Canadian National Quantum-Readiness

BEST PRACTICES AND GUIDELINES

Version 03 - June 12, 2023

Authored by:

Quantum-Readiness Working Group (QRWG)
of the Canadian Forum for Digital Infrastructure Resilience (CFDIR)

TLP:CLEAR

The contents of this document are **TLP:CLEAR**

CONTENTS

ANNEXES:

APPENDICES:

FOREWORD

On behalf of the Canadian Forum for Digital Infrastructure Resilience (CFDIR), I am pleased to introduce the updated Canadian National Quantum-Readiness Best Practices and Guidelines.

The quantum file has made steady progress since the 2020 version of this document was published by the CFDIR's Quantum-Readiness Working Group (QRWG), a team of subject matter experts representing key organizations in Canada's financial sector.

Among other things, Canada has launched a National Quantum Strategy to solidify our country's position among leaders in this fast-growing field. It's evident that new quantum breakthroughs will further transform how people work and live in the years ahead, revolutionizing industries and driving innovation.

We also continue to improve our understanding of the significant potential cyber security issues that could arise as quantum technology overtakes today's security algorithms. This poses risks to personal information, financial systems, utility grids, infrastructure and ultimately Canada's national security.

Both public and private sector institutions can expect a major transition effort over many years to implement new cryptographic technologies. Resources such as this document will be invaluable in that process. New content in this version includes:

- An annex outlining an approach to thinking through a migration of quantum-vulnerable cryptography;
- A white paper on hybrid cryptography standards and technology; and
- A sample quantum-readiness questionnaire to be used with third-parties.

Collaborative work through bodies such as the CFDIR will be critical in the years ahead to identify what needs to be done, and when, to get ready for a post-quantum world.

As the changes expected are still years away, there's no need to panic – yet. But it is important to plan well ahead -- both to realize any future business opportunities and to secure Canada's financial systems for the post-quantum future.

The Bank of Canada will continue to take part in these and other partnerships to promote the ongoing resilience of Canada's financial sector. I would like to convey our appreciation to the CFDIR and QRWG members who work diligently to keep on top of the quantum file. We look forward to continued collaboration as this journey unfolds.

Hisham El-Bihbety

CISO – Bank of Canada

ACKNOWLEDGEMENTS

The contents of this document were developed during the course of CFDIR Quantum-Readiness Working Group (QRWG) meetings and workshops between July 2020 and June 2023.

The information and recommendations contained herein were informed by the active participation and engagement of subject matter experts from the following organizations (listed alphabetically):

CFDIR MEMBERS:

Accenture, AWS, BlackBerry, CCCS, CIRA, Cisco Systems, Google, IBM, ISED, Microsoft, Quantum-Safe Canada, Thales Canada

QUANTUM-READINESS PILOT PROJECT PARTICIPANTS:

Bank of Canada, BMO, CIBC, Desjardins, Financial Services Regulatory Authority of Ontario, Manulife Bank, National Bank of Canada, Payments Canada, Royal Bank of Canada, Scotiabank, Sun Life, TD, 2Keys

QUANTUM-SAFE ECOSYSTEM STAKEHOLDERS:

Crypto4A, Cryptosense, Entrust, evolutionQ, InfoSec Global, ISARA

ADDITIONAL ORGANIZATIONS:

Financial Services Information Sharing and Analysis Center (FS-ISAC)

German Federal Office for Information Security (BSI)

U.S. National Cybersecurity Center of Excellence (NCCoE)

Toronto Metropolitan University (formerly Ryerson University) - Cybersecurity Research Lab

University of Waterloo - Open Quantum Safe (OQS) project

A FEW WORDS ON CRYPTOGRAPHY

Throughout this document, the terms “cryptography” and “crypto” mean the practice of cryptography, which includes constructs such as encryption, digital signatures, hashing, and more. In particular, the term “crypto” does not refer to cryptocurrency, which is a form of unregulated digital currency that utilizes cryptography and often blockchain technologies.

REVISION HISTORY

The following table describes the dates of the major changes to this document.

Authors	Date / Version	Notes
CFDIR QRWG Participants (July 2020 – June 2021)	July 7, 2021 / v.01	Initial version of recommended Best Practices developed from the QRWG's pilot project with members of Canada's Finance CI sector.
CFDIR QRWG Participants (July 2021 – June 2022)	June 17, 2022 / v.02	Updated Best Practices reflecting information obtained during the second year of the QRWG's collaboration with members of Canada's finance critical infrastructure sector, including meetings with post-quantum ecosystem stakeholders and three mini-workshops focused on hybrid cryptography.
CFDIR QRWG Participants (July 2022 – June 2023)	June 12, 2023 / v.03	Refreshed and expanded Best Practices including updates to previously published content, plus brand new guidance on (1) cryptographic-agility and (2) PQC product/service roadmap questions for Information and Communications Technology (ICT) vendors.

1. INTRODUCTION

Cryptographic technologies are used throughout government and industry to authenticate the source and protect the confidentiality and integrity of information that we communicate and store. Cryptographic technologies include a broad range of protocols, schemes, and infrastructures. [1]

> ***Quantum computers will break currently deployed public-key cryptography, and significantly weaken symmetric key cryptography, which are pillars of modern-day cybersecurity. Thus, before large-scale quantum computers are built, we need to migrate our systems and practices to ones that cannot be broken by quantum computers. For systems that aim to provide long-term confidentiality, this migration should happen even sooner.***
>
> Cybersecurity in an era with quantum computers: will we be ready?
> *Michele Mosca, November 2015*

Canadians rely on cryptographic systems to secure their applications and websites, and to protect the confidentiality and integrity of their data from domestic and global cyber threat actors. Quantum computers, when used by malicious actors, will be able to break many of today's cryptographic systems. To counter this threat, digital systems that process, store, or transmit sensitive or confidential information will need to be upgraded to use new "quantum-safe" Post-Quantum Cryptography (PQC).

Unfortunately, quantum-resistant solutions are not yet available. The U.S. National Institute of Standards and Technology (NIST) began work on new standards for PQC in 2015, and is currently on-track to publish a first set of PQC standards in 2024.

> ***If your organization stores or communicates sensitive information, the use of post-quantum cryptography will be an inevitability in the next few years. To make this transition as smooth as possible, there are practical steps you can and should be taking to ensure your sensitive information remains secure both now and in the future.***
>
> Forbes magazine, *January 8, 2021*

The good news is there should be enough time for Canadian businesses and other organizations, including Critical Infrastructure (CI) owners and operators, to plan an orderly and cost-effective transition to quantum-safe cryptography over the next few years, using the recommended practices and guidelines in this document.

[1] Migration to Post-Quantum Cryptography, U.S. National Institute of Standards and Technology, August 2021

1.1 OBJECTIVE

The goals of this document are to provide a set of recommended practices and guidelines:

- that Canadian Critical Infrastructure sector stakeholders and others can use now, to plan and prepare for how they will transition their digital systems to use new quantum-resistant cryptographic technologies and solutions; and
- to shorten learning curves by offering tangible advice and examples that illustrate "how to" undertake the recommendations made herein, so as to reduce the need for organizations to "start from scratch".

This document will be updated annually, to reflect industry feedback from implementing the best practices presented herein, and to provide additional examples of "how to" operationalize more of the strategic recommendations described in Section 3.

1.2 THE QUANTUM THREAT

Asymmetric cryptography, or public-key cryptography, provides confidentiality and integrity for sensitive information. It is used extensively by the Government of Canada (GC) and by private sector organizations to secure and protect communications networks, cryptographic keys during their distribution, data at rest, and more. Most organizations currently rely on public-key cryptography to secure:

- **digital signatures**: used to provide source authentication and integrity authentication as well as support the non-repudiation of messages, documents, or stored data;
- **identity authentication processes**: to establish an authenticated communication session or authorization to perform a particular action;
- **key transport of symmetric keys** (e.g., key-wrapping, data encryption, and message authentication keys) and other keying material (e.g., initialization vectors); and
- **privilege authorization processes**.

Security implications of quantum computing:

Current encryption protocols, such as Secure Socket Layer (SSL) and Transport Layer Security (TLS), based on existing public-key algorithms, are capable of protecting network communications from attacks by classical computers.

A fault-tolerant quantum computer, however, could break the mathematical challenges that underlie these and other protocols in a matter of hours or even seconds.

Deloitte Insights, April 2021

Asymmetric cryptography is based on the premise that two or more parties exchange public keys to establish a shared secret key to encrypt data. Symmetric cryptography on the other hand is

based on the premise that all parties have already shared the exact same key prior to communicating.

Once developed, quantum computers will be able to use quantum physics to efficiently process information and solve problems that are impractical to solve using current computing technologies. Quantum computers will be able to compromise the algorithms used in asymmetric cryptography. This means that all classified, sensitive, and/or confidential information and communications that were protected using public-key cryptography, especially those having a medium to long-term intelligence value or commensurate need for long-term confidentiality, will be vulnerable to decryption by adversaries or business competitors that have quantum computers.[2]

1.3 WHY START PREPARING NOW?

The argument for starting now, to address the threat that quantum computers will pose to existing security systems, is based on the following considerations:

a) cryptographic technologies are integrated into most of the digital products commonly used by organizations to run their daily operations;[3]

b) some of the applications and systems used within energy, transportation, finance and government infrastructures have product lifetimes of 15 - 30 years, and even longer requirements for data protection and privacy;

c) fault-tolerant quantum computers, capable of breaking existing encryption algorithms and cryptographic systems (e.g., public-key infrastructures), are widely expected to be available within the above timeline (e.g., by 2035);[4]

d) the time needed to migrate installed cryptographic technologies (e.g., SHA1) to something newer can take many years;[5]

e) the number of cryptographic systems that organizations will need to migrate to use new "quantum-safe" cryptography will be large; and

---

[2] Addressing the quantum computing threat to cryptography (ITSE.00.017), Canadian Centre for Cyber Security, May 2020

[3] Using Encryption to Keep Your Sensitive Data Secure (ITSAP.40.016), Canadian Centre for Cyber Security, May 2021

[4] National Security Memorandum on Promoting U.S. Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (White House), May 4, 2022

[5] The SHA1 hash function is now completely unsafe | Computerworld, February 2017

f) most organizations have no clear view of the cryptographic technologies used by their existing Information Management (IM), Information Technology (IT) and Operational Technology (OT) systems; this will make it difficult to discover and then prioritize the systems to be upgraded to post-quantum cryptography. [6]

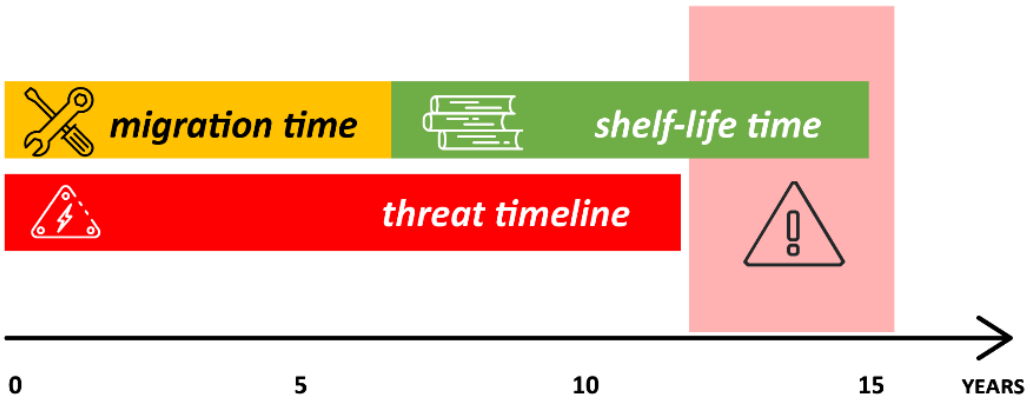
Migrating an organization's cryptographic systems to PQC will require significant effort. Organizations should begin planning now given that:

- the effort and time needed (e.g., to investigate, analyse, plan, procure, migrate, and validate new PQC) will not be small, and it will be different for every organization, and
- the amount of time remaining (until threat actors can access sufficiently powerful quantum computers to break existing cryptography) will decrease every day.

1.4 HOW MUCH TIME IS AVAILABLE?

The amount of time that an organization will have to transition its systems to use new quantum-safe cryptography (QSC) depends on three factors:

- the ***migration time***: the number of years the organization will need to migrate all of the systems that handle its important data to new quantum-safe cryptography;
- the ***shelf-life time***: the number of years that the organization's important, high-value information needs to be protected; and
- the ***threat timeline***: the number of years before relevant threat actors will be able to break the organization's existing, quantum-vulnerable, cryptography. [7]



[6] Post-Quantum Cryptography: Frequently Asked Questions, U.S. Department of Homeland Security (DHS), October 2021. 2 pages

[7] 2022 Quantum Threat Timeline Report, Global Risk Institute, 14 December 2022

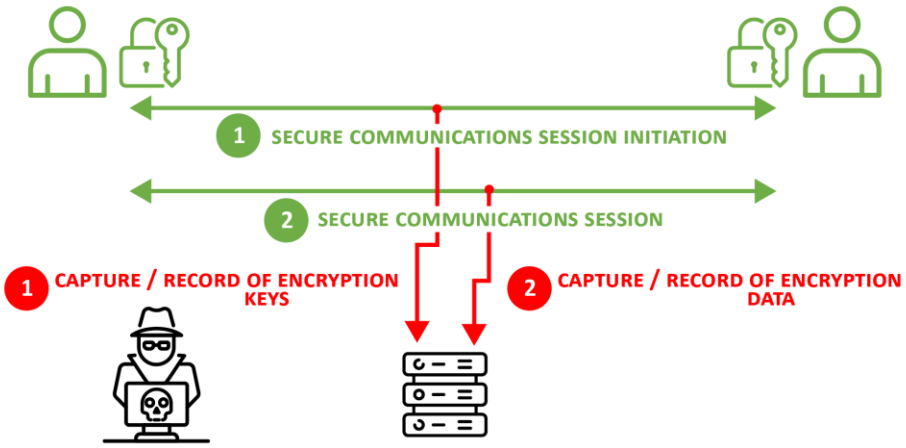
As illustrated on the previous page:

- organizations may need many years to migrate to Quantum-safe cryptography; and
- many organizations have important information (e.g., trade secrets, customer data, business plans) that they wish to keep confidential for a long time.

In the worst case, a threat actor will be able to use a quantum computer to break the encryption protecting important information before that data is protected by QSC.

Some threat actors (e.g., nation state level adversaries) are known to be harvesting copies of encrypted information today, and storing it for decryption in the future. Thus, any information that needs to be kept confidential for a long time (e.g., more than 10 years) may already be at risk of "harvest now, decrypt later" attacks. It must be noted that the shelf-life time for critical data and information such as trade secrets can be over 50 years.

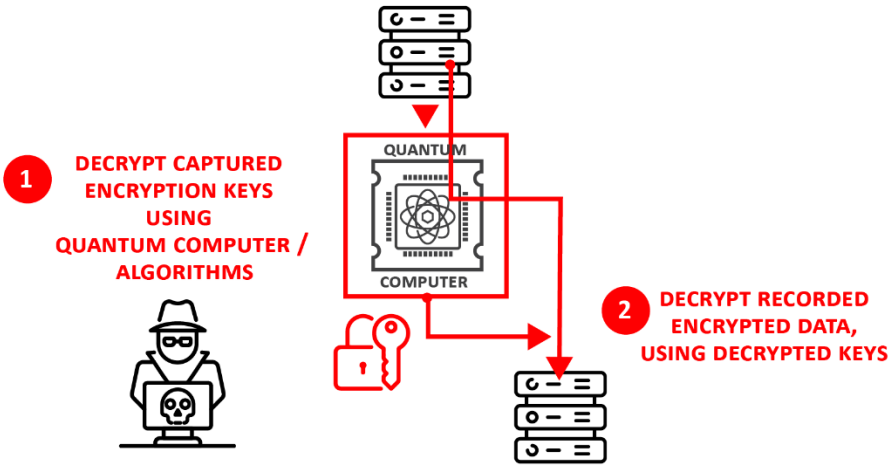
Today



	Users	Threat Actor
1	Secure communications session initiation includes crypto key exchanges	Capture / Record Encryption Keys
2	Encrypted session	Capture / Record encrypted data

Risk Mitigation Actions
Leverage information security and cyber security best practices and controls to help reduce current risks

In the best case, organizations that begin to assess their quantum-readiness now will have time to migrate their most important systems to use quantum-resistant cryptography before threat actors (and business competitors) obtain quantum computers. [8, 9]

Future


	Threat Actor
1	Captured encryption keys are decrypted using large scale quantum computers and quantum algorithms
2	Decrypted keys enable the decryption of captured encrypted data
Risk Mitigation Actions Immediate start of Quantum Readiness planning and actions to prepare for future quantum threats	

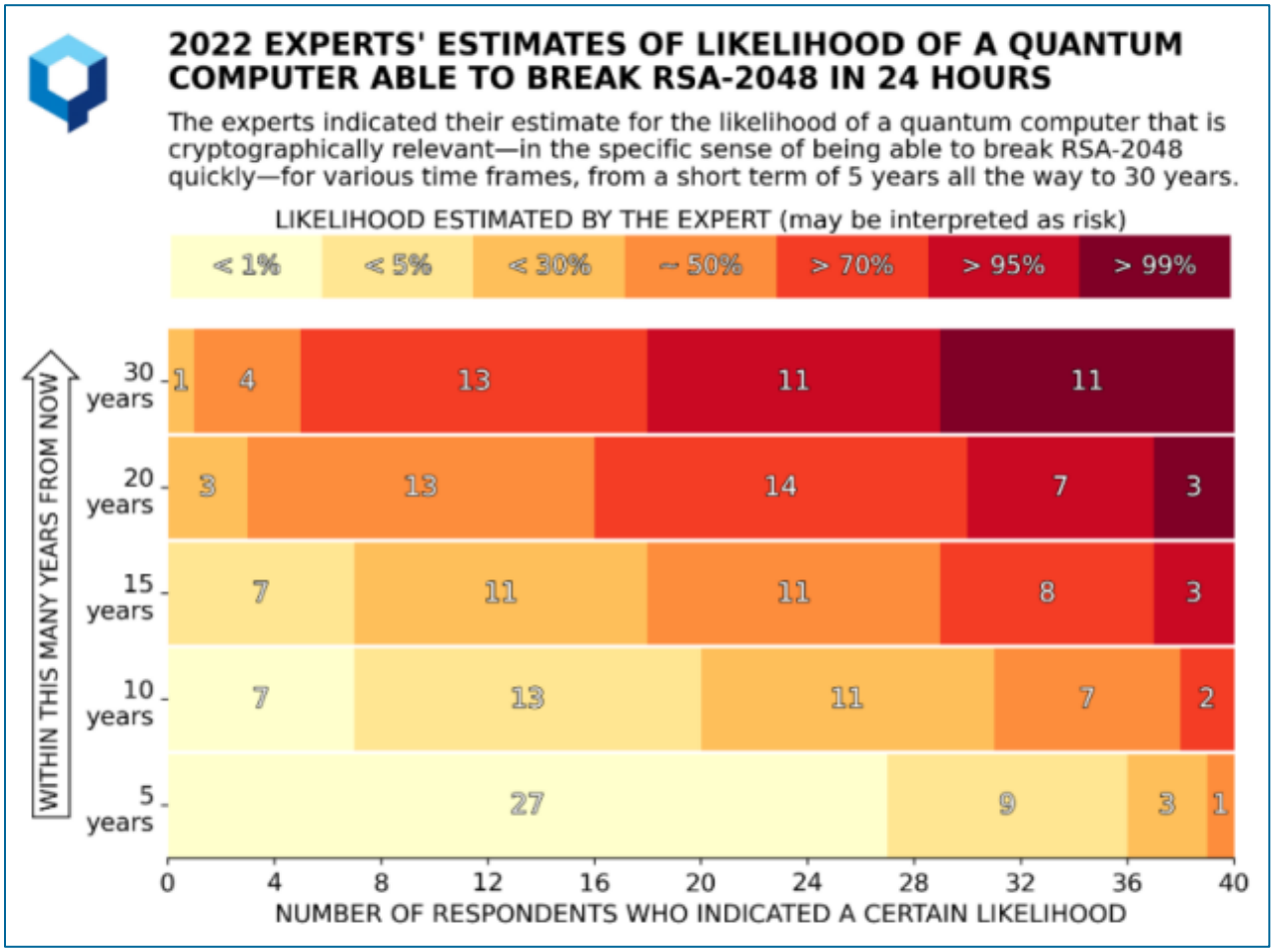
With respect to the threat timeline, the figure on the next page summarizes the latest opinions of 40 global quantum experts.

---

8 The US is worried that hackers are stealing data today so quantum computers can crack it in a decade MIT Technology Review, November 3, 2021, 5 pages

9 The race to protect us from a quantum computer that can break any password (inews.co.uk), May 18, 2023, 9 pages

Every organization will need to review information such as this, and then decide on how much time they have, based on their own risk tolerance.



The opinions (of 40 experts from 14 countries) suggest that the quantum threat will become non-negligible relatively quickly and it could well become concrete sooner than many expect. For example, 20 out of 40 respondents felt it was more that 5% likely already within a 10 year timeframe, with 9 respondents indicating a likelihood of about 50% or more.

