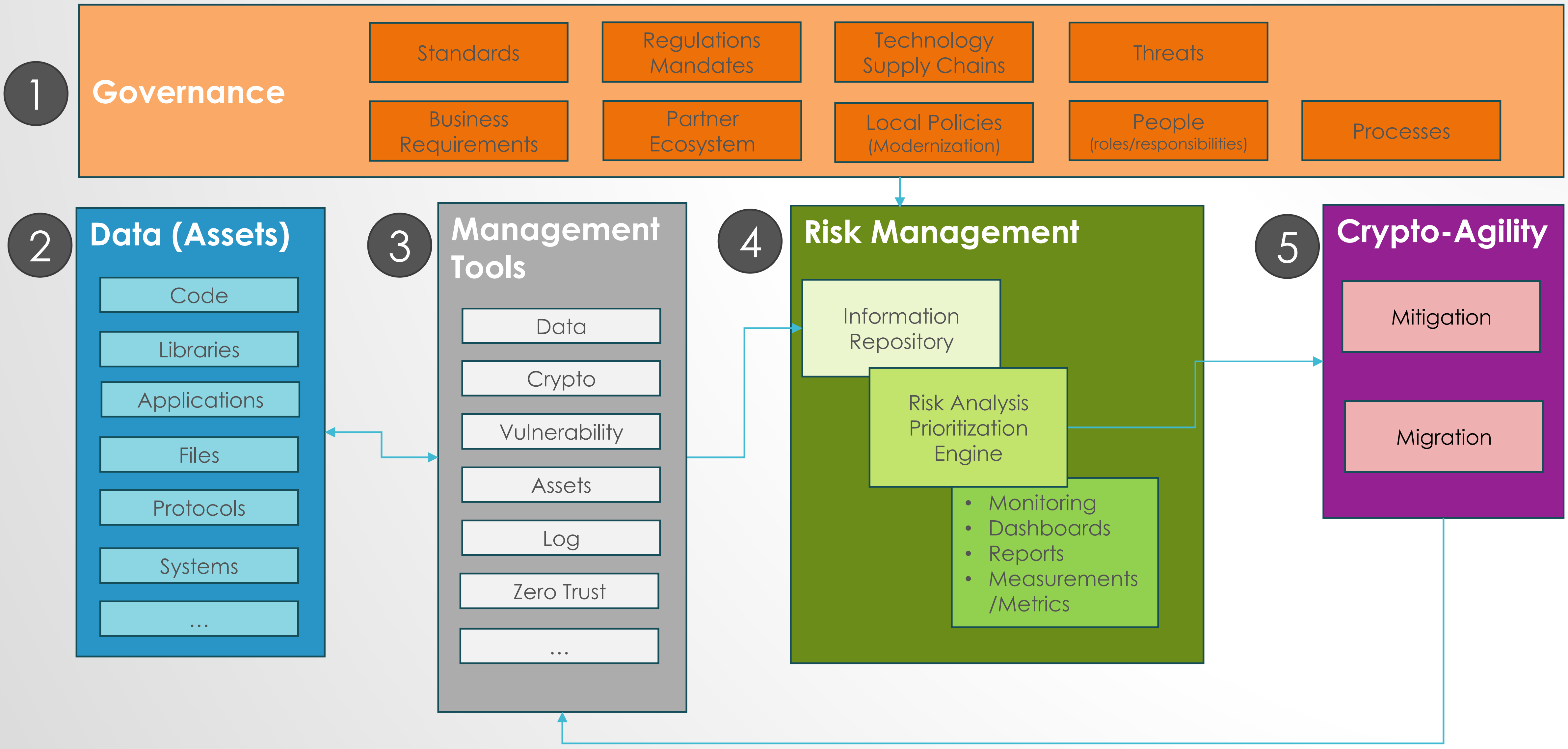
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



Functions	Categories	Subcategories
Govern		
Identify		
Protect		
Detect		
Respond		
Recover		