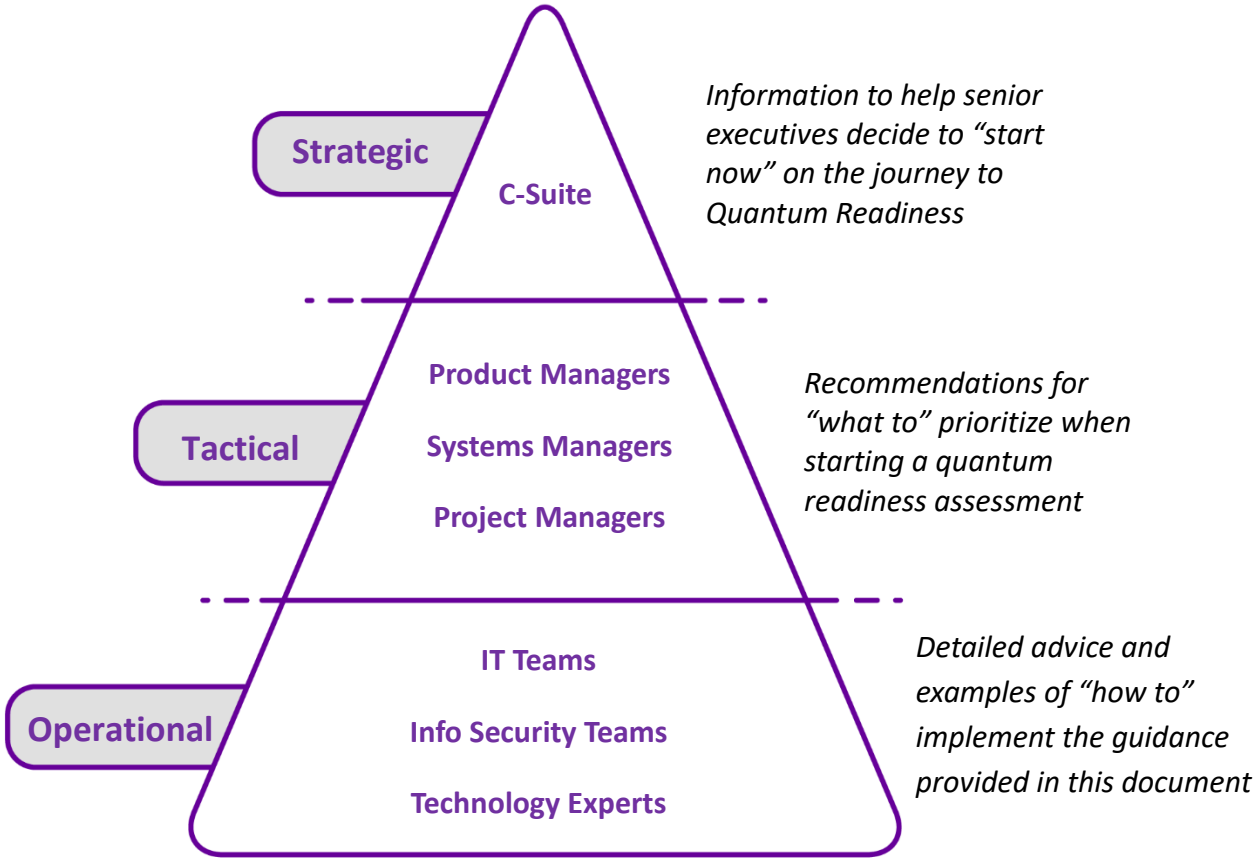
2022 Quantum Threat Timeline Report
Global Risk Institute, 14 December 2022

1.5 ABOUT THIS DOCUMENT

In June 2022, the Canadian Forum for Digital Infrastructure Resilience (CFDIR) rechartered its Quantum-Readiness Working Group (QRWG) to continue developing and updating its previously published best practices and guidelines for owners and operators of Critical Infrastructure (CI) systems. A series of discussions, discoveries and in-depth examinations were organized, in conjunction with stakeholders from Canada's Finance CI sector and the ICT vendor community, to refresh the guidance in this document on key considerations that C-suite executives, their direct reports, and their IM, IT, and OT staff will need to address to evolve their existing cryptographic systems to be "quantum-ready" (i.e., quantum-safe) in the coming years.

The information herein can be used and adapted by organizations as needed to inform decision makers on why and when to start their organization's journey to quantum-readiness, and to provide guidance to operational staff on "how to" implement the recommended actions.

The contents of this document include strategic and tactical recommendations (in Sections 3 to 5), and operational advice (e.g., sample "how to" guides) in its Annexes and Appendices.



2. SOURCES OF INFORMATION

The sources of information used to formulate the practices and guidelines recommended in this document have been drawn from an extensive variety of sources in the public domain, and from discussions and deliberations within the CFDIR QRWG.

Primary sources include:

- Canadian Centre for Cyber Security (CCCS) publications;
- U.S. National Institute of Standards and Technology (NIST) Computer Security Resource Center Publications on Post-Quantum Security;
- European Telecommunications Standards Institute (ETSI) Quantum-Safe Cryptography working group documents; and
- Internet Engineering Task Force (IETF) Request For Comments (RFC) documents.

Where appropriate in later sections of this document, links to specific publications from the above sources may be identified as “normative references”. Normative documents are publications that must be read to understand or to implement the guidance being provided.

In contrast, some of the other sources highlighted in this document are referred to as “informative references”. Informative documents help the reader to develop a better understanding of a particular subject area.

Informative sources cited in this document include:

- Open source magazine articles, peer-reviewed papers and conference proceedings;
- World Economic Forum (WEF) and Global Risk Institute papers;
- Archived webcasts of expert panel discussions and presentations from PQC conferences (e.g., PCI Consortium’s March 2023 PQC Conference); and
- Open source content (e.g., white papers, case studies, application notes) from private sector CFDIR member companies and other suppliers of ICT products or services involved in the supply-chain for “Quantum-safe” solutions.

3. RECOMMENDED QUANTUM-READINESS BEST PRACTICES

Executives are encouraged to direct their organizations to start preparing now: [10]

- to understand the risks that quantum computing advancements will pose to their IM, IT and OT systems and data; and
- to plan how to manage the risks to their quantum-vulnerable systems by transitioning those systems and important data assets to introduce support for standardized quantum-resistant cryptography as early as 2025.

Recommended actions that can be started now include the following steps: [11]

1. Educating your peers and your teams on the emerging quantum threat and the new technologies for quantum-safety including **hybrid cryptography** and **cryptographic agility**. [12, 13]

2. Evaluating the sensitivity of your organization's information assets and determining their lifespans to identify information that may be at risk (e.g., as part of ongoing risk assessment processes).

3. Inventorying the IM, IT and OT systems in your organization that use cryptography, and then implementing new policies and procedures in your change management activities to maintain this inventory on an on-going basis.

4. Asking the vendors of your cryptographic products if they support cryptographic agility, as well as when and how they will implement standardized and validated quantum-safe cryptography. [14]

5. Talking to your business partners and other third party suppliers about their current PQC posture and timelines for quantum-safety. [15]

---

[10] Getting Quantum Safe in 5 Slides – Executive Presentation, Cloud Security Alliance Quantum-Safe Security working group, February 2022

[11] Preparing Your Organization for The Quantum Threat to Cryptography (ITSAP.00.017), Canadian Centre for Cyber Security, February 2021

[12] Overview of Hybrid Cryptography, CFDIR QRWG, Annex H of this document

[13] Guidance on Becoming Cryptographically Agile (ITSAP.40.018), May 2022

[14] PQC Roadmap Questions to Ask Vendors, CFDIR QRWG, Appendix G of this document

[15] Questions to Assess the PQC posture of a 3rd party, CFDIR QRWG, Appendix E of this document

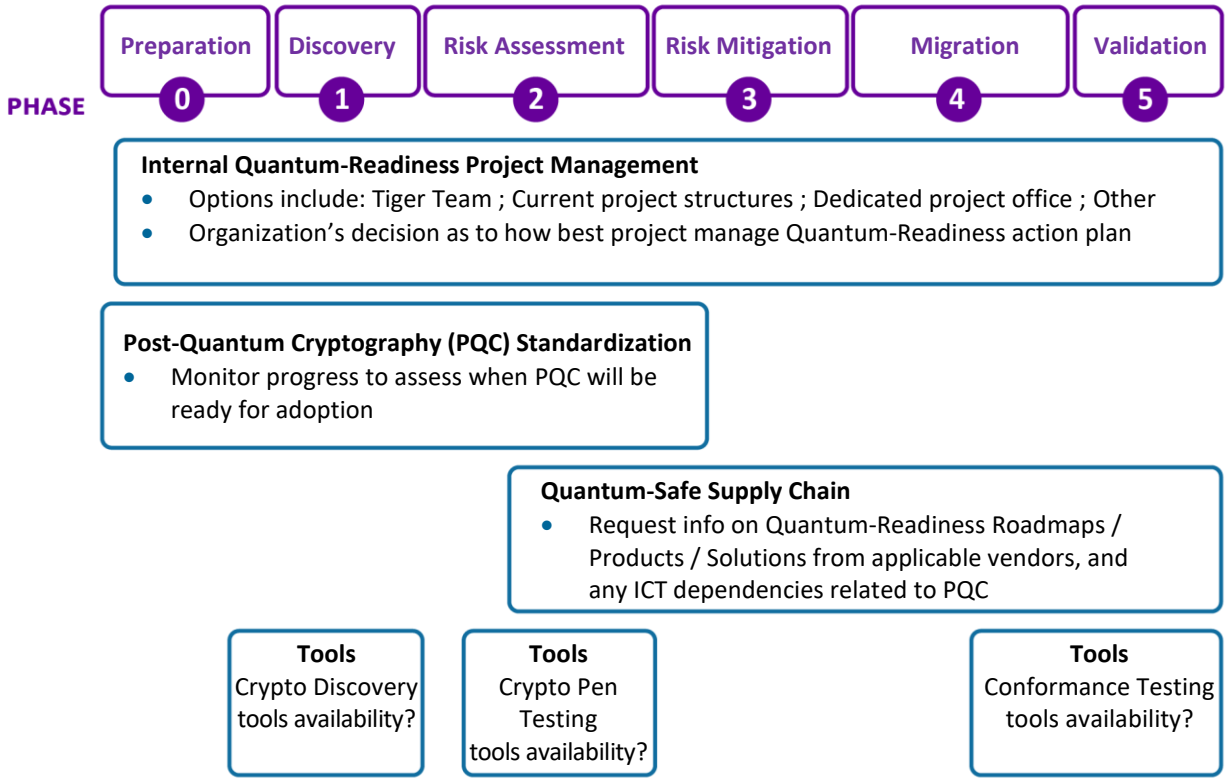
6. Budgeting for potentially significant software and hardware updates, as the timeframe for necessary replacement approaches.

7. Updating your IM, IT, and OT life-cycle management plans to explicitly describe how and when your organization will implement post-quantum cryptographic algorithms to protect your most important data and systems starting 2024-2025, or when validated cryptographic modules become available (e.g., a year later).

With respect to organizing these recommended actions into a Quantum-Readiness program, a multi-year and multi-phase timeline is recommended, as described below.

Quantum-Readiness Program Elements

Some Conceptual Building Blocks



While recognizing that every business is unique and that no one size fits all, each organization's Quantum-Readiness work plan should progress through the following project ***Stages*** and ***Phases***:

- **Stage I: Initial Planning & Scoping**, managed as three distinct project phases that should be started before the first standards for new Post-Quantum Cryptography (PQC) are completed in 2024:

  Phase 0 - Preparation

  Phase 1 - Discovery

  Phase 2 – Quantum Risk Assessment

- **Stage II: Implementation**, starting in 2025, also consisting of three distinct phases:

  Phase 3 - Quantum Risk Mitigation

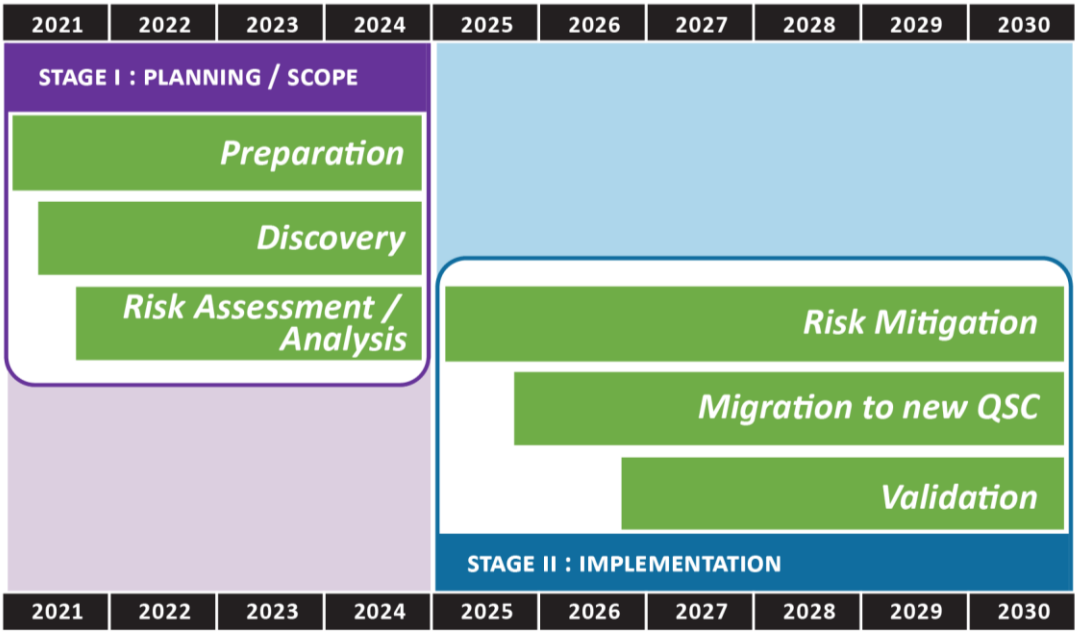
  Phase 4 - Migration to new QSC

  Phase 5 - Validation

The following timeline is recommended to set expectations with respect to the number of years that organizations may need to achieve full quantum-readiness using standardized PQC.

Quantum-Readiness Program Timeline

Recommendations as of June 2023



The anticipated duration (in years) for each Stage and Phase shown above reflects the current consensus of the CFDIR QRWG.

Sections 3.0 to 3.2 of this document recommend ***Planning and Scoping*** actions and best practices for the first three phases. They describe what an organization needs to do to start preparing their IM, IT, and OT systems for new quantum-safe technologies between now and 2024.

Future versions of this document will offer additional guidance and recommended best practices for the post-2024 ***Implementation*** phases.

3.0 PHASE 0 - PREPARATION

(RECOMMENDATIONS FOR C-SUITE EXECUTIVES)

1. Develop an understanding of the threats that quantum computing will pose for your ICT infrastructure in the coming years. Request a briefing within 6 months.

   Normative reference:

   - **NIST**: Cybersecurity White Paper - Getting Ready for PQC April 2021, 10 pages

   Informative references:

   - InfoSec Global Blog: The Time for Post-Quantum Readiness is Now, January 28, 2022, 1 page
   - Cloud Security Alliance: Getting Quantum Safe in 5 Slides – Executive Presentation, February 2022

2. Ask one (or more) of your staff to form a team to investigate the scope of the effort that will be needed for your organization to start using standardized and new "quantum-resistant" cryptography in the coming years, and to identify which of your IM, IT and/or OT systems may need be remediated first.

   Normative references:

   - **CCCS**: ITSAP.00.017 – Preparing Your Organization for the Quantum Threat to Cryptography, February 2021, 2 pages

   Informative reference:

   - U.S. QED-C: A Guide to a Quantum-Safe Organization, December 6, 2021 (updated July 2022), pages 15-16
   - World Economic Forum: Transitioning to a Quantum-Secure Economy, September 2022, 35 pages

3. Request periodic reporting on the progress of #2 (e.g., quarterly) and decide when to advance to Phase 1 (Discovery), as described in Section 3.1 of this document.

   Informative reference:

   - Internet Society: Cryptography: CEO Questions for CTOs March 2018, 15 pages

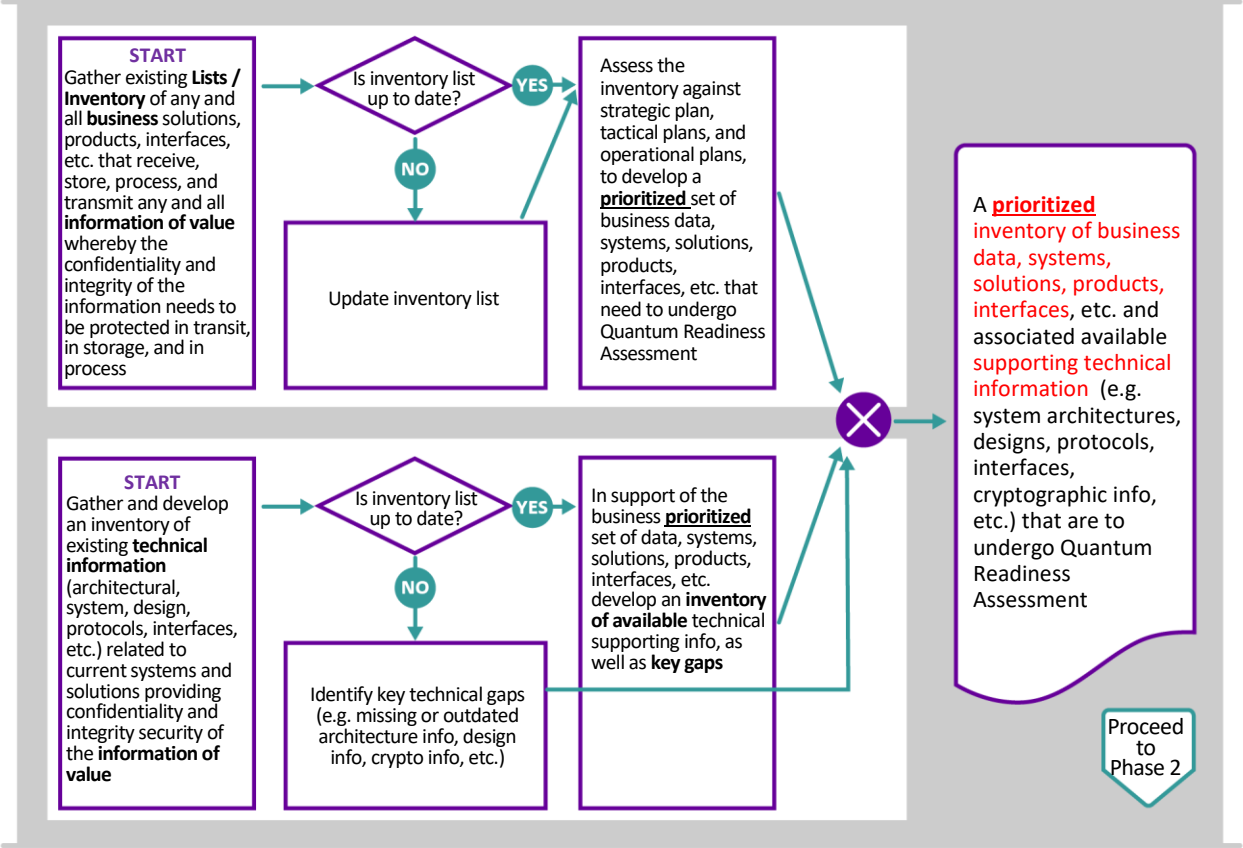
4. Email the CFDIR Secretariat with any questions on the above.

3.1 PHASE 1 - DISCOVERY

(RECOMMENDATIONS FOR C-SUITE EXECUTIVES AND THEIR DIRECT REPORTS)

5. Review the information to be collected during this phase, as illustrated below.
    - The goal is discover where and how cryptographic products, algorithms and protocols are used by your organization to protect the confidentiality and integrity of your organization's important data and digital systems.
    - The information collected during this phase will be needed to assess your organization's quantum risks in the next phase.

Phase 1 : Flow Chart : DISCOVERY



6. Appoint and empower someone to plan and execute a detailed discovery of where and how public-key cryptography is used by your organization.

    Informative references:

    - IBM Redbook: Chapter 2 - The journey to quantum protection, 19 July 2022, pages 15 – 26
    - Entrust: 6 Reasons to do a Cryptography Risk Assessment Right Now, November 2021

7. Investigate whether using automated tools would facilitate your crypto discovery. Organizations should balance their security needs with their needs for usability and availability when considering such automated tools.

   Informative reference:

   - InfoSec Global: AgileSecTM Analytics - Uncovering Certificates, Keys and Cryptography, 6 pages
   - NIST: Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography (Preliminary Draft); Volume A: Executive Summary, SP 1800-38A, April 2023 (updated May 2, 2023), 5 pages

8. Build an inventory of where and how your organization uses public-key cryptography to protect its most important data and IM, IT and OT systems. Also identify any legacy cryptographic systems being used.

   Normative reference:

   - **CISA, NSA** and **NIST**: Quantum-Readiness: Migration to Post-Quantum Cryptography, 2023, Page 2

   Informative references:

   - Forbes Technology Council: Building a Strong Cryptography Strategy (Part I): Securing Your Data Assets April 20, 2021, 3 pages
   - FS-ISAC: Infrastructure Inventory Technical Paper, March 2023, 19 pages

9. Identify the important factors in which public-key cryptography affects the operation and security of your systems and applications (e.g., key sizes, latency and throughput limits, current key establishment protocols, how each cryptographic process is invoked, dependencies).