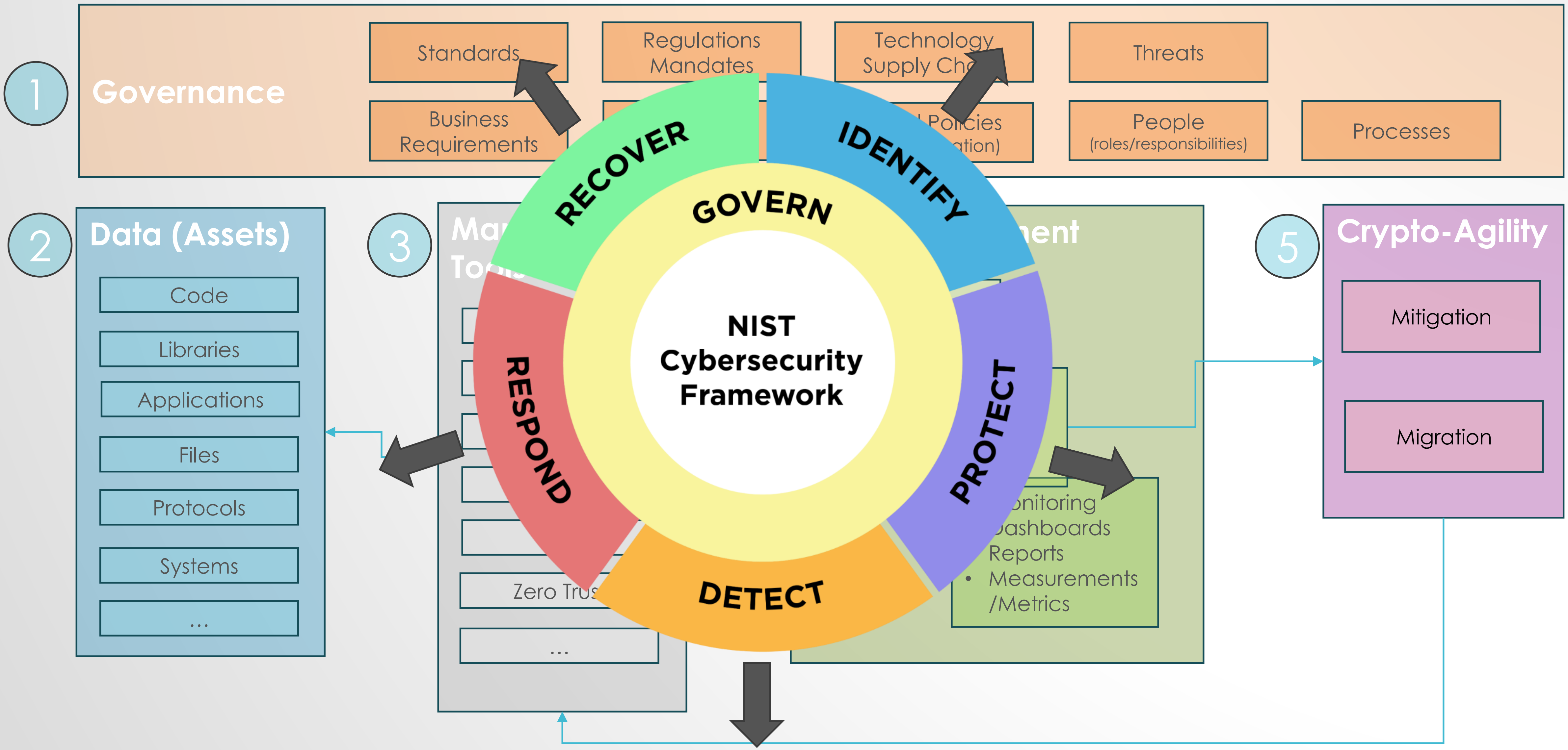
Implementation Examples	*Informative References*

DATA CENTRIC CRYPTO RISK MANAGEMENT APPROACH



INTEGRATION AND ALIGNMENT WITH CSF

CSF PROFILE FOR MANAGING CRYPTO RISK



MANY DIMENSIONS TO CRYPTOGRAPHIC AGILITY

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

May 1 2024

Started the discussion with the NIST PQC consortium to develop guidance to support use cases

- **Motivations** for crypto-agility in migration (designers, developers, implementers, users, etc.)
- Crypto-agility **guiding principles**
  - Independence to applications
  - Simplicity
  - Abstraction
  - Exchangeability
  - Manageability
  - Portability
- **Security** considerations
  - Attack surface
  - Downgrade attacks
- **Maturity model**
  - Measurements, testing, and validation
- **Legal** and **regulatory** considerations
- A **framework** approach
  - Modularity and abstraction
  - Dynamic configuration and management
  - Algorithm adaptability and standardization
- Crypto-agility **technical mechanisms**
  - Protocol level negotiation
  - API abstraction for applications
  - Libraries for algorithms
  - Hardware accelerators
- **Resource and performance**
  - Hardware, firmware, software, and communication protocols
  - Microcontrollers to clouds
- **Use cases** driven demonstrations to inform development of practical guidance

POST QUANTUM CRYPTOGRAPHY – GUIDELINES FOR TELECOM USE CASES VERSION 1.0

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

- Internal to Mobile Network Operator Use Cases
  - Protection and configuration / management of link between base stations and security gateway.
  - Virtualized network functions (on cloud, on NFV infrastructure), including integrity of the uploaded firmware and VNFs. Authentication of privilege access.
  - Cloud Infrastructure (to support virtualized network functions).
  - RSP (Remote Sim Provisioning / eSIM), for M2M (SGP.02), Consumer Electronics (SGP.22) and IoT (SGP.32).
  - Devices and firmware upgrade. This is linked to code signing and ability to have Root of Trust in the device to enable further secure and trustable updates.
  - Concealment of the Subscriber Public Identifier
  - Authentication and transport security 4G (MME-S-GW-P-GW)

https://www.gsma.com/newsroom/gsma_resources/securing-the-mobile-industry-in-a-post-quantum-future/

POST QUANTUM CRYPTOGRAPHY – GUIDELINES FOR TELECOM USE CASES VERSION 1.0

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

- Customer Facing Use Cases
  - Quantum-Safe VPN
  - Quantum-Safe SD-WAN (for enterprise and government clients)
  - Protecting Critical Devices: Electrical Smart Meters
  - Prepare automotive for quantum-safe cybersecurity
  - More linked to privacy (vs security), but key as well regarding privacy preserving and associated regulation (GDPR, …)
  - Lawful Intercept and Retained Data
  - Cryptographic agility: migrating from PQC1 to PQC2

https://www.gsma.com/newsroom/gsma_resources/securing-the-mobile-industry-in-a-post-quantum-future/

NCCOE MIGRATION TO PQC PROJECT REFERENCES

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

- **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 PQC migration project team**
  - applied-crypto-pqc@nist.gov
- **Contact for crypto-agility**
  - lily.chen@nist.gov
- **Contact for FIPS 140 Validation**
  - christopher.celi@nist.gov