   Normative references:

   - **CFDIR QRWG**: Content Needed to Describe an Organization's Uses of Cryptography, Annex C of this document
   - **CFDIR QRWG**: Sample Use Case #1 - Using Kerberos for Authentication, Annex D of this document
   - **CFDIR QRWG**: Sample Use Case #2 - PKI/CA's, Annex E of this document
   - **CFDIR QRWG**: Sample Use Case #3 - sFTP, Annex F of this document
   - **CFDIR QRWG**: Matrix of Cryptography Use Cases, Annex G of this document

   Informative reference:

   - NIST: Getting Ready for Post-Quantum Cryptography, Cybersecurity White Paper, April 28, 2021, Page 5

10. Analyze the findings from #8 and #9 to develop a prioritized list of your organization's most important quantum-vulnerable systems that must be protected.

    Informative reference:

    - CCCS: ITSAP.00.017 – Preparing Your Organization for the Quantum Threat to Cryptography February 2021, 2 pages

3.2 PHASE 2 – QUANTUM RISK ASSESSMENT

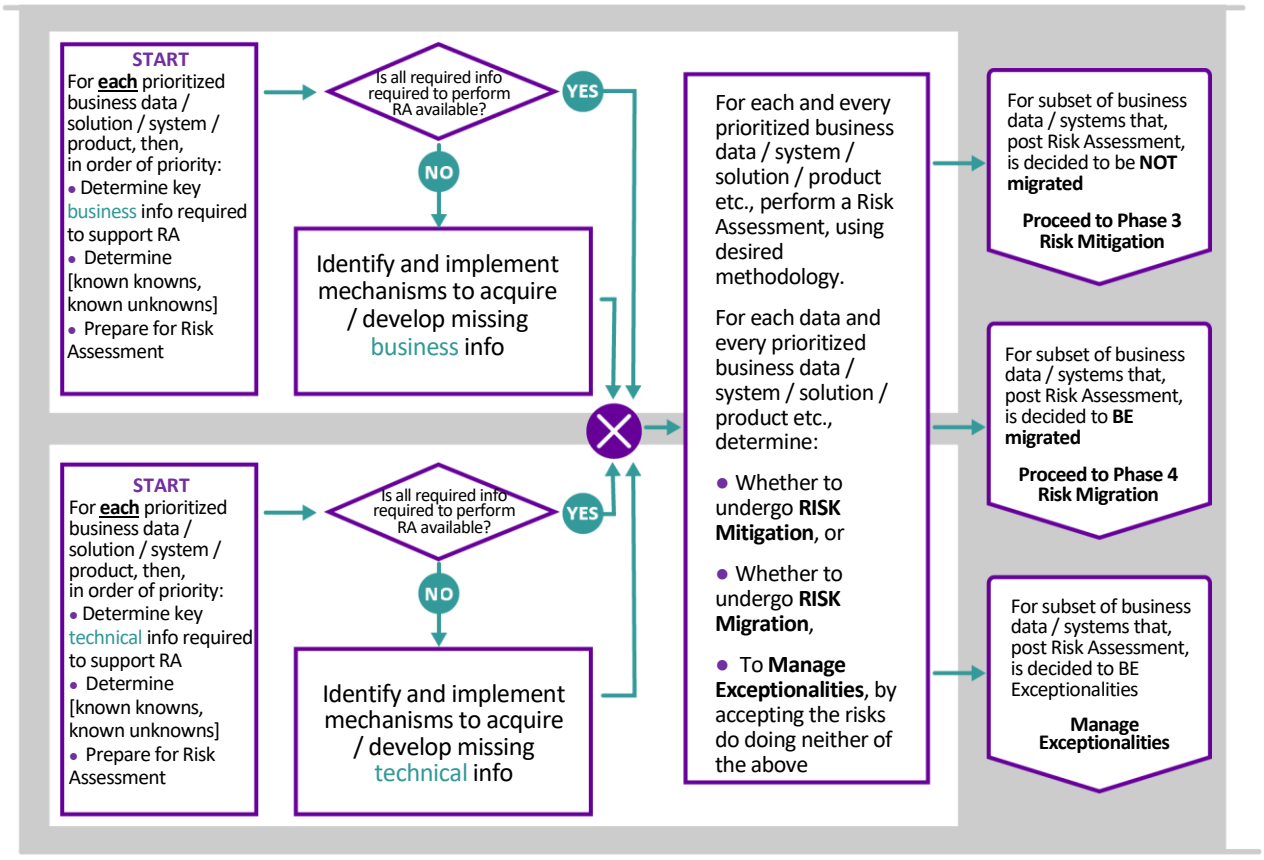
(RECOMMENDATIONS FOR IM, IT, OT MANAGERS AND THEIR DIRECT REPORTS)

11. Review the objectives of this Phase, as illustrated in the diagram below.

The objectives include:

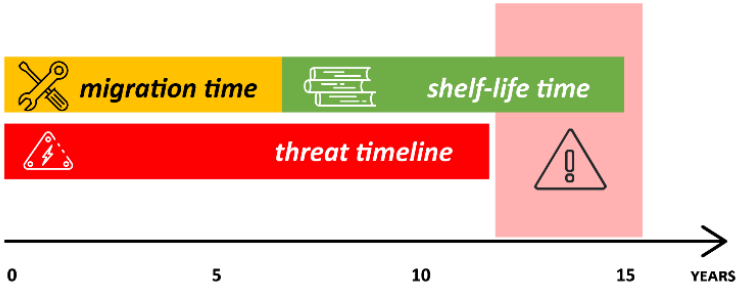
- Evaluating the sensitivity of your organization's information and determining its lifespan to identify the information that may be at risk (e.g. as part of ongoing risk assessment processes).
- Educating yourself and your teams on the threats that quantum computing will pose to your existing uses of cryptography.
- Asking your IM, IT and OT vendors and suppliers about their plans and timetables to implement quantum-resistant cryptography and crypto-agility, to understand any new hardware or software that will be needed.
- Reviewing your IT lifecycle management plans and budgeting for potentially significant software and hardware updates.

Phase 2 : Flow Chart : RISK ASSESSMENT (RA)



12. Start your Quantum Risk Assessment by reviewing the quantum risk equation introduced in Section 1.4, and the inventory of information discovered in Phase 1. That information is needed to determine the following variables for each of the digital systems that handle or store your organization's most sensitive information:

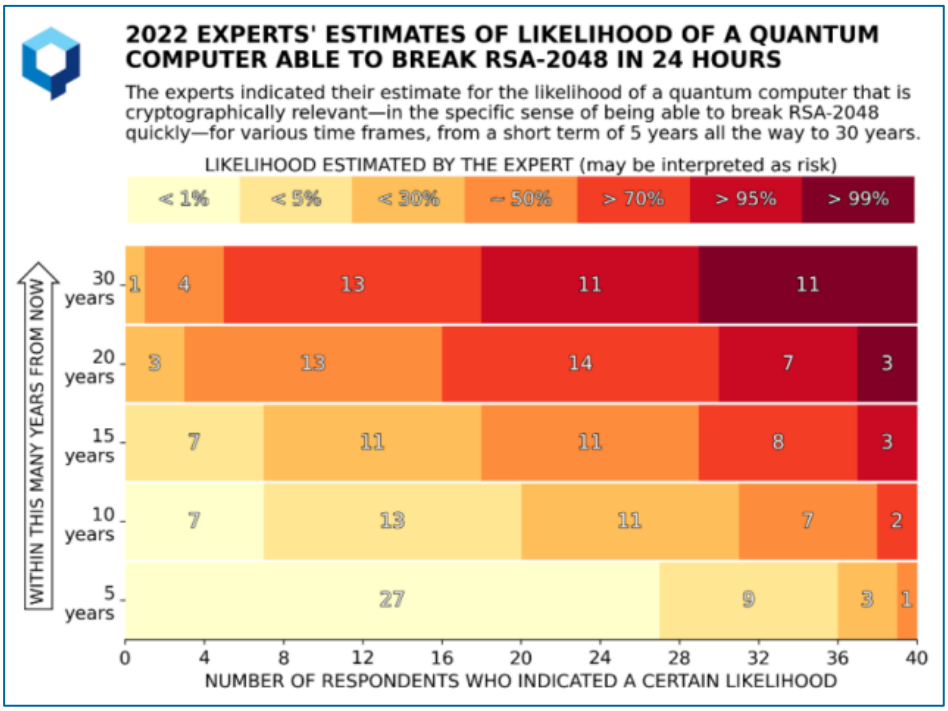
    - the ***shelf-life time*** (measured in years) that your most important data must be protected; and
    - the ***migration time*** *(also measured in years)* that your organization will need to upgrade the systems that handle your longest shelf-life data, to be quantum-safe.



Informative reference:

- Global Risk Institute: 2022 Quantum Threat Timeline Report, 14 December 2022, pages 8-9

13. Decide how the currently anticipated quantum ***threat timeline*** affects your organization's risk posture. To do this, review open source information such as the following and then determine your threat timeline based on your risk tolerance.



Normative reference:

- **Global Risk Institute**: 2022 Quantum Threat Timeline Report, 14 December 2022, page 18

14. Evaluate the sensitivity of your organization's information and determine its lifespan (i.e., the ***shelf-life time*** that your most important data must be protected) to identify information that may be at risk.

    Normative reference:

    - **CCCS**: ITSAP.00.017 – Preparing Your Organization for the Quantum Threat to Cryptography February 2021, Page 2

    Informative reference:

    - FS-ISAC : PQC Future State Technical Paper, March 2023, pages 13 and 14

15. Review your technology lifecycle management plans for each of the quantum-vulnerable systems identified in step #10 of Phase 1. Ask your IM, IT and OT vendors if their product development roadmaps include supporting crypto-agility and/or quantum-resistant cryptography in future updates. If yes, ask when those capabilities will be available.

    Normative reference:

    - **CCCS**: ITSAP.40.018 - Guidance on Becoming Cryptographically Agile, May 2022, 2 pages
    - **CFDIR QRWG**: PQC Roadmap Questions to ask Vendors, Appendix G of this document
    - **CFDIR QRWG**: Questions to Assess the PQC Posture of a 3rd Party, Appendix E of this document

    Informative references:

    - CFDIR QRWG: Template to Catalog Technology Vendor/Supplier PQC Capabilities, Appendix F of this document
    - CFDIR QRWG: Crypto-Agility Notes, Annex I of this document
    - Accenture: The race to crypto-agility, 2021, 18 pages
    - IBM: Transitioning to Quantum-Safe Cryptography on IBM Z, updated August 3, 2022, 208 pages

16. Using the information from #15, estimate the ***migration time*** *(measured in years)* that your organization will need to migrate each of the systems that handle your longest shelf-life data.

    Informative references:

    - CFDIR QRWG: Crypto-Agility Notes, Annex I of this document
    - NIST: Migration to Post-Quantum Cryptography - Project Description, August 2021, Pages 4-6

17. Prioritize the systems that will need the most urgent attention, by listing all of the systems that handle important data for which:

Migration Time + Shelf-life Time > Threat Timeline

Normative reference:

- **CFDIR QRWG**: Matrix of Cryptography Use Cases, Annex G of this document

Informative reference:

- FS-ISAC : PQC Future State Technical Paper, March 2023, pages 26, and 29 to 33.

18. For each dataset, product, system, or solution flagged in #17, determine:

a) whether to undergo risk mitigation (per Phase 3), or

b) whether to start migration to PQC (per Phase 4), or

c) to manage exceptionalities, by accepting the quantum risk and doing neither of the above.

Informative references:

- FS-ISAC: Preparing for a Post-Quantum World by Managing Cryptographic Risk, March 2023, 7 pages
- FS-ISAC: PQC Future State Technical Paper, March 2023, pages 8 to 11, and 30
- Boston Consulting Group: Ensuring Online Security in a Quantum Future, March 2021, 11 pages

19. Also determine if your staff will need new training or additional resources (e.g., tools) to migrate your systems to use quantum-safe, post-quantum cryptography. If yes, the time needed to obtain those tools and/or training should be factored into the per-system migration time estimates developed in #16.

Informative reference:

- FS-ISAC: PQC Future State Technical Paper, March 2023, Pages 16 to 22

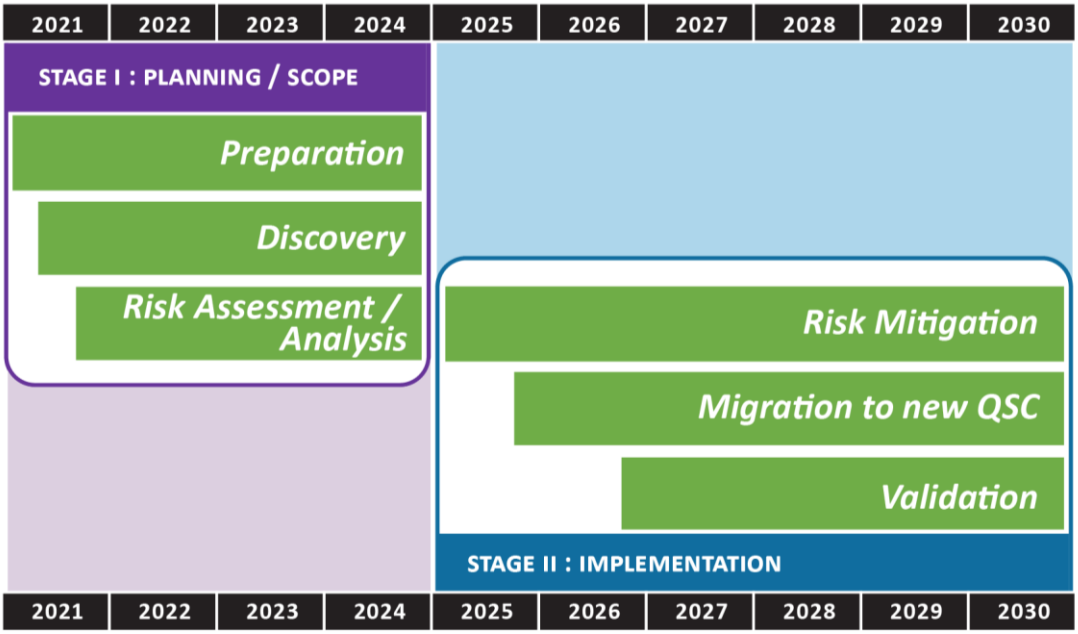
3.3 STAGE II – IMPLEMENTATION (PHASES 3, 4 AND 5)

Future versions of this document will offer guidance and best practice recommendations for the three post-2024 ***Implementation*** phases, namely:

- Phase 3 - Quantum Risk Mitigation
- Phase 4 - Migration to new Quantum-Safe Cryptography (QSC)
- Phase 5 - Validation

Quantum-Readiness Program Timeline

Recommendations as of June 2023



To enable planners to begin preparing for the above now, this document contains the following brand new and/or updated sections with guidance that is relevant to Stage II :

- Annex H contains an updated whitepaper on the topic of **Hybrid Cryptography**. The use of standardized hybrid cryptography may help system owners to mitigate some of the risks of migrating to PQC. Annex H was initially published in 2022 and then refreshed during May 2023 for inclusion in this document;
- Annex I contains brand new notes on a systematic approach to thinking about how and where to start migrating quantum-vulnerable IT systems to make use of quantum-safe cryptography by leveraging **Cryptographic-Agility**; and

- Appendix G of this document contains newly developed **PQC Roadmap Questions** that system owners and operators can use today, to ask when and how their technology providers will introduce PQC capabilities into their products and services.

4. AWARENESS AND SKILLS DEVELOPMENT

Creating an effective quantum risk awareness program will be important for every organization that uses cryptography, large or small, in the coming years.

The CFDIR QRWG developed a suite of slide decks to provide foundational building-block information and materials that can be used and adapted by organizations as needed to raise awareness and to inform decision makers and staff on why and how to begin their Quantum-Readiness journey. These decks may be obtained by emailing the CFDIR Secretariat.

	Contents & Focus	Pages	File Name	Version & Date
1	**Introduction & Context**	5	Quantum-Readiness-WG-Overview-v01	Version 01 July 7, 2021
2	**Master Chart Deck**	62	Quantum-Readiness-Best-Practices-Guidelines-v01	Version 01 July 7, 2021
3	Subset of Master Chart Deck Example #1 – **Executive Primer**	2	EX-01-Quantum-Readiness-Exec-Primer-v01	Version 01 July 7, 2021
4	Subset of Master Chart Deck Example #2 – **Executive Overview**	8	EX-02-Quantum-Readiness-Exec-Overview-v01	Version 01 July 7, 2021
5	Subset Example #3 – **Executive Overview with backup slides**	34	EX-03-Quantum-Readiness-Exec-Overview-with-Backup-v01	Version 01 July 7, 2021
6	Subset Example #4 – **Detailed Overview for Managers**	32	EX-04-Quantum-Readiness-Mgmt-Overview-v01	Version 01 July 7, 2021
7	Subset Example #5 – **Detailed Overview for Managers with Backup slides**	60	EX-05-Quantum-Readiness-Mgmt-Overview-with-Backup-v01	Version 01 July 7, 2021
8	Subset Example #6 – **Detailed Overview for Implementors**	56	EX-06-Quantum-Readiness-Implementors-Overview-v01	Version 01 July 7, 2021

5. RECOMMENDATIONS FOR ENGAGING QSC VENDORS OR OTHER THIRD PARTIES

Solutions to transition to quantum-safe infrastructure are coming … IT and procurement teams must ask their current and prospective vendors for their quantum readiness plans to clarify who will handle which part of the transition and to ensure that investments that are being made today will position organizations towards quantum resilience.

A guide to a quantum-safe organization
U.S. Quantum Economic Development Consortium, December 2021

5.1 PQC ROADMAP QUESTIONS TO ASK ICT PRODUCT OR SERVICE VENDORS

It is recommended that system owners and operators start now to develop insights into the PQC roll-out plans of ICT vendors they depend on. [16]

Appendix G of this document contains eight "PQC Roadmap" questions that a system owner or operator could send to any technology product or service vendor today. These questions were developed by the QRWG during the spring of 2023 and then tested and verified to yield meaningful insights.

- The intent / focus is to provide system owners and operators with a way to start learning about the PQC product or service development plans of each of their technology vendors, in order to inform their own plans (and budgets) for migrating their systems to PQC.
- A secondary benefit (to all) may be that having more organizations asking their ICT vendors about their PQC Roadmaps will increase overall demand or "customer pull" for PQC solutions from vendors which may, in turn, accelerate the availability of PQC solutions.

[16] See step #15 in Section 3.2 of this document.

5.2 RECOMMENDED PQC QUESTIONS TO ASK OTHER THIRD PARTIES

Appendix E of this document contains a different series of questions to help system owners and operators to begin assessing the PQC maturity or 'posture' of any 3rd Party organizations they may do business with. A 3rd Party in this context may be any supplier of products, goods or services (including ICT an non-ICT products/services), or any business partner or any customer.

- The intent/focus is to facilitate an evaluation of a 3rd Party's cryptography and PQC posture to assist the organization that asks the questions in Appendix E, to determine their risk of doing business with the 3rd Party.
- This risk determination can and will vary in different organizations based on their risk tolerance associated to this topic.

5.3 QSC PROCUREMENT CLAUSES FOR RFI'S AND RFP'S

Future versions of this document will offer guidance and best practices for this section.

6. CONCLUSION / KEY TAKEAWAYS

- Canadian businesses, organizations, and Critical Infrastructure owners and operators are advised to take action now, using the recommended practices and guidelines offered in this document, to begin planning an orderly and cost-effective transition to quantum-safe cryptography over the next few years to manage the risks that Quantum computers will pose to them.

Risks	
Cyber attack threat	• **Capture or 'Harvest' Now ; Replay and decrypt later ;** • **Data at Rest ; Data in Motion ;**
Key data at risk	• **Encryption keys ; PII ; Business "crown jewels" ;** • **Intellectual Property**
Risk scope	• **Organization ; Customers ; Supply Chain ; Ecosystems ; Dependencies/Interdependencies**
Perform Organizational Quantum-Readiness Risk Assessment to determine risk	

- Given that every organization is unique, there can be no "one-size-fits-all" approach.

- Quantum-Readiness planning should be started now because migrating an organization's quantum-vulnerable systems to use new quantum-safe PQC will be a multi-year process.

Cryptography	
Discovery	• **Key first step: Develop an accurate inventory of your organization's cryptographic usage across all of the products that depend on your digital systems**
Quantum-Readiness	• **Develop strategies, plans and budgets to upgrade or replace products and/or systems as needed for quantum-safety**
Crypto-Agility	• **One option to facilitate migrating existing cryptography to different or new crypto (e.g., standardized PQC)**
Organizations must prepare to upgrade / replace all cryptographic functions to standards-approved Post-Quantum Cryptography	

- Backward compatibility and interoperability between current and new cryptographic platforms, systems and solutions will be essential during the multi-year transition to Quantum-Safe Cyptography.

- Organizations should leverage all available information resources for the above, including but not limited to:
  - the recommendations presented in this document;
  - internal business and technical experts;
  - open source information; and
  - private sector Canadian and multi-national expertise and/or companies with experience and skills or products related to Quantum-Readiness.

Resources	
CFDIR Quantum-Readiness WG	• **Quantum-Readiness Best Practices and Guidelines**
Canadian Centre for Cyber Security	• **Open-source publications, including cryptographic guidance, alerts and advisories**
Canadian crypto supply chain	• **Canadian supply chain for cryptographic products/services**
Canadian as well as global resources available to help guide organizations prepare for Quantum-Readiness	

ANNEX A: GLOSSARY

- CA - Certificate Authority
- CCCS - Canadian Centre for Cyber Security
- CFDIR - Canadian Forum for Digital Infrastructure Resilience
- CI - Critical Infrastructure
- DECT - Digital Enhanced Cordless Telecommunications
- ENISA - European Union agency for Cybersecurity
- FIPS - (U.S.) Federal Information Processing Standards
- HSM - Hardware Security Module
- IETF - Internet Engineering Task Force
- IKE - Internet Key Exchange
- IM - Information Management
- IPsec - Internet Protocol Security
- IoT - Internet of Things
- ISO - International Organization for Standardization
- IT - Information Technology
- Kerberos - Computer network authentication protocol to allow server communication over a non-secure network
- LDAPS - Lightweight Directory Access Protocol
- MFA - Multi-Factor Authentication
- mTLS - Mutual Transport Layer Security authentication
- NCCoE - (U.S.) National Cybersecurity Center of Excellence
- NIST - (U.S.) National Institute of Standards and Technology
- OAuth - Open standard for access delegation
- OT - Operational Technology
- PGP - Pretty Good Privacy
- PII - Personally Identifiable Information
- PKI - Public-Key Infrastructure
- PQC - Post-Quantum Cryptography
- QRWG - Quantum-Readiness Working Group
- QSC - Quantum-Safe Cryptography

- S/MIME - Secure/Multipurpose Internet Mail Extensions
- SAML - Security Assertion Markup Language
- sFTP - SSH File Transfer Protocol
- SHA1 - Secure Hashing Algorithm version 1
- SSH - Secure Shell
- TLS - Transport Layer Security
- TLP - Traffic Light Protocol

ANNEX B: RECOMMENDED CRYPTOGRAPHY USE CASES TO BE DISCOVERED & DOCUMENTED

This Annex contains a list of technology protocols and broader IM / IT cryptography use-cases applicable to most public and private organizations and businesses across Canada.

Common Protocols:

1) TLS
2) mTLS
3) sFTP
4) FTPS
5) SSH
6) SAML
7) OAuth / OpenID Connect
8) IPsec
9) IKE
10) DMARC
11) DKIM
12) SPF
13) Kerberos
14) LDAPS
15) PGP
16) EAP-TLS
17) WPA (WiFi)
18) S/MIME
19) DECT
20) Mobile NEC
21) DNSSEC
22) DOT / DOH
23) MACsec

Broader Cryptography Use-case Considerations:

A. Code Signing
B. Multi-Factor Authentication (MFA)
C. Encryption of Data at Rest – may be vendor-specific
D. Cloud Native Encryption
E. Hardware Security Modules (HSMs)
F. Certificate Authorities (CAs)
G. Application Layer Payload Encryption

ANNEX C: CONTENT NEEDED TO DESCRIBE AN ORGANIZATION'S USES OF CRYPTOGRAPHY

This Annex provides a list of the information to be sought and then collated when an organization is ready to inventory the cryptography it relies on for any of the use cases listed in Annex B. This information is appropriate to develop during Phase 1 - Discovery.

The content to be inventoried per items 1 to 10 (below) will describe "how things currently are" in one or more of an organization's existing IM, IT and/or OT systems.

1. Use Case Description
2. Business Value
3. Potential Business Data in Scope / Volume of that Data / Lifespan of that Data
4. Use Case Class (e.g., Data in Transit, Data at Rest, Data in Processing, Digital Signature)
5. Technical and Threat Considerations
6. Types of Cryptography Currently in Use
7. Technical Components (e.g., end-points, networks, databases, file servers)
8. Locations where Cryptographic Information Exists (e.g., DLL, hardware)
9. Technical Dependencies (e.g., details on components within this Use Case that depend or rely on other systems for their own security)
10. Ability to Support (Pre and Post-Quantum) Cryptographic Algorithms Simultaneously

After the above information is collected, analyzing it will enable planning "What to do to reduce the quantum risk?" in later project phases (e.g., Quantum Risk Assessment, Quantum Risk Mitigation, Migration to Quantum-safe PQC), including:

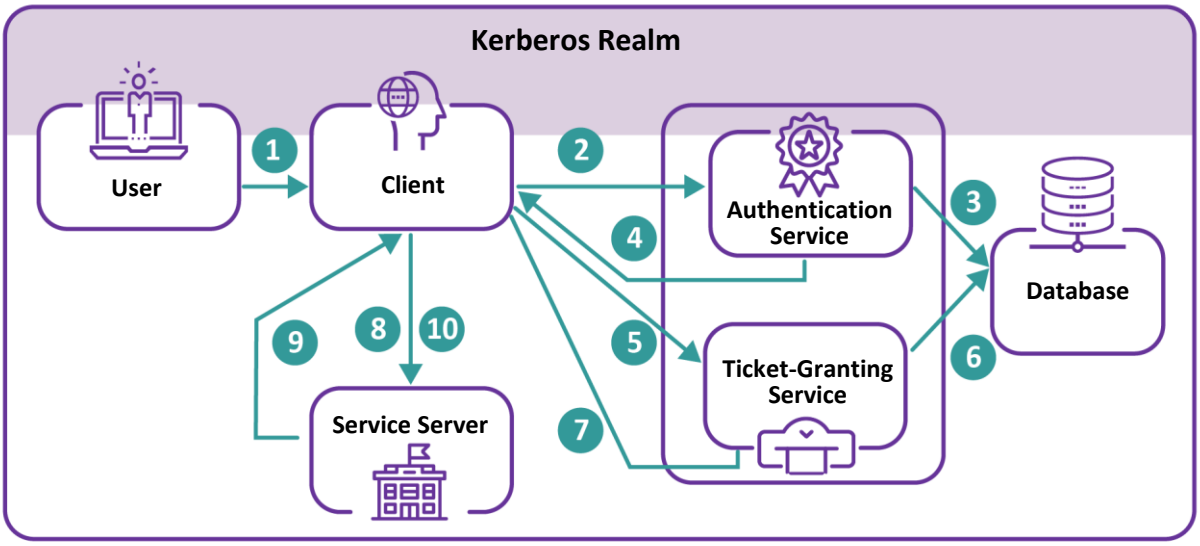
11. Best Choice of Algorithm to Use
12. Order or Sequence of what needs to be Upgraded
13. Path To Inline Quantum Remediation
14. Alternate Paths to Quantum Remediation (e.g., upgrade of entire system, change in paradigm)

ANNEX D: SAMPLE USE CASE #1 – USING KERBEROS FOR AUTHENTICATION

Section 1: Use Case Description

Kerberos is an authentication protocol on computer networks that allows clients to access services from providers. It does so by leveraging a Ticket-Granting Service (TGS) from a Key Distribution Centre (KDC) which will provide tickets to the service requestor to give to the service provider for access. It is often used as a main ingredient in Single-Sign-On (SSO) functionality.

A generic diagram of the network architecture in which Kerberos is used is given here.



1) User enters credentials (username + password).
2) Send KRB_AS_REQ.
3) Lookup user (and password) in database.
4) Send KRB_AS_RSP.
5) Send KRB_TGS_REQ.
6) Lookup service (and password) in database.
7) Send KRB_TGS_RSP.
8) Send KRB_AP_REQ.
9) Send KRB_SP_RSP.
10) Send service request to Service Server.

It should be mentioned that the initial contact and authorization of the client may occur over an insecure channel and, therefore, require some protection such as TLS. This channel is outside the scope of this use case.

Section 2: Business Value

Kerberos is mainly used to grant users and machines access to different services. It is often a critical ingredient in SSO implementations. Kerberos is also one of the basis elements of Microsoft Active Directory (AD).

Section 3: Potential Business Data in Scope/Volume/Lifespan

The data used by Kerberos is often limited to user and/or machine access data or data regarding the service being accessed. This would include userIDs and passwords, IP addresses, and potentially other limited-use and transitional information. Most of the information is of limited use and there is a limited time it would be available.

The data that is available to be accessed due to compromise of Kerberos would be unlimited as it theoretically can be used to access any service. However, this would be within the scope of the service being accessed and not directly tied to the Kerberos implementation.

Section 4: Use Case Class

Identity Management and Access Control

Section 5a: Technical Considerations

The following are considerations for Kerberos with regard to implementing quantum-safe technology:

1) **Availability:** A system implementing Kerberos will often be accessed by many different users and services at the same time. There is always a Denial-of-Service (DOS) risk in any change.
2) **Compatibility:** Kerberos can be used by m any different services, each with its own coding. Any change would have to be one in a way which is compatible with the services that use it.
3) **Credential Management:** Kerberos does manage credential from users and services in order to properly authenticate them. Changes should not put these at risk.

Kerberos is often embedded into other products. Most organizations would be dependent on having their vendors make Kerberos be quantum-safe. However, individual organizations would need to track and test in order to ensure that any changes would not be disruptive.

Section 5b: Threat Considerations

Kerberos implementations often serve as the central access point for user interaction to services within an organization. Compromise of the Kerberos system can range from a limited one-time service access to complete, catastrophic access control failure.

It would be a target both for malicious insiders as well as external attackers.

There exist current classical attacks on Kerberos (e.g., pass-the-hash).

Section 6: Types of Cryptography

Kerberos is traditionally based on symmetric key cryptography and so is not especially vulnerable to quantum. However, there do exist extensions where asymmetric cryptography is used for initial authentication (e.g., IETF RFC 4556, RFC 8062 and RFC 8636).

There are two instances where asymmetric cryptography can be used in Kerberos:

1) **User Authentication:** Classical Kerberos will verify users through traditional access control methods such as a userID and password. However, the public key extension for Kerberos allows a user to send a client certificate which can be verified by a trusted CA.
2) **Session Key Agreement:** Classical Kerberos will use user information (e.g. password) to compute a session key between the client and Key Distribution Centre for encryption purposes. The public key extension allows asymmetric key agreement such as Diffie-Hellman.

Section 7: Technical Components

The main technical components of Kerberos are:

1) **Client (Service Requestor):** the user or machine that is requesting the service.
2) **Service Provider:** the service that is being accessed.
3) **Client Authenticator:** The entity responsible for authenticating the client. This is often embedded within the KDC.
4) **Ticket-Granting Service (TGS):** The service which will grant a ticket to the client which will allow it to access the service. This is often a part of the KDC.
5) **Certificate Authority (CA):** This optional for the extensions which rely upon a CA to verify client certificates.

Domain controllers are an example of a KDC as they often implement the Kerberos protocol.

The network over which communication will take place can also be considered to be a component. However, as Kerberos is not a network protocol, this is considered out of the scope of this use case.

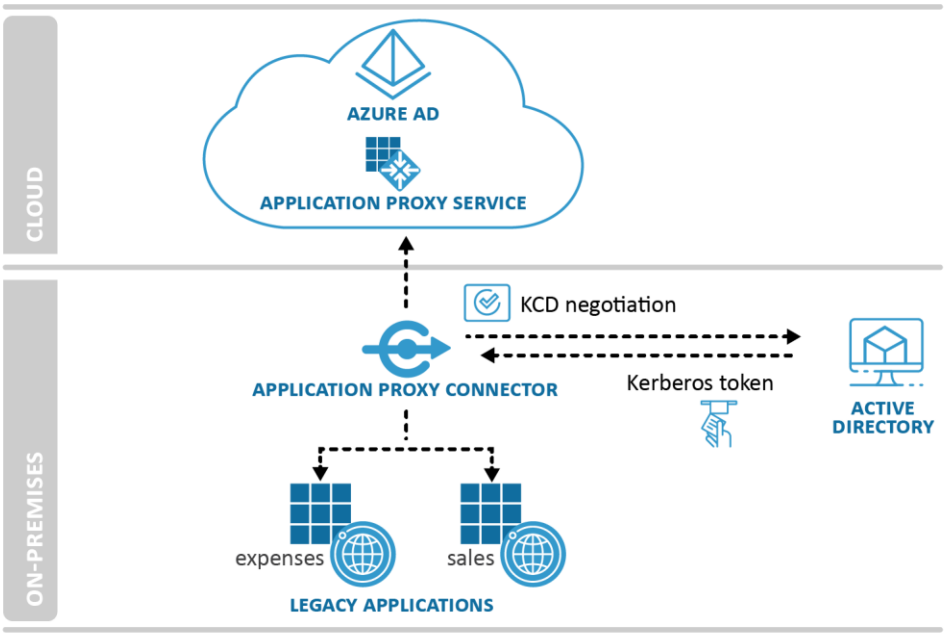
The Client Authenticator and TGS form the heart of the Kerberos system, often within the KDC. The client and Service Provider are separate systems which must be compatible with Kerberos KDC in order to function properly.

Section 8: Crypto Locations

A Kerberos implementation (i.e., the KDC) is usually a centralized system with its own cryptographic code and/or libraries. Its exact location would be product-specific. It must also be able to access a proper CA to verify a client certificate when used for initial authentication extension.

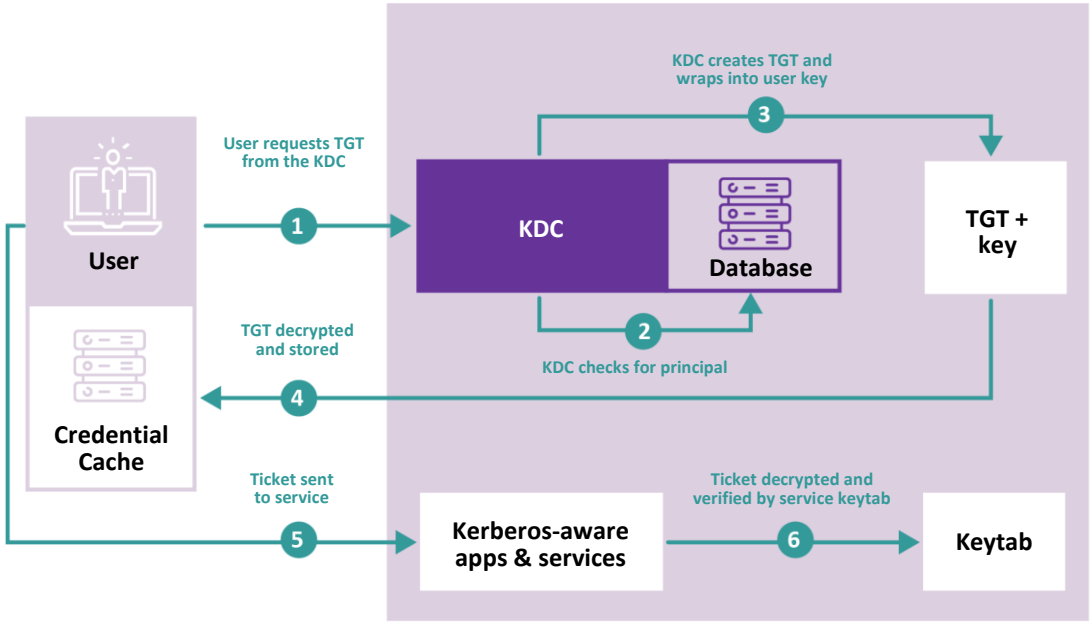
Note that asymmetric keys used within the KDC are ephemeral and so do not need to be stored for any length of time. Client certificates are used only for initial authentication and can then be discarded whereas the asymmetric keys used for key agreement can be discarded once the symmetric key is established.

The client and service provider would have their own method and location of cryptography. This, again, would be very implementation-dependent. The client would need to store the private key for its certificate. However, the asymmetric keys needed for key agreement would be ephemeral and would not need to be stored.



The most popular implementation of Kerberos is within Microsoft Active Directory (AD). An example in Azure AD is diagramed above.

Kerberos is also implemented by Red Hat. The following diagram shows its structure.



Section 9: Dependencies

The dependent use cases for Kerberos are:

- Data Storage – for client private keys (if certificates were used to establish authenticity of public keys)
- PKI/CA – (if certificates were used to establish authenticity of client public keys)
- TLS – to protect the initial client authentication.

Section 10: Ability to Support Algorithms Simultaneously

The main entity which would be required to support algorithms simultaneously would be the KDC. It would need to simultaneously authenticate quantum-safe and non-quantum-safe client public key authentication requests.

If the KDC can support both simultaneously, then it would make sense that it would be upgraded first. The client and service provider would need to support whichever version of the protocol the KDC has implemented. Hence, these can gradually be upgraded at their own pace after the KDC. These upgrades would be independent of each other.

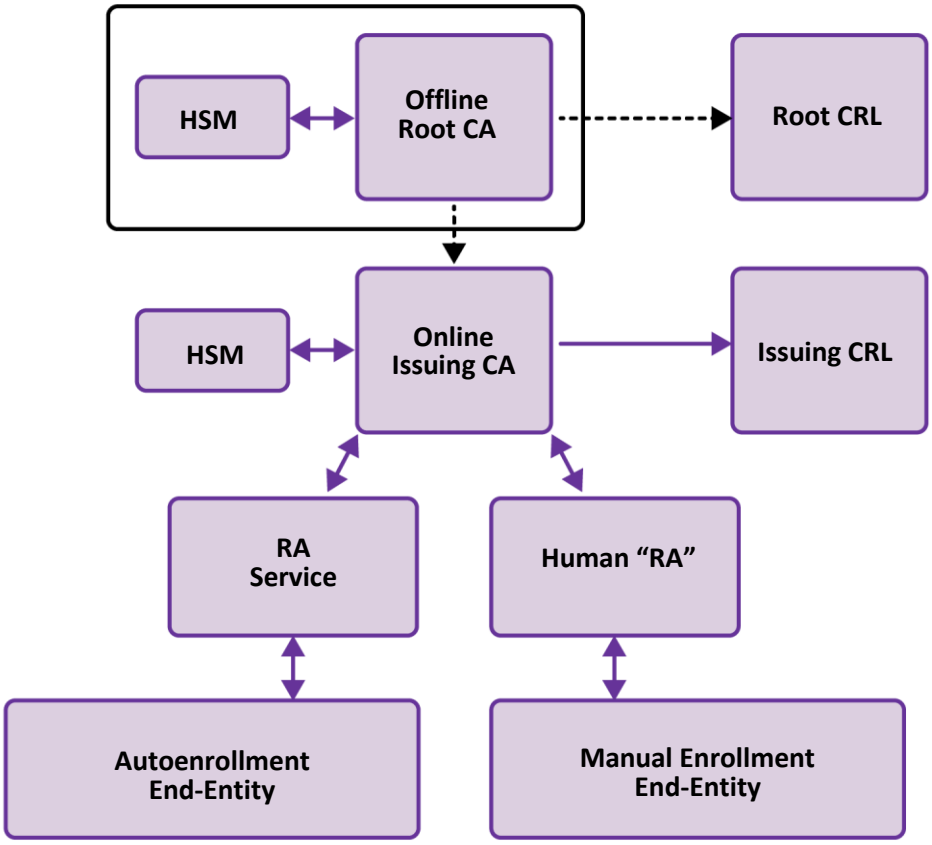
ANNEX E: SAMPLE USE CASE #2 – PKI/CAs

Section 1: Use Case Description

The purpose of a Public-Key Infrastructure (PKI) is to provide the technology and processes to leverage certificates for various other use cases such as TLS, sFTP, IPSec, and many others.

This is accomplished through the use of a Certificate Authority (CA) which has the ability to issue certificates which relying parties can use to authenticate individual entities. The certificates leverage public-key cryptography for authentication which makes it inherently susceptible to quantum computing.

A Certificate Authority will typically have a hierarchy such as shown in the diagram below:



CAs may have more or fewer levels, but they have the same basic structure.

In terms of scope, this use case will cover only the CA structure itself. It will not cover the use of certificates in such protocols as TLS and sFTP as those will be covered in their own separate use cases.

The CA/PKI use case will be separated into several sub-use-cases:

1. Public CAs – CAs which issue publicly or universally trusted certificates (e.g., Entrust, DigiCert)
2. On-Premises Internal CAs – CAs established within and managed by an internal organization (e.g., Microsoft PKI, KeyFactor)
3. Managed Internal CAs – CAs which are trusted only by an internal organization but managed by an external entity
4. Special Purpose CAs – CAs which are typically application specific within a well-defined domain (e.g., IoT CAs for mobile devices)
5. Inspection CAs – CAs which are used to intercept traffic in a Man-In-The-Middle scenario and inspect content (e.g., web content filtering and TLS inspection)

While similar each have their own characteristics which will be called out where different.

Section 2: Business Value

PKIs are typically classified as technology infrastructure. Its business value lies in its position as a key element in the operational security of critical operations. Thus, it would essentially inherit the business value of whatever application would depend upon it. As most applications which make use of a network require some level of security, PKIs are ubiquitous within most high- and low-value applications.

Section 3: Potential Business Data in Scope/Volume/Lifespan

While PKIs are involved in the protection of business data, they do not typically directly protect business data. This is often left to end-entity certificates within use cases such as TLS, sFTP, etc. This would be out of scope for this use case.

Furthermore, CA certificates are typically used for signing, not encryption or key agreement. Hence, there is no harvest-and-decrypt risk for CA certificates.

The only data present within a PKI would be infrastructure data such as Fully Qualified Domain Names (FQDNs) or routing information. With the advent of Certificate Transparency (CT), much of this information is now publicly available. Hence, it is most important to protect this information from an integrity and authenticity perspective.

Section 4: Use Case Class

Entity Authentication for Critical Infrastructure

Section 5a: Technical Considerations

The following are considerations for PKI with regard to implementing quantum-safe technology:

1) **Certificate Size:** Applications may have limitations on size such as through-the-device or channel constraints or hard-coding of buffer sizes.
2) **Signing Performance:** Some applications require a high throughput CA for large volume or high-speed signing capabilities. The Inspection CAs are a good example as they must create new certificates on-the-fly with little to no noticeable impact to user browsing.
3) **Verification Performance:** Some applications such as IoT or high-volume servers may have restrictions on verification performance as devices may be constrained or deal with large amounts of verifications.

Note that technical considerations of CA chain verification for applications is not in scope as it would be covered in the use cases using the certificates.

Section 5b: Threat Considerations

The CA is often the central root of trust for a large number of systems. Compromise of a CA private key could lead to a large amount of fraudulent certificates and connections and, hence, unauthorized transactions. The potential fraud is directly attributable to the capabilities of the applications leveraging these certificates.

The following would be further considerations for each separate use case:

1) Public CAs are universally accepted, so compromise could be catastrophic and worldwide.
2) On-premises CAs would have affects typically only for the organization. As it is hosted internally, it would likely require access to the organization's internal network to determine the CA certificates and to conduct malicious activity.
3) Managed CAs would be similar to on-premises CAs in that access to the organization is required to conduct fraud. There is an additional threat vector in that compromise of an managed CA provider could compromise many different organizations.
4) Special purpose CAs would be specific to the application they are dedicated to. One of the threat considerations would be discovering these CAs. Quite often, these CAs are embedded within products and agnostic to users and administrators.
5) Inspection CAs would be similar to on-premises CAs except that compromise would likely be limited to browser-based applications accessed by internal users.

Section 6: Types of Cryptography

The cryptography is asymmetric mainly used in:

1) Signing of CA intermediate certificates.
2) Signing of end-entity certificates

3) Signing of Certificate Revocation Lists (CRLs)
4) Authentication of Registration Authority credentials

Note that root certificates are self-signed. However, the signing is often of little value as applications will accept a root if it simply exists within its root store.

The certificates also make use of a hash function within signing and for thumbprint purposes.

The PKI will also make use of random number generation in order to generate public/private key pairs and produce signatures.

Section 7: Technical Components

The technical components in implementing the CA depends on the type of CA being implemented. Several types of CAs are listed here:

A) Root CA
Root CAs are typically held offline and is only used for signing intermediate CAs and the corresponding root CRLs. The components typically consist of:
- Offline Hardware Security Module (HSM) and related peripherals
- Offline machine to facilitate signing (e.g. laptop, desktop, some sort of device)
- Software to facilitate CA functions
- Offline secure storage device to store private key information

B) Intermediate CAs (Networked)
The intermediate CAs are typically used for issuing certificates
- Online networked HSM and related peripherals
- Online server, virtual machine, or equivalent
- Software to facilitate issuing CA functions such as:
  - Certificate Signing Request (CSR) validation and signing
  - OCSP or equivalent compatibility
  - CRL generation and signing
  - RA credential verification
  - Public/private key pair generation (for some use cases where the CA generates and end entity's certificate)
- Online accessible file lookup for CRL
- Access control functionality
- Backup systems to store log and data

C) RAs (either manual or automated)
RAs would need the technical capability to accept certificate requests and perform verification of the request and validation of the entity. This would typically consist of:
- A machine (e.g. laptop, server) to run the RA software
- A portal or Access Control List (ACL) to provide information to validate
- RA credentials (usually an RA certificate)

D) Inspection CAs
Inspection CAs would usually be embedded within an appliance of some sort and have their own protection capabilities for the private key such as an onboard crypt card.

E) Special Purpose CAs
The components of a special purpose CA would be dependent upon the type of application it is used for. For example, such a CA to handle registration of surveillance cameras would have very different components than one for conferencing software. However, there would be at minimum:

- A machine to handle registration, signing, and issuance of the special purpose certificates.

F) End Entities
While end entities are generally out of the scope of this use case, we will include specifically the end entity function of generating a CSR and installing a certificate. In order to do so, the end entity components would be:

- The end entity itself
- The software used to generate the CSR and install the certificate.
- The storage location of the private key as well as any related protection mechanisms.

Section 8: Crypto Locations

1) Root and Intermediate CAs
The primary location of the cryptography in play would be within the HSMs. This would be heavily dependent upon the type of HSM and manufacturer. There may be some residual crypto functionality from the software which is meant to facilitate CA functionality or to perform OCSP signing and RA credential verification.

2) RAs
For RAs, this would likely be the software which facilitates RA login.

3) Inspection CAs
Inspection CAs would mostly rely on the crypto card that they use for certificate generation as well as the corresponding software. This is usually packaged together within an appliance.

4) Special Purpose CAs
This would be completely dependent upon the implementation and would be vendor-specific.

5) End Entities
This would be embedded within the CSR generation software on the entity such as OpenSSL.

For the majority of the use cases, there is typically no CA cryptography outside of the HSM. Crypto for the HSMs is handled in the HSM use case.

When a software-only implementation is used, the private keys are typically stored locally on the machine which is performing the signing. The code is embedded in the software product that is being used.

In terms of generating private keys and CSRs, one standard implementation is OpenSSL's req command-line utility. The requisite code is within the OpenSSL binaries and the keys and CSRs are output to a file specified in the command line.

Section 9: Dependencies

The following use cases are dependencies for this one:

- Data Storage
- HSMs

In addition, certain considerations from other use cases may need to be taken into account from other use cases for which this use case is a dependency in order to ensure compatibility.

Section 10: Ability to Support Algorithms Simultaneously

Proposals exist for combining quantum-safe technology with existing methods to support both as a hybrid as listed here:

- draft-ietf-lamps-cmp-algorithms-15 - Certificate Management Protocol (CMP) Algorithms
- draft-ounsworth-pq-composite-sigs-09 - Composite Keys and Signatures For Use In Internet PKI (ietf.org)

Thus the remaining work would be in getting the CA and end-entity components to implement them. The HSMs and all CA software must be able to support this. Applications would need to support as well.

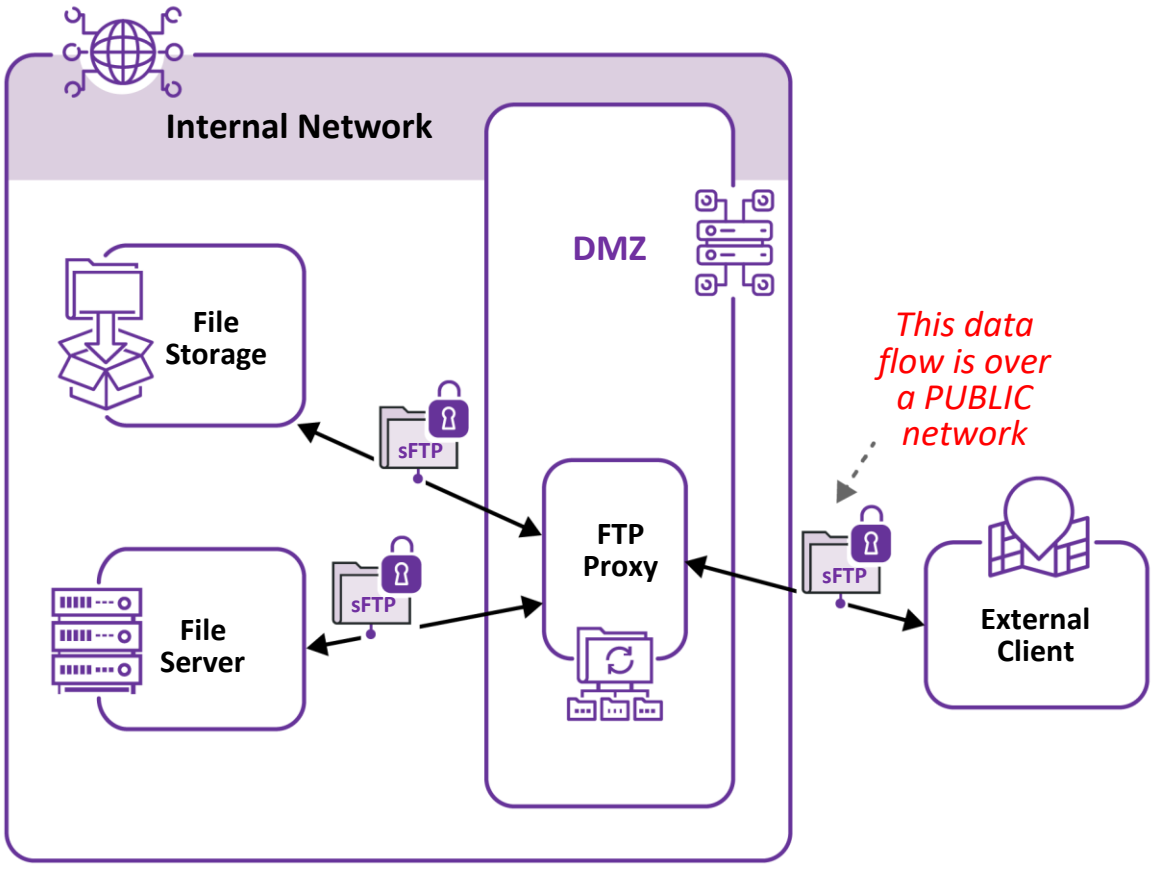
ANNEX F: SAMPLE USE CASE #3 – sFTP

Section 1: Use Case Description

sFTP, the Secure File Transfer Protocol (not to be confused with the Simple File Transfer Protocol) is a network protocol that leverages SSH authentication to securely transmit and manage files between two endpoints.

The SSH protocol is actually its own use case and so will not be considered in generality. However, for scoping purposes, as sFTP is widely used and has high business value, this use case will consider the use of SSH as bound to sFTP protocol and so will be considered one and the same. A separate SSH use case will be created for non-sFTP uses.

A generic diagram of the network architecture in which sFTP is used is given here.



Section 2: Business Value

Many organizations use sFTP servers to exchange files and other critical business documents with their trading partners. It is typically not used for low-latency transactional systems and is

more apt for batch or bulk file transfers. Since these types of file transfers are ubiquitous in the technical implementation of business systems, sFTP could have a place within any business system.

Section 3: Potential Business Data in Scope/Volume/Lifespan

sFTP can be used to transfer any type of data as long as it is in file format. Hence, there is essentially no limit to the value of the data which is transferred. The data itself will be largely dependent on the intended business use of the application leveraging sFTP.

Section 4: Use Case Class

Data-In-Transit Protection – (files)

Section 5a: Technical Considerations

The following are considerations for PKI with regard to implementing quantum-safe technology:

1) **File Size:** sFTP can be used to transfer files of arbitrary size. The only limit could very well be the technical limit of the underlying hardware and software using sFTP.
2) **Throughput:** sFTP is not typically used for low-latency transactional applications, so real-time throughput is NOT typically a consideration. However, some business applications depend on sFTP to transmit large amounts of data within a restricted time window. Throughput becomes a consideration in this sense.
3) **Credential Management:** The underlying protocol enabling sFTP authentication (usually through SSH) requires credentials such as private keys to be properly and securely stored on the endpoints facilitating the sFTP connection.
4) **Support of Underlying Technology:** The endpoints facilitating the sFTP connection need to have the proper capabilities (e.g. OS, network connections, cryptographic software) to implement the sFTP connection.

Section 5b: Threat Considerations

sFTP servers have become a primary target for hackers, putting sFTP servers at risk of a costly data breach. (https://www.goanywhere.com/blog/2018/01/23/10-essential-tips-for-securing-ftp-and-sftp-servers).

The exact threats to sFTP depend upon the security environment in which it is used. For example, sFTP connections which are external over a public network are inherently more vulnerable to attack than those that are internal to an organization. Additional controls such as logging and monitoring can affect the overall threat level.

As sFTP uses asymmetric cryptography for authentication and key agreement, there is a both an inherent quantum threat to compromise the connection as well as a "Harvest-and-Decrypt" risk for the business data that is being transmitted.

Section 6: Types of Cryptography

sFTP mainly uses both symmetric and symmetric cryptography for protection of the file data which is being transmitted.

The asymmetric cryptography is used by the underlying SSH protocol to establish authentication and key agreement between the two endpoints. The files are then protected with symmetric cryptography during transmission.

Section 7: Technical Components

The main technical components are:

1) The Endpoints: the two endpoints engaged in the active session and their underlying technology.
2) The Network: the network over which the transmission occurs.

Note that the network may have several hops in between the connection endpoints. However, for the purpose of this use case, they are transparent passthroughs and so need not be given consideration.

The endpoints must:

3) Have the requisite capabilities to support the sFTP software including the requisite cryptographic functions.
4) Have the requisite capabilities to support the underlying authentication software (SSH).
5) Have the ability to store or otherwise send or receive the files being transmitted.
6) Have the ability to store and manage the credentials of the underlying authentication software (e.g. private keys).
7) Have access to the appropriate network over which the communication is to occur.

The network must be able to support the authentication protocol as well as the transfer of files.

Section 8: Crypto Locations

The sFTP protocol will either leverage its own cryptography as part of its own software when it was installed or will leverage the underlying cryptographic libraries of the machine on which it is used.

Any change to the cryptography used in the sFTP protocol amounts to a change in the cryptographic code in one of these locations. It is important to note that any such changes have some additional considerations:

1) The location of any cryptographic keys should be taken into consideration.
2) The surrounding protocols must be ensured to be compatible with any change in buffer size, throughput or protocol steps.

Please note that some sFTP implementations may either be bundled together with SSH or be modularly separated. In these situations, the cryptography and cryptographic locations of the two protocols may need to considered in tandem instead of separately. When considering changes to the cryptography of an implementation, whether or not the sFTP and SSH implementations are bound together or not should be taken into consideration.

Many popular sFTP products operate similarly in terms of cryptographic locations. The cryptographic code is embedded within the source code and binaries of the product. The private keys or certificates are typically stored locally and exist in .pem or .ppk files.

Section 9: Dependencies

The dependent use cases for sFTP are:

- Data Storage
- PKI/CA – (if certificates were used to establish authenticity of public keys)

Additionally, one would normally consider SSH as a dependent use case, but we have bound it together with sFTP for the purpose of this use case.

Section 10: Ability to Support Algorithms Simultaneously

By its nature, an sFTP endpoint would establish an individual sFTP connection with any number of other endpoints. Each connection would use fixed, established cryptographic algorithms for the lifespan of that connection. However, the connections between different endpoints would be theoretically independent of each other. Hence, any sFTP endpoint could theoretically implement different cryptographic algorithms for different connections. Thus, any migration to new algorithms can be done connection by connection when the other endpoint is ready.

The ability to support different algorithms simultaneously, therefore, depends on whether the particular sFTP product has been programmed to support this functionality. It would be beneficial to encourage sFTP providers to enable this functionality.

ANNEX G: MATRIX OF CRYPTOGRAPHY USE CASES

Annexes D, E and F of this document contain detailed multi-page write-ups of three different organizational uses of cryptography:

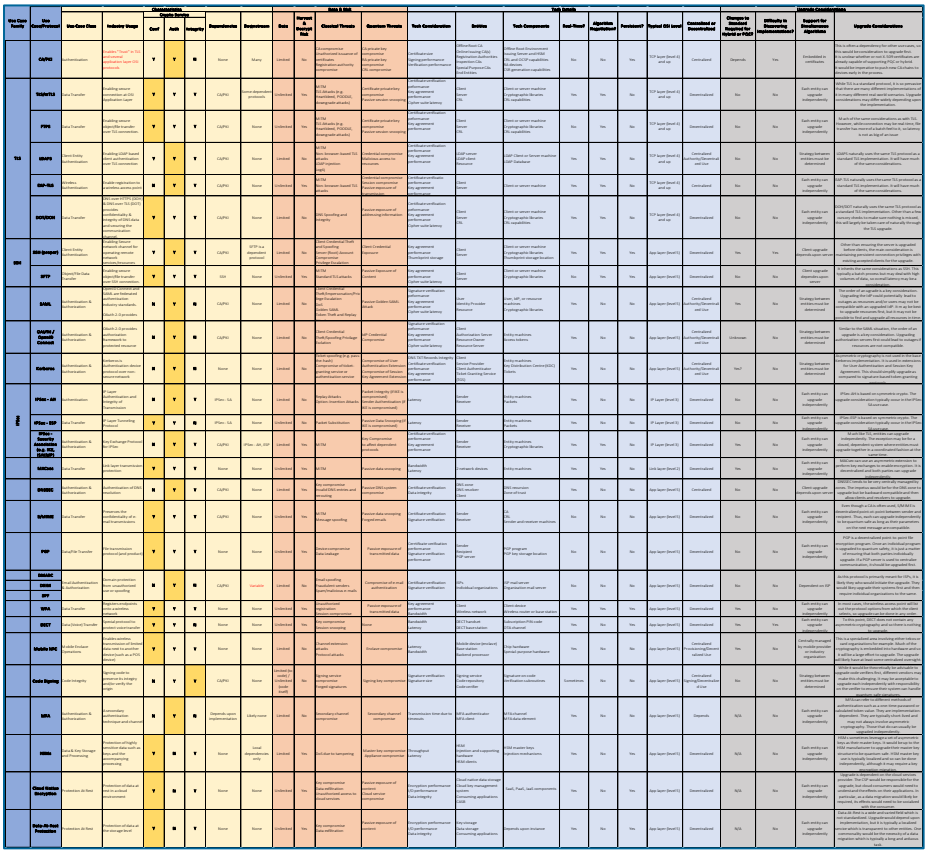
- Using Kerberos for Authentication
- Public Key Infrastructure & Certificate Authorities
- Secure File Transfer Protocols

This Annex is meant to give a more streamlined, referential view of the different factors which are of relevance to quantum-safe migration for the use cases listed in Annex B. Its main purpose is to display relevant use case considerations in a single pane of glass in order to serve as a starting point for planning a migration and/or transition to Quantum-Safe Cryptography (QSC). It has the potential to be used as both a point of reference for individual organizations in understanding the factors and potential consequences in planning a quantum migration as well as a basis for future workgroup activities in expanding guidance for the industry-at-large.

All of the information about the above use-cases can be summarized in a tabular format, in three of the twenty-nine rows of information within the matrix shown here (viz., rows 11, 7 and 8).

The other rows in this matrix are intended to provide planners with a starting point to discover how and where cryptography is used in the other use cases listed in Annex B.

A full-sized copy of this matrix may be obtained by emailing the CFDIR Secretariat.



Term used in the Matrix	Definition of the Term
Use Case Family	The overarching family in which the use case belongs (where applicable). For example, TLS (1-way) and mTLS are both TLS protocols while FTPS and LDAPS both leverage the TLS protocol as part of a more extensive protocol.
Use Case Protocol	The actual use case.
Use Case Class	The main purpose of the protocol.
Industry Usage	A short description of what the protocol is typically used for.
Conf (Confidentiality)	"Yes/No" if the protocol provides confidentiality for the data involved. This is highlighted if it is the main purpose of the protocol.
Auth (Authentication)	"Yes/No" if the protocol provides authentication for one of the participants. This is highlighted if it is the main purpose of the protocol.
Integrity	"Yes/No" if the protocol provides integrity for the data involved. This is highlighted if it is the main purpose of the protocol.
Dependencies	Other use cases which would be an upstream dependency for this protocol.
Downstream	Other use cases downstream which would leverage this protocol.
Data	Usually "Limited/Unlimited". Limited if the data involved in the protocol itself is constrained. For example, SSH is Limited as it contains only simple identification and authorization information. However, SFTP is Unlimited as any type of file containing any type of data can be transmitted.
Harvest & Decrypt Risk	"Yes/No" if there is a Harvest & Decrypt risk.
Classical Threats	Lists the well-known classical threats associated with this protocol.
Quantum Threats	Lists the new quantum threats associated with this protocol.
Tech Consideration	Lists the main tech considerations or constraints needed to be taken into account in implementing this protocol. Examples include high latency, low bandwidth, memory restrictions, etc.
Entities	Lists the entities that are typically involved in the protocol.
Tech Components	List the main technical components of the protocol.
Real-Time?	"Yes/No" depending on whether or not the protocol is used in real-time systems. For example, SAML is “Yes” as it is used for Single

Term used in the Matrix	Definition of the Term
	Sign On (SSO) which happens in real time. SFTP is N since it is often used for batch processes.
Algorithm Negotiation?	"Yes/No" depending on whether or not the cryptographic algorithms are negotiated during the protocol itself.
Persistent?	"Yes/No" depending on whether or not a previous connection or instance retains knowledge of the previous one or starts anew.
OSI Layer	The layer in the OSI computing model in which this protocol typically operates.
Centralized or Decentralized	The details of the amount of centralization of the protocol. For example, CA/PKI are usually centrally managed. TLS is decentralized as any two devices can independently form a TLS connection. SAML has centralized authority (identity provider), but its users and resource owners work decentralized.
Changes to Standard Required for Hybrid or PQC?	"Yes/No" depending on whether changes to the standard need to occur in order to enable hybrid or PQ algorithms. For example, TLS is “No” since its new cipher suites can be added without changing the basic protocol. SAML is “Yes” since it is not clear how SAML will treat hybrid or PQ algorithms, particularly when some users and relying parties are quantum-ready while others may not be.

ANNEX H: OVERVIEW OF HYBRID CRYPTOGRAPHY

This Annex contains a whitepaper on the topic of **hybrid cryptography** to introduce this emerging area of standards and technology development in the context of Post-Quantum Cryptography (PQC) considerations. This Annex was initially published in 2022, and then updated to reflect new developments and discussions (e.g., in standards development organizations) as of May 2023.

Background / Overview

As the world prepares for the upcoming quantum era, work is underway globally to prepare for its potential impact on cryptography. The advent of powerful quantum computers able to run known quantum algorithms will threaten the cryptography in use today.

This preparation work is underway among international, regional and national standards bodies, as well as the global information and communications technology (ICT) industry and community. For example, the Post-Quantum Cryptography Standardization project by the U.S. National Institute of Standards and Technology (NIST) will select and standardize post-quantum cryptography (PQC) algorithms. Not only is there a need to standardize and implement these PQC algorithms, but also to provide guidance for the transition from the current cryptographic paradigms for the current ICT protocols, tools, and processes, to a future PQC paradigm for ICT protocols, tools and processes.

Two topics related to the upcoming transition to a PQC future are **cryptographic agility** and **hybrid cryptography**. These topics are receiving attention from stakeholders including academia, standards bodies, the ICT supply chain providing cryptographic products, services, and solutions, and enterprises and governments.

While at a high level the term '**hybrid cryptography'** has been used globally, there is not yet a consensus on the best-detailed approaches related to **hybrid cryptography**.

Alternative terminology is sometimes used, such as **dual signatures**, **composite cryptography** and **multiple encryption**. The term **hybrid cryptography** might not be ideal, but so far there is not yet a consensus on a better alternative.

This objective of this paper is to provide an overview of **hybrid cryptography** to increase the reader's understanding of this complex topic. This understanding will be essential to inform and facilitate appropriate decision-making during the upcoming transition to a quantum era.

It is anticipated that updated versions of the guidance outlined in this Annex will be released in the future.

What is Hybrid Cryptography?

Hybrid cryptography, in the context of this whitepaper, is defined as the usage of a post-quantum cryptographic system combined with another public-key cryptographic system (whether post-quantum or traditional) that contributes to the same cryptographic objective. The cryptographic objectives that rely upon public-key cryptography most commonly involve the use of digital signatures or key-establishment methods.

The goal of hybrid cryptography is for the cryptographic objective to achieve the security of the strongest of all cryptographic methods used in the combination. This goal may be achieved over time depending on how hybrid is employed. For example, a hybrid digital signature might enable backwards compatibility for verifiers that do not yet support PQC, but the ultimate goal will be that all verifiers will validate the stronger PQC signature at the end of the migration. Strictly speaking, during the migration, legacy verifiers may or may not support hybrid cryptography produced by the signer during the migration, but the system does.

In the context of this whitepaper, the following are **not** considered hybrid cryptography:

- In key establishment, obtaining key contributions out-of-band, such as previously established keys, passwords, or keys from quantum key distribution devices.
- Using different public-key cryptosystems at different network protocol layers (such as the lowest physical layer and the highest application layer)
- In public-key encryption, using public-key cryptography to establish a secret key, and using symmetric cryptography to encrypt the message with the secret key. This is occasionally called “hybrid public-key encryption”, as in RFC 9180.

Why is Hybrid Cryptography important to understand?

Some threat actors may already be storing encrypted information that they have intercepted and copied, with a view to decrypting it in the future using quantum computers. Any information that needs to be protected for a long time (e.g., corporate trade secrets, classified government documents, personal health information) may already be at risk if traditional cryptography, such as ECC and RSA, is used to safeguard that information today. Both ECC and RSA are known to be at risk from quantum computer attacks. Organizations should therefore transition to using post-quantum cryptography (PQC) to protect their information. However, the transition itself has its own costs and risks to consider.

Relevant considerations include:

- Migration:

  A total transition to using PQC may take **several years or even decades**. Business requirements need to be maintained throughout the duration of this transitional state.

- Resiliency:

  Post-quantum cryptography systems are relatively new. PQC uses mature designs and has been intensively evaluated over the past five years, but it has still not been subjected to as many years of cryptanalysis as the current public-key cryptography (ECC and RSA). So, there remains a risk that a particular PQC system—or even cryptographic family of PQC systems—could be broken by some unforeseen cryptanalytic attack. However, the risk to systems that do not transition to PQC is generally considered to be greater.

Hybrid cryptography has been proposed to address both considerations.

Advantages of hybrid cryptography may include:

- Facilitating migration:
  - Testing post-quantum cryptography in real world settings before the quantum threat materializes, and before we rely entirely on post-quantum cryptography.
  - Continuing to comply with existing cryptography requirements or certifications, while also defending against quantum attacks.
  - Providing backwards compatibility with legacy applications, in the context of digital signature cryptography.
- Improving resiliency:
  - Reducing the cryptographic risk of an unknown classical or quantum attack on a single cryptographic system (or family of cryptographic systems).
  - Support defence-in-depth by providing redundant cryptographic systems.
- Compatibility:
  - Allowing parties with differing policies on required cryptography to comply with both policies by applying both required kinds of cryptography.

Applicability of Hybrid Cryptography in cryptographic systems

The quantum threat to cryptographic systems predominantly targets public-key cryptography in its two most common use cases: digital signatures and key establishment. It is in these use cases that new post-quantum cryptography is being proposed and where system owners may wish to use hybrid cryptography.

Hybrid key establishment combines keys from two or more different key-establishment methods in such a way that a weakness in any individual method will not be sufficient to expose the resulting shared key. Typically, we would measure the security of the hybrid key establishment to be at least that of the strongest key-establishment method used in the combination. In particular, combining a traditional key-establishment method (e.g. Elliptic Curve Diffie Hellman (ECDH) or RSA key transport) with a post-quantum method would result in hybrid key establishment that maintains its security against the quantum threat only if the PQC method remains strong. Therefore, resiliency use cases may require hybrid to combine multiple PQC methods to ensure security against the quantum threat.

A hybrid digital signature combines two or more digital-signature methods in such a way that validation requires verification of some or all of the signatures, based on policy. If the verifier's policy requires all the included signatures to pass verification, the resulting security of the hybrid digital signature would be considered to be equal to the strongest signature. In the case where a policy requires only a subset to be verified, the policy could be specific to which signature(s) must be verified or only specify the size of the subset to be verified. The verifier’s policy might be configurable or imposed by the signer. Hybrid digital signatures that combine a traditional digital signature (e.g., Elliptic Curve DSA or RSA) and a PQC signature with a policy that one signature must be valid may allow for backwards compatibility to assist in system migrations. In such a use case, the policy must be configurable and should specify which signature must be valid in order to achieve the migration end-state where the post-quantum algorithms must be valid.

The security of hybrid digital signatures must be carefully assessed based upon the verifier policy and the strength of the underlying signatures. For example, if a policy allows any signature and does not specify which signatures must be valid, the security of that hybrid digital signature would be considered to be equal to the weakest of the signature methods; therefore, if a traditional digital signature is included, the hybrid cryptography would not be secure against the quantum threat under that policy. It is important for system administrators to understand the policy applied by the hybrid cryptography in use.

Implementation

Hybrid is a **very complex** topic, from cryptanalysis and implementation perspectives. Thus, **additional time and effort** will be required during some phases, such as risk analysis, migration and testing, so this should be factored into the overall plans and strategy for quantum readiness.

General considerations:

- Avoid in-house development; strongly prefer a standardized method when that becomes available.

- Prefer a solution that allows for cryptographic agility. **Cryptographic agility** describes a system, architecture or state where cryptography is **planned**, **built** and **operated** to ensure that replacing an algorithm does not significantly change the functioning of the application, protocol or system. The goal is to minimize the impact of changing cryptographic functions in terms of cost, time, resources, and information security risk. Cryptographic agility can assist in the transition to using hybrid cryptography, or from hybrid cryptography if a different end state is desired. Information on how an organization can employ cryptographic agility is available from the Canadian Centre for Cyber Security in ITSAP.40.018.

If the motivation to use hybrid is to improve resiliency by reducing cryptographic risk, then one should choose the component methods in the hybrid solution to satisfy cryptographic diversity. **Cryptographic diversity** is the availability of cryptographic methods from different families which are unlikely to be vulnerable to the same cryptanalytic attack. Hybrid cryptography employing cryptographic diversity will mitigate a broader cryptographic risk. Cryptographic diversity can also be of benefit to cryptographic agility, allowing a vulnerable method to be replaced with a different cryptographic family in a timely manner. With a plan to standardize a PQC portfolio that has cryptographic diversity, NIST issued a fourth call for additional digital signature proposals in September 2022. The deadline for submissions was June 1, 2023. As a result, NIST currently has a suite of alternate PQC candidates for key establishment under consideration in Round 4 of its Post-Quantum Cryptography Standardization process. [17]

It is important to consider the availability of a proposed hybrid solution, whether and/or how a third-party vendor provides the solution, and whether the solution has intellectual property restrictions.

It is also important to assess the suitability of a hybrid solution for the desired use case. In a migration use case, the hybrid solution will combine a traditional method with a post-quantum method. In a resiliency use case, the hybrid solution should combine more than one post-

[17] NIST Announces Additional Digital Signature Candidates for the PQC Standardization Process, July 17, 2023

quantum method. Parameters to consider include processing time, memory requirements, bandwidth requirements, certification (regulations, standards), backwards compatibility, forwards compatibility, upgrade complexity, configuration complexity, management / operations. Specific protocols may require the use of hybrid cryptography, since PQC is often not a drop-in replacement for traditional cryptographic methods.

Resources, next steps, and references

Organizations requiring assistance are encouraged to contact the Canadian Centre for Cyber Security (contact@cyber.gc.ca or 1-833-CYBER-88) or the CFDIR Secretariat (cfdiroffice-bureaudufcrin@ised-isde.gc.ca).

Provided below is a list of informative references that provide more information on hybrid cryptography. However, be aware that hybrid is currently a fluid topic and these documents may not reflect the final approach standards development organizations may take. The CFDIR Quantum-Readiness Working Group will continue to update this hybrid guidance paper and its other Best-Practices and Guidelines documents during the quantum-safe transition.

Products from Government Agencies and Standards Development Organizations:

- **Cloud Security Alliance**, “Mitigating the Quantum Threat with Hybrid Cryptography”, https://cloudsecurityalliance.org/artifacts/mitigating-the-quantum-threat-with-hybrid-cryptography/, 2019-06-17.
- **ENISA**, "Post-Quantum Cryptography: Current state and quantum mitigation", https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation, May 2021.
- **ETSI** TS 103 744, "Quantum-safe Hybrid Key Exchanges", https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?wki_id=56901, 2020-12-23.
- **IETF** RFC 9370, “Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)”, https://www.rfc-editor.org/rfc/rfc9370.txt, May 2023.
- **ITU-T** X.509, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", https://www.itu.int/rec/T-REC-X.509-201910-I/en, 2019-10-14.
- **NIST,** “Post-Quantum Cryptography FAQs”, https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs#xisl, 2020-01-28.

Draft Work from Standards Development Organizations:

- Mike Ounsworth and Massimiliano Pala, "Composite Public and Private Keys For Use In Internet PKI", draft-ounsworth-pq-composite-keys-05 <https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-keys/05/>, 2023-05-29.
- Mike Ounsworth and Massimiliano Pala, "Composite Signatures For Use In Internet PKI", draft-ounsworth-pq-composite-sigs-09 <https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs/09/>, 2023-05-29.
- Douglas Stebila, Scott Fluhrer, and Shay Gueron, "Hybrid key exchange in TLS 1.3", draft-ietf-tls-hybrid-design-06 <https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/06/>, 2023-02-27.
- Alison Becker, Rebecca Guthrie and Michael J. Jenkins, “Related Certificates for Use in Multiple Authentications within a Protocol”, draft-ietf-lamps-cert-binding-for-multi-auth-00 <https://datatracker.ietf.org/doc/draft-ietf-lamps-cert-binding-for-multi-auth/00/>, 2023-02-27.
- Stavros Kousidis, Falko Strenzke and Aron Wussler, “Post-Quantum Cryptography in OpenPGP”, draft-wussler-openpgp-pqc-01 < https://datatracker.ietf.org/doc/draft-wussler-openpgp-pqc/01/>, 2023-03-25.
- Florence Driscoll, “Terminology for Post-Quantum Traditional Hybrid Schemes”, draft-ietf-pquip-pqt-hybrid-terminology-00 < https://datatracker.ietf.org/doc/draft-ietf-pquip-pqt-hybrid-terminology/00/ >, 2023-05-04.

Academic Papers:

- Nina Bindel, Britta Hale, “A Note on Hybrid Signature Schemes”, Cryptology ePrint Archive, Report 2023/423 <https://ia.cr/2023/423>, 2023 03 24
- Alexandre Augusto Giron, João Pedro Adami do Nascimento, Ricardo Custódio, and Lucas Pandolfo Perin, "Post-Quantum Hybrid KEMTLS Performance in Simulated and Real Network Environments", Cryptology ePrint Archive, Report 2022/1639 <https://ia.cr/2022/1639>, 2022 11 25.
- Mila Anastasova, Panos Kampanakis and Jake Massimo, "PQ-HPKE: Post-Quantum Hybrid Public Key Encryption", Cryptology ePrint Archive, Report 2022/414 <https://ia.cr/2022/414>, 2022-11-05.

- Jiewen Yao, Krystian Matusiewicz, and Vincent Zimmer, "Post Quantum Design in SPDM for Device Authentication and Key Establishment", Cryptology ePrint Archive, Report 2022/1049 <https://ia.cr/2022/1049>, 2022 10 04.
- Diana Ghinea, Fabian Kaczmarczyck, Jennifer Pullman, Julien Cretin, Stefan Kölbl, Rafael Misoczki, Jean-Michel Picod, Luca Invernizzi and Elie Bursztein, "Hybrid Post-Quantum Signatures in Hardware Security Keys", Cryptology ePrint Archive, Report 2022/1225 <https://ia.cr/2022/1225>, 2022 09 15.
- Sara Stadler, Vitor Sakaguti, Harjot Kaur and Anna Lena Fehlhaber, "Hybrid Signal protocol for post-quantum email encryption", Cryptology ePrint Archive: Report 2021/875 <https://ia.cr/2021/875>, 2021-06-24.
- Reza Azarderakhsh, Rami El Khatib, Brian Koziel and Brandon Langenberg, "Hardware Deployment of Hybrid PQC", Cryptology ePrint Archive: Report 2021/541 <https://ia.cr/2021/541>, 2021-05-06.
- Matthew Campagna and Adam Petcher, "Security of Hybrid Key Encapsulation", Cryptology ePrint Archive: Report 2020/1364 <https://ia.cr/2020/1364>, 2021-01-14.
- Jia Xu, Yiwen Gao and Hoonwei Lim, "Practical Quantum-Safe Stateful Hybrid Key Exchange Protocol", Cryptology ePrint Archive: Report 2020/763 <https://ia.cr/2020/763>, 2020-06-21.
- Nina Bindel, Jacqueline Brendel, Marc Fischlin, Brian Goncalves and Douglas Stebila, "Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange", Cryptology ePrint Archive: Report 2018/903 <https://ia.cr/2018/903>, 2019-10-21.
- Panos Kampanakis, Peter Panburana, Ellie Daw and Daniel Van Geest, "The Viability of Post-quantum X.509 Certificates", Cryptology ePrint Archive: Report 2018/063 <https://ia.cr/2018/063>, 2018-01-27.
- Jacqueline Brendel, Marc Fischlin and Felix Günther, "Breakdown Resilience of Key Exchange Protocols: NewHope, TLS 1.3, and Hybrids", Cryptology ePrint Archive: Report 2017/1252 <https://ia.cr/2017/1252>, 2019-09-16.

ANNEX I: CRYPTOGRAPHIC-AGILITY EXERCISE NOTES

I.1 INTRODUCTION AND EXERCISE DESCRIPTION

This Annex contains a detailed example of a systematic approach to think about "how and where to start planning" to migrate quantum-vulnerable cryptography, that may currently be used in an information technology system, to make use of standardized quantum-safe cryptography in the future. There is general consensus in the industry that making use of "cryptographic agility" may facilitate such a migration. This being said, there are many different perspectives on the precise meaning of crypto-agility, and a lack of clarity with respect to what crypto-agility means in practice for a system owner.

The approach documented in this Annex was developed during the course of fifteen meetings and greenlighting sessions by members of the CFDIR Quantum-Readiness Working Group (QRWG), spanning six months of elapsed time. The inputs and perspectives of security and cryptographic experts from sixteen different public and private sector organizations are reflected in this work.

I.1.1 Purpose

The purpose of the exercise described in this Annex is to provide an example of working through a cryptographic migration on a conceptual Information Technology (IT) system to identify and articulate the practical considerations for different use cases which the migration must consider. The belief is that thinking through a migration using a systematic approach will enable finding more of these considerations than if we were to attempt to list them.

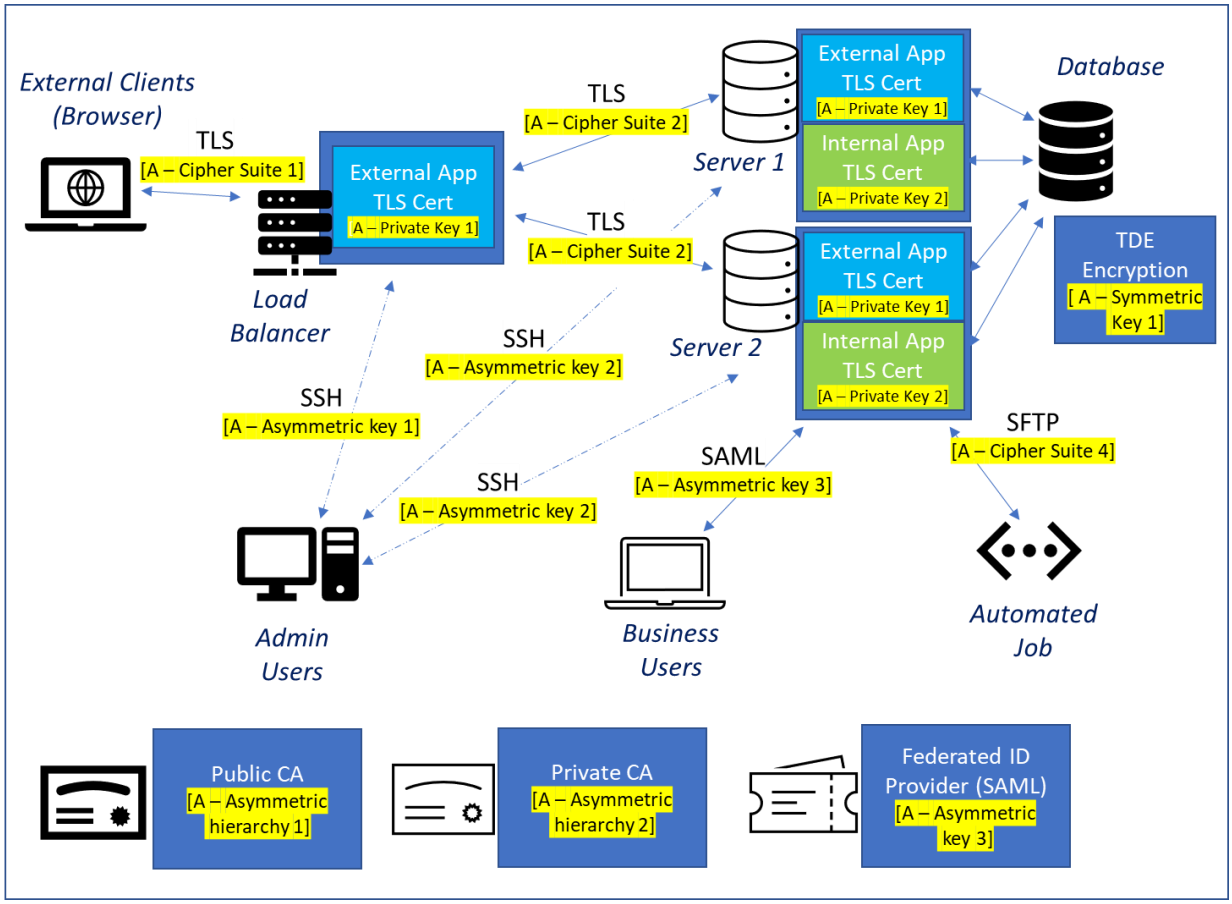
The general method is to start with the scenario:

> Your CEO comes to you and says: *"I want you to make our system quantum-safe*."
>
> **What do you do?**

For this exercise, we diagramed an arbitrary IT system that any organization may be using today to interact electronically with its customers, suppliers, and/or other parties (internal and external to the organization). This system is illustrated in Figure I-1 on the next page.

We then worked through all of the considerations we could think of which could arise in the course of migrating the cryptography needed to protect the confidentiality and integrity of data handled by each component in the system. We also considered the cryptography necessary to authenticate users, a major use of cryptography that spans many of the use cases examined. While the quantum-safe angle was the specific focus of this exercise, the same process should

be applicable to any cryptographic algorithm migration. These considerations will be key in determining what would need to be done to make a system cryptographically agile.



Notes:

1. The cryptography locations are highlighted in yellow. The goal is to change only these.
2. This is the "before" picture. An equivalent "after" picture is needed.
3. Public Certificate Authority (CA), Private CA, and Federated Identity (ID) Provider are enterprise services used by other systems.
4. The external application uses the public CA and the internal app uses the private CA.
5. The Federated ID Provider provides access for the business users to the internal app.
6. Administrative users can SSH into any box or 'appliance'.

Figure I-1. Arbitrary IT system, not currently "Crypto-agile", to be migrated to become "Quantum-Safe".

For the purpose of this exercise, we defined **crypto-agility** to be **the ability to achieve the desired cryptographic end state** (e.g., quantum-safety) **by changing ONLY the cryptographic algorithms used in a system**. With reference to the system illustrated in Figure I-1, pieces highlighted in yellow indicated a starting point for discussing elements that need to be migrated.

There are other components of the system that were identified through our systematic discussions that will need to be migrated as well. The details of the migration considerations for each identified component are captured in the text that follows.

A major goal of crypto-agility is enable to quick reactions to resist new cryptographic attacks, ideally through system configuration updates, as outlined in the following references :

- ***Guidance on becoming cryptographically agile - ITSAP.40.018***, Canadian Centre for Cybersecurity, https://www.cyber.gc.ca/en/guidance/guidance-becoming-cryptographically-agile-itsap40018, May 2022
- ***Cryptographic agility***, Wikipedia contributors, https://en.wikipedia.org/w/index.php?title=Cryptographic_agility&oldid=1077337177, (last visited June 12, 2023)
- ***Cryptographic Agility Infographic****, U.S. Department of Homeland Security, https://www.dhs.gov/publication/cryptographic-agility-infographic,* May 12, 2022

We note there are other options that could contribute to achieving quantum-safety, such as:

- Changing the architecture of a system (i.e., ***architectural agility***);
- Changing the data flows of a system (i.e., ***data agility***);
- Changing the technology within a system (i.e., ***technological agility***);
- Changing the process involved (i.e., ***process agility***);
- Changing the business requirements involved (i.e., ***business agility***).

Although these types of agility are all worthy of their own studies, this Annex concentrates on the aspects of crypto-agility as defined at the top of this page.

I.1.2 Structure of this Annex

The next section of this Annex describes thirteen different use cases. Each use case is explored in depth and based on the example system diagrammed in Figure I-1. The use cases were discussed among industry, academic, and governmental experts. Please note these use cases are by no means an exhaustive list. It is envisioned that new use cases may explored and added to future revisions of this Annex.

The notes for each of the use cases described in Section I.2 contain the following subsections:

1. **Description:** A general description of the use case with details material to this analysis.
2. **Discovery/Inventory:** Analysis on how to discover instances of this use case and/or a recommendation as to what data elements should appear in a related inventory.
3. **Migration Considerations:** The key factors to be aware of when planning a migration of cryptographic algorithms, and as preparatory elements which should a priori be in place in order to be cryptographically agile.
4. **Cutover Strategy:** Direction and analysis of what is involved in actually implementing the migration.
5. **Governance:** Elements that should be in place to assist with the overall governance of the migration, preparatory work to be cryptographically agile, and post-migration monitoring.

I.1.3 Scope of this Annex

There are certain considerations that are ever-present when dealing with crypto-agility or the considerations of a migration. These include:

- Budgeting and resourcing;
- Project management; and
- Executive and staff communication.

These considerations tend to be non-technical in nature and were not analyzed in this exercise, although it may be an interesting exercise (for future work) to determine what these considerations entail.

Note that some non-technical considerations did arise directly as part of this exercise (e.g., third-party governance) and they are explicitly mentioned where appropriate. Also, as there may be multiple transitions to different cryptographic technologies, it may be worthwhile to map out future transitions.

I.2 CRYPTO-AGILITY USE CASES AND FINDINGS

Thirteen different use cases are described in the remainder of this Annex, in the following subsections:

I.2.1: Public Certificate Authority (CA) / Public Key Infrastructure (PKI);

I.2.2: Private Certificate Authority (CA) / Public Key Infrastructure (PKI);

I.2.3: End-Entity Certificate Requirements;

I.2.4: TLS Connections to General External Client Browsers;

I.2.5: Vendor Appliances Establishing TLS Connections;

I.2.6: Internally Developed Applications;

I.2.7: Code Signing;

I.2.8: Database Encryption;

I.2.9: Centralized File Encryption;

I.2.10: Tactical File Encryption;

I.2.11: Full Disk Encryption;

I.2.12: SSH Connections for Administration;

I.2.13: SAML or Other Federated Identity.

I.2.1 Public Certificate Authority (CA) / Public Key Infrastructure (PKI)

I.2.1.1 Description

This use case will cover the crypto-agility aspects of the signing algorithm for certificates issued by a public Certificate Authority (CA) from the perspective of a subscriber. In particular, the CA will be one which has been designated by the organization as being allowed to issue certificates on domain names belonging to that organization. The actions of an individual entity during the certificate lifecycle are handled in Section I.2.3 of this Annex.

For concreteness, we will assume that there will be a simple three-level hierarchy:

- root -> intermediate -> end-entity.

I.2.1.2 Discovery/Inventory

It is important to have a list of all CAs from which the organization can obtain certificates.

For each such CA, the following should appear in an inventory:

- The different types of certificates available (e.g., Class 3 server, Class 2 client, Extended Validation);
- For each type, an inventory of the actual certificates which have been issued. For each certificate, this should include:
    - Fully Qualified Domain Names (FQDNs) and Subject Alternate Names (SANs), or other identifying information appropriate to the certificate use case;
    - Certificate Expiry;
    - Algorithm, fingerprint and/or public key;
    - Locations where the CA certificates exist.

- Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) server.

Most public CAs provide an inventory of the certificates it issues. Alternatively, there are scanning tools available that can find certificates in use on different systems within an environment. Organizations should balance their security needs with their needs for usability and availability when considering such automated tools.

I.2.1.3 Migration Considerations

Organizations are dependent on the public CA migrating their service to a new certificate signing algorithm. The following are dependencies that the public CA would be expected to address as part of the migration:

- If a new algorithm is required, establish or stand up a new root CA certificate with the new type of cryptography and make it publicly available;
- If a new algorithm is required, stand up a new intermediate CA certificate with the new cryptography; note that the intermediate CA may migrate at a different time than the root CA;
- Deploy a new Certificate Policy (CP) or Certificate Practice Statement (CPS) that describes the specifics with respect to how the cryptography works (e.g., hybrid, placing it in extensions); for example, in X.509 certificates it is common practice for new data elements to go into an X.509 extension of the certificate although this is not a requirement;
- Detail the extent to which the end-entity certificates are backward compatible (i.e., verifiable by entities expecting the older format);
- Specify any cross-signing hierarchy (e.g., the typical cross-signed hierarchy depicted in Figure I-2 on the next page);
- Update the CP/CPS to specify how the CRL or OCSP responses will be signed and provided for both root and intermediate CAs;
- Be responsible for the legitimacy of the CA via audits (e.g., Web Trust audits);
- Detail any specification the CA is doing from a requirement's perspective with respect to the subscriber Registration Authorities (RA).

With these items having been addressed, an organization preparing for a migration should do the following:

- Verification of new CA hierarchy and guidelines:
    - Understand what the new guidelines mean for the organization;
    - Understand how the cryptography (e.g., hybrid) is implemented and how it will affect general applications and clients that use those applications;
    - Communicate the implications to authorized subscribers to Certificate Authorities.

- Registration Authority:
  - Ensure that what the Registration Authority (RA) is doing, is considered in making yourself compatible with the new procedure or algorithm;
  - The RA may need to use new asymmetric key pairs according to specifications and compatibility (e.g., TLS certificates to use new algorithms). This will apply to RAs which are used for both manual and automated renewal.

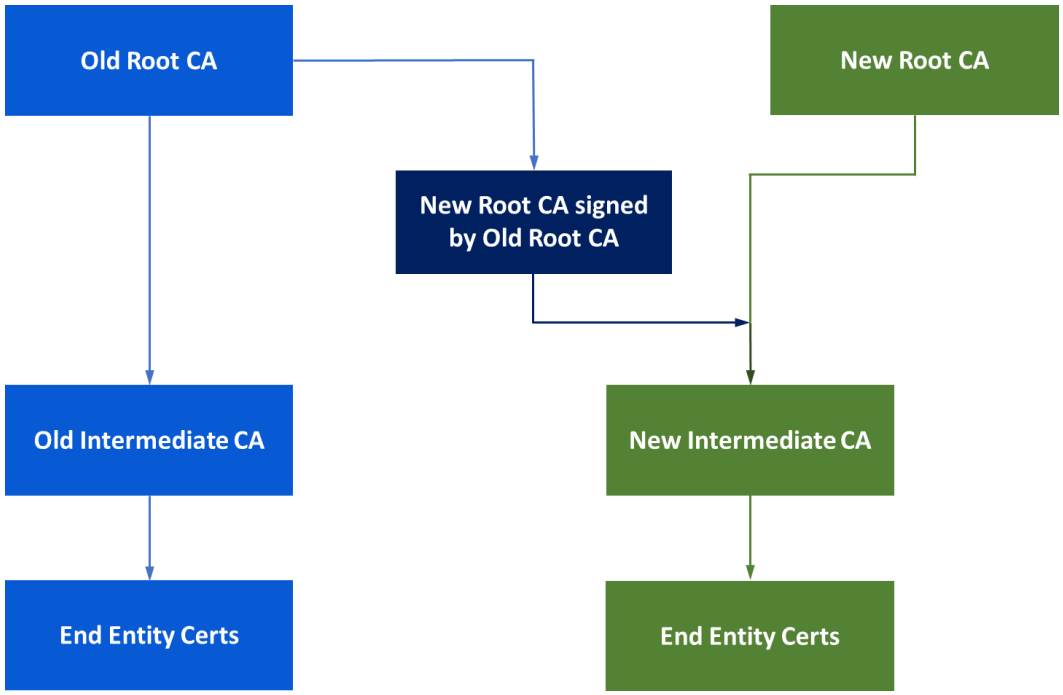


Figure I-2. Typical Cross-Signed Hierarchy

I.2.1.4 Cutover Strategy

Cutting over CAs to new cryptography has been done successfully in the recent past. Many CAs transitioned from 1024-bit RSA keys to 2048-bit RSA keys or to ECC, and then later signatures were transitioned from using SHA1 to SHA2. We suggest the following cutover strategy for organizations, modelled on those successful transitions.

- Once the new cryptographic algorithms and/or certificate profile are known, any systems that will interact with the new certificates as signers, verifiers, or servers must be updated to handle the changes; this could potentially occur through a software update, configuration change or other method;

- Once the new public CA has been stood up, a transition period and cut-off point should be established; the timelines may depend on the CA, as they may have a requirement for transitions to be completed by a certain time; these timelines may be different for the root and intermediate CAs and may be subject to CA policy or CA/B forum baseline requirements;
- During the transition period, any new certificates and certificate renewals should be done under the new CA, provided the relevant systems have been upgraded;
- Continually monitor the progress of system upgrades, to ensure that all systems will be able to transition before the cut-off:
    - Develop a plan for any systems having difficulty cutting over.
- As the transition cut-off approaches, any certificates still using the old cryptography should be renewed outside of the regular schedule; ensure that any valid certificates using the old cryptography are revoked.

I.2.1.5 Governance

The overall governance for the migration would incorporate existing certificate governance of renewal upon expiry as standard process. It would additionally include the following:

- Monitoring of systems and their certificates to keep track of which ones have migrated and which ones have not;
- Removal of old CAs from active Trust Stores when the migration has completed;
- Proper audit mechanisms to ensure compliance.

I.2.2 Private Certificate Authority (CA) / Public Key Infrastructure (PKI)

I.2.2.1 Description

This use case will cover crypto-agility aspects related to the setup and use of a private CA managed internally by an organization. A private CA is the authority for a public key infrastructure (PKI) for a specific organization or a closed network of peers, and typically issues certificates that are intended for use only by the organization or its peers to which it is assigned. The actions of an individual entity during the certificate lifecycle are described in Section I.2.3. For simplicity, we will assume that there will be a simple three-level hierarchy:

- root -> intermediate -> end-entity.

In many ways, the crypto-agility of the signing algorithm used by a private CA is similar to that of the public type. The main difference is that the organization now controls much, if not all, of the considerations involved. This is reflected in the considerations below.

There are various types of CAs which fall into the category of private, including:

- **Inspection CAs:** These are CAs which are specifically in place to intercept incoming and outgoing content for the purpose of inspection of traffic. This would include performing content filtering and malware detection. This CA is typically an intermediate CA off of an enterprise-accepted CA.
- **Special Use CAs**: Some applications require their own CA in order to function. These are often limited in scope to the devices involved with the application. Examples include special purpose hardware such as Encryption PIN Pads (EPPs) on an ATM or POS device, routers from a specific vendor, or IoT implementations such as cameras or display monitors.

I.2.2.2 Discovery/Inventory

It is important to have an inventory of the different private CAs that exist within an organization. Enterprise-wide CAs are generally well-known, but special-use CAs can sometimes be embedded and hidden from normal business operations. Discovering special use CAs may require either consulting application vendors or performing a network scan for certificates (e.g., scan ports 443, 1443, 8443 for HTTPS, other ports for TLS).

For each private CA, the inventory outlined in Section I.2.1.2 for public CAs should be followed. If the CA is internally hosted, then it would be important to also have information on the CA's operating infrastructure such as:

- Servers;
- Hardware Security Modules (HSMs);
- Network location;
- Location of CA private key including online or offline backups;
- CRL location.

For a special-use CA, it would also be important to have an inventory of devices that leverage the special-use CA.

I.2.2.3 Migration Considerations

Since this is an internal CA, it is assumed that the organization controls all aspects of its setup for crypto-agility, including the following:

- Decide on the new type of cryptographic algorithms that will be used by the CA for signing certificates and can support the organization's needs with respect to designated factors (e.g., latency, throughput, storage space, etc.);
- Decide how the new cryptographic algorithms will be realized within the CA and its certificates (e.g., certificate extension fields);
- Decide on the cryptographic algorithms to be used for the CRL signing;
- Decide on how the CA is structured (e.g., cross-signed with old root);

- Establish the infrastructure for a Root CA (e.g., HSM, offline device, cryptography card) which is compatible with the new crypto;
- Create the new root CA certificate and export for backup purposes as appropriate;
- Establish the infrastructure for an online issuing intermediate CA (e.g., server, VM, HSM, networking capabilities, etc.) which are compatible with the new cryptographic algorithms;
- Create the new intermediate CA certificate and perform any additional operations such as cross-signing;
- Make the CA certificates available to the organization and/or push them out to the requisite systems;
- Establish or modify the registration authority (RA) setup to leverage the new cryptographic algorithms;
- Ensure provisioning protocols such as SCEP or PKCS#10 are able to leverage the new certificates;
- For a special-use CA that may be specific to a particular service or hardware, ensure that the devices leveraging this CA are compatible with the new hierarchy; this may require an upgrade to a different generation of device.

I.2.2.4 Cutover Strategy

Once established, the new CA would need a cutover strategy similar to that of the Public CA.

- Develop and manage a cutover strategy for moving from the old CA to the new CA:
  - Establish a cut-off point for a defined transition period;
  - Establish and communicate organizational guidelines for cutover;
  - Establish oversight for removal of old CAs.

An inspection CA would be similar to that of a standard private CA, with the exception that it is likely dependent upon the private CA from which it was signed. It can be treated as another intermediate issuing CA of the private CA.

Special-use CAs are vendor dependent. It would be up to the vendor to determine or recommend a cutover strategy. It could either be gradual or all at once, depending on the options provided by the vendor and the characteristics of the business use case.

I.2.2.5 Governance

Governance for this use case would be similar to that of the public CA/PKI. For special-use CAs, there would need to be an additional level of governance to track the different implementations and assessing each one's ability to migrate. Note that audit requirements here would be internal unless a specific use requires external oversight.

I.2.3 End-Entity Certificate Requirements

I.2.3.1 Description

This use case will cover crypto-agility in the use of certificates throughout their lifecycle from an end entity perspective. This would include Certificate Signing Request (CSR) generation and certificate loading as well as revocation, and distribution, but not be tied to a protocol such as TLS.

Many organizations leverage a Content Delivery Network (CDN) (e.g., Akamai, AWS CloudFront) to filter the content that enters their systems. These often leverage certificates to assist with facilitation of services. From the perspective of this document, they will simply be considered as an end-entity requiring a certificate.

I.2.3.2 Discovery/Inventory

Having an inventory of end-entity certificates should be a requirement. Any inventory should include:

- Certificate details (e.g., common and subject alternate names, expiry date, etc.);
- CA it was obtained from;
- Locations where this certificate is used (i.e., where private key exists);
- Owner or accountable officer of certificate or appliance(s) on which it exists;
- Whether or not this certificate is associated to a CDN.

I.2.3.3 Migration Considerations

- CSR Generation:
    - The appliance on which the certificate will reside must have access to a tool which will create the Certificate Signing Request (CSR) that is compatible with the new CA requirements:
        - If multiple hierarchies exist with different cryptographic algorithms or specifications, the CSR generation tool(s) will need to have these capabilities/flexibility.
    - In cases where the CSR is generated on a different appliance:
        - The device that generates the CSR must have a tool compatible with the new formats and algorithms;
        - The appliance on which the certificate resides must be able to import the response to the CSR including the private key in the new format.
    - The tool used to generate the CSR must support new protection mechanisms for the file formats of the old and new CSRs and responses (e.g. .pem, .pfx):
        - It must be able to import private keys from certificates in the old format.
    - The asymmetric key pair must be generated using the new cryptography;

    - The key store for the new private key must be compatible with new format:
        - Hardware key stores must ensure the HSM vendor can support this:
        - Software key stores must leverage any new cryptographic algorithms for key store protection and be able to import private keys and certificates for the new cryptographic algorithms.
- Certificate Distribution and Loading:
    - If the CSR was created on a different device, the distribution method used to move private keys must be compatible with any new private-key format;
    - The mechanism used for distribution of the certificate must be compatible with the new certificate:
        - This may be a manual process or it may be an automated process.
    - The receiving device must be able to load the new hierarchy into its trusted store. Depending on the type of device this may mean a cross-signed hierarchy;
    - The receiving device must be able to properly load the certificate;
    - The receiving device must be able to verify the appropriate Certificate Revocation List (CRL) with its new signature;
    - At an appropriate time, the device must be able to remove the old hierarchy and/or switch away from cross-signed hierarchy.

I.2.3.4 Cutover Strategy

Most of the work in a cutover is on the part of the CA. The end-entity can cutover whenever it sees fit if it is in the window given by the CA. The key points an end-entity must take into account when cutting over are:

- Ensuring that it can support the new cryptography;
- Ensuring that the entities that consume its certificate can support the new cryptography.

I.2.3.5 Governance

Overall tracking of end-entity readiness to migrate is usually handled by the operational entities of the organization. Each end-entity needs to take it upon itself to ensure that cutover will be successful.

I.2.4 TLS Connections to General External Client Browsers

I.2.4.1 Description

This use case will cover the use of certificates in a Transport Layer Security (TLS) connection to general external client browsers. This use case is discussed from the point of view of connections to the browsers. The properties of the server establishing the TLS connection are discussed in Section I.2.5.

I.2.4.2 Discovery/Inventory

An inventory of the different domains and subdomains accepting TLS connections is important.

In order to support crypto-agility and ease of migration, the main inventory item for each domain/subdomain is a list of the different browsers that are supported. This would include:

- Browser name;
- Browser version;
- Approximate number of connections for each name and version (e.g., daily average);
- Any interesting factors to note about the browser itself.

This data can be discovered through traffic monitoring or log analysis.

I.2.4.3 Migration Considerations

The browser community and/or public CAs (likely through the CA/Browser Forum) would be expected to address the following as part of the migration:

- Provide direction to external browsers to leverage the new TLS protocol and/or its new cryptography; (note: any changes to the TLS protocol itself would be managed by the Internet Engineering Task Force or equivalent standards development organization);
- Provide direction to external browsers to leverage the new certificate capabilities and CA hierarchies;
- Manage the upgrade path of most browsers in use by the public.

I.2.4.4 Cutover Strategy

The organization responsible for the server would then need to perform the following tasks:

- Extent of backward compatibility needed:
    - Understanding of how the new certificates and protocol will affect older browsers and technology;
    - Amount of external client on old browsers which will be degraded or unusable;
    - Plan to deal with handling those using old technology;
    - Determine if both old and new cryptographic algorithms can be used simultaneously.
- Anticipate and plan around any downtime;
- Establish a cut-off point for a defined transition period.

I.2.4.5 Governance

Governance requirements are very basic. Keep track of the different sites for which this applies and how well they are cutting over.

I.2.5 Vendor Appliances Establishing TLS Connections

I.2.5.1 Description

This use case will cover the end-entities that implement a TLS connection and that have been supplied by a third-party vendor. Note that whether the TLS connections are one-way or mutual is immaterial.

I.2.5.2 Discovery/Inventory

An inventory of vendor appliances implementing TLS connections should be a requirement. Any inventory should include:

- Inventory of appliances/servers/load balancers or equivalent used in this use case;
- Vendor for each of these appliances, etc.;
- Hardware, software, firmware versions.

I.2.5.3 Migration Considerations

The appliance in place must be able to perform the required functions, namely:

- Upgrade to the proper version to leverage the new cryptographic algorithms and support both old and new protocols as appropriate;
- Perform the requisite certificate provisioning and loading functionality as described in the End-Entity use case in Section I.2.3;
- Perform the TLS connection using the new cipher suites as determined in the TLS protocol (Note: any changes to the TLS protocol itself would be managed by the Internet Engineering Task Force (IETF) or equivalent standards development organization);
- Conduct proper testing of functionality.

I.2.5.4 Cutover Strategy

TLS connections are typically non-persistent, so new connections can start fresh. The following must be considered in any cutover strategy:

- Extent of backward compatibility needed (in addition to the considerations outlined in Section I.2.4.4):
    - The appliance must be able to support old and new cryptographic algorithms and old and new CA hierarchies simultaneously.

    - In the cases where the appliance can only support one root CA, it is preferable to use a cross-signed CA until all connections have been migrated.
    - Assessment of the impact of connections which will be degraded or unusable.
    - Plan to deal with connections which use old technology
        - If industry wide (i.e., outside the purview of the organization), follow plan as for external browsers
        - Otherwise, keep updated on the migration status of connections
        - Have a plan to deal with those who cannot/will not migrate
- Anticipate and plan around any downtime
- Establish a cut-off point for a defined transition period
- Remove old roots after transition
    - Move away from cross-signed hierarchy if applicable.

For non-persistent TLS connections, it is important to consider how to manage session resumption and data persistence. A proper cutover strategy would need to be formed.

I.2.5.5 Governance

There are some additional governance requirements:

- The appliance itself will often be supplied by a vendor. Processes must be in place to ensure:
    - The vendor is aware of the vulnerability/security risk
    - The vendor understands the associated risks as it applies to their product
    - The vendor has a roadmap to make their product secure against the vulnerability
    - The vendor takes all considerations from Sections I.2.5.1 to I.2.5.4 into account.

I.2.6 Internally Developed Applications

I.2.6.1 Description

This use case will cover aspects in dealing with internally developed applications. The general assumption is that whatever pipeline used to produce these applications (e.g., SDLC, DevOps, CI/CD) will not structurally change. I t is the artifacts within these pipelines which will change. Examples of artifacts include: a crypto library (openSSL) in your application, code base, application code, secrets such as an SSH key.

I.2.6.2 Discovery/Inventory

For existing applications, the following are important to list in an inventory:

- Application name and version

- Framework or platform on which it is built
- Programming language(s)
- Software Bill of Materials (SBoM)[18] in order to work with submodules
- Cryptographic Bill of Materials (CBoM)[19] or at least a list of cryptographic libraries used
- Dependencies and constraints (e.g., throughput, hardware, latency)
- Appropriate software documentation
- Any instances of hard-coded cryptographic assets
- List of authentication mechanisms in place.
- List of clients for the application (sanitized as appropriate)

Application inventories can be obtained through different activities:

- Manual list
- A general material scan
- A cryptography-specific scan of source code or binaries (e.g., using a code scanning tool such as BlackDuck, Vericode that search for vulnerabilities).

I.2.6.3 Migration Considerations

In order to prepare software development for crypto-agility, it is important to make sure the development pipeline can handle it. The following are required:

- The pipeline has access to appropriate cryptography-compatible libraries for development
- Cryptography related vaulting and data-retrieval mechanisms are compatible with the new cryptography, including:
  - Passwords, secrets, or other authentication-credential retrieval methods
  - Certificates and private keys
- Vaulting and retrieval mechanisms support new cryptographic algorithms
- There is compatibility with other tools involving cryptographic assets, such as automated certificate management
- Pipeline pieces are each separately compatible with new cryptographic algorithms where cryptography is applied

As a general rule, a consistent development or application stack to make migration (as well as many other things) much easier.

The pipeline should maintain its normal lifecycle with these changes, and should now be set up to develop new applications using new cryptography in a crypto-agile way.

[18] Software Bill of Materials (SBOM) | CISA

[19] GitHub - IBM/CBOM: Cryptography Bill of Materials

As for migrating existing applications, the following would need to be done:

- Triaging and prioritization:
  - As there will be many applications to migrate, there will need to be some sort of prioritization. This prioritization will be based on the internal requirements of the organizations, such as:
    - Risk of breach;
    - Availability risk;
    - Public accessibility;
    - Attack surface, ease of access;
    - Difficulty of upgrade;
    - Time to migrate;
    - Refresh cycle;
    - Application lifecycle;
    - Client support.
- Planning:
  - This stage is where the plan to change the actual application is developed. During planning, the following factors should be considered:
    - Understanding the requirements of the application (e.g., low-bandwidth, large amount of data processing, etc.);
    - Dependency chain of migration – migrating an application may depend on migrating the modules on which it is based first (some of which are made by vendors); this includes crypto libraries;
    - Understanding how to integrate the new code into the existing code base;
    - Understanding the extent to which the application can be made crypto-agile;
    - Understanding how the application will communicate with other applications or infrastructure;
    - Understanding how these changes will affect the system as a whole;
    - Whether or not developers have been appropriately trained to work in a crypto-agile fashion.
- Implementation:
  - Send the application back through the pipeline to get a migrated application.
- Testing:
  - Normal testing procedures should apply, including first testing in lower environments and performing regression testing.
- Deployment, Operations, and Monitoring:
  - Follow a standard deployment, operations, and monitoring cycle.

Finally, we would note that developers would need to be trained on crypto-agility. At minimum, the following should be included: [20]

- Hard-coding elements reduce agility, including:
  - Cipher suites;
  - Buffer size;
  - Paths;
  - Hostnames;
  - Passwords;
  - Secrets;
  - Configuration items;
  - Cryptography provider libraries;
  - Certificate fields;
  - So as to avoid hard-coding of cryptography, there needs to be a layer of cryptographic abstraction;
  - Use forward-leaning libraries.
- Document the developer('s) code:
  - Where the certificates are;
  - How certificates are used;
  - Which libraries are used;
  - Instances of cryptographic algorithms;
  - General standard developer documentation.
- Hardening requirements with respect to crypto-agility:
  - Get rid of old ciphers / old libraries you do not want to be used;
  - Reduce side channels;
  - Harden cryptographic implementations (i.e., have the implementations do exactly what we want them to do, such as to provide confidentiality, or integrity, and to not do anything extra).

Even with the best of training and education, elements which will prevent crypto-agility will inevitably occur in code. One of the main ways to account for these instances is to implement code scanning. In terms of crypto-agility, it is again assumed that the structure of scanning will not change. Only the content of scanning will change. This will now include scanning for:

- Cryptography implementations;
- Interoperability and backward compatibility;
- Downgrading cryptographies;
- Hard-coding of parameters or data.

[20] https://learn.microsoft.com/en-us/archive/msdn-magazine/2009/august/cryptographic-agility

In terms of what is scanned, the following should be considered:

- Source code;
- Binaries;
- Input/Output;
- Containers;
- Infrastructure;
- Code repositories;
- Pipelines.

Output from code scanning should be handled with usual process including filtering out false positives, ranking the severity of a finding, and working to remediate.

I.2.6.4 Cutover Strategy

The cutover strategy will follow the normal SDLC, CI/CD, DevSecOps processes of the organization. An organization may also need to consider the upgrade path for clients.

I.2.6.5 Governance

The standard governance mechanisms relevant to internal development of application would still apply. However, there are additional steps which would be useful in ensuring crypto-agility:

- Incorporating crypto-agility in risk management processes to determine risk related to internally developed applications;
- Leveraging new avenues through which to find issues with regards to crypto-agility such as crypto-agility-related bug bounty or red teaming;
- Developing a scale which measures the extent to which an application is made to be crypto-agile.

I.2.7 Code Signing

I.2.7.1 Description

This use case deals with the structure of code signing within an organization. The main entities involved are the Code-Signing Requestor (such as a developer), the Code-Signing Service, and the relying parties or Code-Signing Verifiers (such as the operating system of the end user). The Code-Signing Service may have a Timestamp Service as part of its service. There may be a separate CA service which provides the signing certificate. This use case is regarded on its own and separate from the development cycle as it does not relate to the development of applications, but instead its own service involving cryptography.

Code signing uses the basic model shown in Figure I-3, on the next page.

The cryptography spans from the Code-Signing Service to the Code-Signing verifier as it is usually a digital signature of some kind.

I.2.7.2 Discovery/Inventory

The inventory should list each signing service. For each code signing service, the inventory should include:

- Signing service metadata (e.g. name, vendor (if applicable), and version);
- The signing certificate and developer private key;
- The valid requestors;
- If possible, the code signing verifiers and their capability to support new cryptography and be backward compatible.

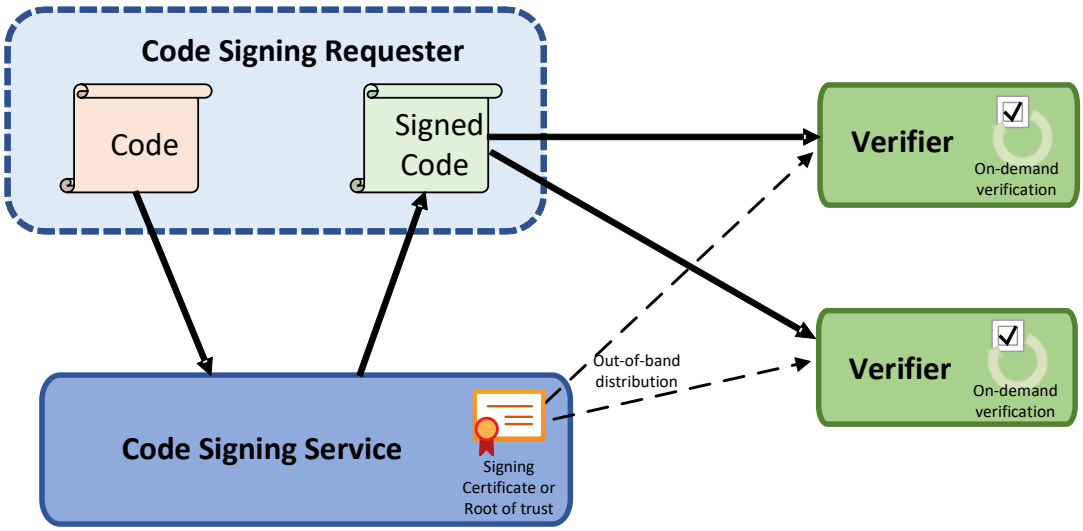


Figure I-3. Basic Code-Signing Model

I.2.7.3 Migration Considerations

Migrating to new cryptography will involve:

- Ensure that the Code Signing Service is migrated to be crypto-agile. If the service is in-house, this would include the following:
  - Choosing the new signing algorithm;
  - Defining the signature structure taking into account backward compatibility;
  - Being able to handle the new Certificate Lifecycle as described in the End-Entity Use Case (Section I.2.3).

- Migrating each separate Verifier:
  - Being able to accept the new certificate hierarchy;
  - Being able to store the new signature and parameters;
  - Being able to implement the new verification requirements.
- Assessing the verifier's ability to be backward compatible:
  - If a hybrid signature is used, it is important to note whether or not the verifier will be able to accept the new signature before it is migrated.

I.2.7.4 Cutover Strategy

If the Code Signing Service is in-house, have a cutover strategy similar to the TLS Connections with External Browser Use Case described in Section I.2.4.

The difference between these use cases is that code signing is:

- Persistent – the old code must be remembered for backup purposes during migration;
- Not real-time – the code verification occurs when new code is deployed, which could come at a later point than when it is signed.

I.2.7.5 Governance

Governance requirements are basic. Keep track of verifiers and their current state towards migration.

I.2.8 Database Encryption

I.2.8.1 Description

This use case deals with databases or other structured data environments which have been encrypted. Typically, the method of cryptography is Transparent Data Encryption (TDE) which will encrypt the entire database in totality or encrypt the columns of the database tables individually. In the latter case, the data within a column of a table may be encrypted and use different encryption from that used for the data in other columns of the same table or may not be encrypted at all.

The encryption is referred to as *transparent* since the data is encrypted as it is committed to the database and decrypted as it is accessed. The encryption is thus transparent to any application which is accessing the data. The encryption is typically symmetric and the key is held in or near the database itself.

One important assumption which we are making is that the encryption schema of the database (e.g., encryption policy) will not change. Columns that are encrypted now will continue to be encrypted. Columns that were not encrypted will continue not to be.

I.2.8.2 Discovery/Inventory

In terms of an individual database, it would be important to have the following information available:

- The database purpose;
- The database product, version, platform;
- The database schema;
- Column metadata (i.e., what each column contains);
- The type of encryption applied to each column.

I.2.8.3 Migration Considerations

The main considerations when migrating the data are as follows:

- Migrating the database product itself:
  - The database vendor would need to upgrade its product to allow the new encryption technology;
  - The vendor would need to support the new algorithms;
  - The vendor would need to state changes to considerations which its clients would need to take into account (e.g., disk space expansion, latency);
  - The vendor would need to state any effect that this would have on applications which access them; (note: as the encryption is transparent, there should be no impact theoretically, but any deviation from this should be communicated).
- For many databases, the amount of data is massive, and therefore the migration will be a monumental task; it should be noted that this is somewhat an existing problem today in terms of key rotation;
- How the change in cryptography may affect data format or size limits;
- Migration across database replication systems;
- A proper plan would need to be developed with appropriate contingencies.

I.2.8.4 Cutover Strategy

When cutting over to the new encryption, the foremost decision to be made is whether or not to adopt an all at once or take a forward-looking approach. In order to do an all at once approach, the following must occur:

- Set up an alternate database instance;
- Decide whether or not to hold off on data commits for the migration period of time or simply keep track of changes after the migration begins;
- Perform the translation of the data, taking into account any commit changes after migration starts;
- Switch to the new database at a designated point in time;

- Monitor application use and access and be ready to rollback if necessary.

The forward-looking approach will encrypt data using the new encryption as it is committed to the database. Note that this will work in cases where encryption occurs at a row level. It may not be feasible depending on the product or if complete encryption is used. The following must occur:

- Assess whether this approach is possible given the product, schema, and encryption pattern;
- Understand the performance impact, if any, in taking this approach;
- Develop a plan for existing rows which are not re-committed, including whether to do a bulk translation when their percentage drops below a certain threshold.

In all cases, it will be important to manage multiple copies of a particular database and manage how these are copied, put into service, and deleted. One also needs to consider how long to maintain legacy encryption keys for database backups.

Another important consideration is to determine the extra cost in resources for potential extra storage space needed to accommodate the new algorithms. This would include the loss of de-duplication and compression capabilities

I.2.8.5 Governance

The governance requirements would be very basic. Overall tracking of readiness for each database implementation would be needed, but each database implementation would be responsible for its own migration and ability to be crypto-agile.

I.2.9 Centralized File Encryption

I.2.9.1 Description

This use case deals with unstructured data such as file servers, Network-Attached Storage (NAS) shares, document repositories, etc., but where the encryption has been centralized. This use case does share some similarities with the structured Database Encryption use case. The encryption would be considered transparent. File encryption primarily uses symmetric encryption, but asymmetric encryption may be occasionally used.

I.2.9.2 Discovery/Inventory

An inventory in this case, would consist of:

- File or filesystem name;
- File type;
- File sensitivity label (i.e., level of confidentiality);
- Location;

- Encryption technique.

Quite often a data discovery tool can be implemented to find and determine these files (e.g, IBM Guardium, Varonis, Microsoft's MIP).

In addition, where appropriate, the key hierarchy should be included in the inventory as well.

I.2.9.3 Migration Considerations

The considerations would closely parallel those of the Database Encryption use case. In particular, the decision of all at once vs a forward-looking approach would need to be decided. A few notes to highlight are:

- The product itself must be upgraded to the new technology. This would include the key store if it is internal. The same applies if it is an external key store, although the integration between the two would need to be included in the migration.
- Due to the unstructured nature of the file server, the forward-looking approach would likely be much more feasible.
- While it could be another monumental effort, access to centralized file storage is not typically high-availability or in real-time. Thus, the migration could happen gradually.
- There are cases where the administrator dictates what is encrypted globally. But there may also be cases where the user decides which files are to be encrypted.

I.2.9.4 Cutover Strategy

If a forward-looking approach is decided upon, the centralized authority could encrypt all new files created and encrypt existing files the next time they are saved. A cleanup activity to decrypt/re-encrypt the files which have not been accessed since the migration started could occur at a later time.

If an all at once approach is used, then there may be some downtime needed while files are decrypted and re-encrypted. Note that this activity could happen in batches.

I.2.9.5 Governance

This use case depends on having an accurate inventory of files and locations. This is not always feasible with 100% accuracy. However, a data discovery and retention program may be of great use for this use case.

One major issue with this use case is the idea of crypto-shredding (defined as the deletion/destruction of an encryption key for the purpose of making data inaccessible). From a governance perspective, it is often the case that crypto-shredding is seen as a valid method of data destruction. This is useful in cases such as cloud environments where there is essentially

no control over data. However, the idea that cryptography can be broken brings this paradigm into question.

I.2.10 Tactical File Encryption

I.2.10.1 Description

This use case handles unstructured file encryption, but where the service is not centralized such as PGP, secure file zipping, or other file encryption tools. In this case, instead of a centralized key server, keys will be disparately located. It is possible that a key-escrow service is in place in this case.

I.2.10.2 Discovery/Inventory

As with the centralized case, a data discovery scan (using the same tools as described in Section I.2.9) would yield a similar inventory. The one item that is different is that the encryption key may not inherently be centralized, so there may be no determination as to where it would be, so it cannot be listed in the inventory.

If a key escrow service is used, this service would have an inventory of the keys used and the files to which they apply.

I.2.10.3 Migration Considerations

Since this use case is typically for ad hoc file encryption, the migration would be split into all of the individual instances of the encryptions. In particular, for each one,

- The appropriate encryption tool would have to be upgraded to a compatible version;
- The appropriate files would have to be migrated;
- The appropriate keys would have to be placed in an accessible location.

One of the biggest considerations is being able to find and perform all of these migrations. It is not always clear if this would be possible in a practical setting.

When key escrow is used, the following additional considerations should take place:

- The key-escrow service, including the key-recovery agent, should be upgraded;
- The keys stored by the service and their corresponding files should be migrated;
- The key lifecycle should continue to be monitored.

I.2.10.4 Cutover Strategy

Since files are individually encrypted, the migration can happen any time at the discretion of the file owner.

I.2.10.5 Governance

Governance options include:

- Shifting these instances to the Centralized File Encryption use case;
- Enforcing key escrow;
- Setting up a tracking program.

I.2.11 Full Disk Encryption

I.2.11.1 Description

This use case deals with the encryption of the storage space of a particular device. Note that this is at a lower level than that of a database or file encryption.

This could apply to individual user-level devices such as a laptop, mobile device, or Internet of Things (IoT) device. However, it could apply to larger appliances, such as servers which house databases, as it may be seen as an alternative to Database Encryption.

I.2.11.2 Discovery/Inventory

An inventory of devices is essential to this use case. It would include:

- Device name, OS, other device information;
- If appropriate, person to whom it is assigned;
- Type of encryption technology being used;
- How the encryption key is protected or regenerated.

I-2.11.3 Migration Considerations

The following considerations are involved:

- The tool used to encrypt needs to be upgraded to support the new algorithm;
- Storage-space requirements and cost would need to be taken into account;
- The compression and de-duplication issue would still be present. De-duplication refers to the removal of duplicated data streams within large data sets. Both compression and de-duplication are used to reduce data size. However, encryption of large data sets typically render compression and de-duplication ineffective;
- Strength of the encryption key protection (e.g. password strength, biometric, multi-factor);
- The availability and use requirements would need to be taken into account as they may be different.

I.2.11.4 Cutover Strategy

The method for migration would be dependent upon the type of device which is being migrated.

- Laptop or IoT devices could be made to install updates by an administrator and translation could occur as part of updates. This would be dependent upon either inventory or access edict.
- Servers could be in situation similar to Database Encryption in terms of availability and real-time requirements. The 'all at once' approach would likely be the only option.
- Data backups would be offline by nature and so could be translated offline. The keys are often held by the client, in which case the key vault would need to be upgraded and there would need to be coordination.

I.2.11.5 Governance

Governance would again be very basic. A general tracking program is a good idea, but each instance would be responsible for its own migration.

I.2.12 SSH Connections for Administration

I.2.12.1 Description

The SSH protocol allows users to remotely connect to a resource, such as a server or appliance. Users may use public key cryptography, single sign-on methods, or passwords to authenticate to the resource. Public-key-based authentication requires generating an asymmetric key pair and storing the public key on the resource. Then, when the user attempts to connect to the resource, they are challenged to prove that they hold the private key as part of the authentication process. Server authentication may be implicit or explicit, but the server will have its own asymmetric host key regardless.

While SSH keys may sometimes be tied to a certificate, they are often not. Thus, connections are pairwise and can occur between client and server with no interaction or oversight from other entities. Clients will often cache the fingerprint of a server's public key to trust it for future connections. This often creates a "wild west" situation where SSH connections can occur from anywhere and be active at any time. That includes keys still being valid after many years of inactivity.

Organizations often find themselves in one of four states, listed here in increasing level of maturity:

- ***The "Wild West":*** SSH user keys are completely decentralized with no or minimal centralized involvement;

- ***Centralized Tracking:*** SSH keys are created and exist as in the "Wild West" situation, but there is a centralized inventory to keep track of where the SSH keys exist;
- ***Centralized Management***: SSH connections still occur between client and server, but in addition to tracking, a centralized service will create, distribute, and renew SSH keys to client and server. There is likely some level of automation in this stage;
- ***Centralized Operations:*** SSH connections themselves are managed through a centralized platform so that not only are keys distributed to client and server, but the connection itself will run through the platform. There is a greater degree of automation in this stage. The centralized entity may be part of a Privileged Access Management (PAM) environment.

It should be noted that even in the most mature state, there is still the possibility that "wild west" SSH connections will occur.

The SSH protocol also uses key agreement and symmetric key cryptography to provide confidentiality. The confidentiality properties of SSH have not been considered in this version and will be addressed in a future revision.

SFTP is a file transfer protocol which usually leverages SSH to make an initial connection. SFTP as a protocol has no cryptography, rather it assumes it is run over a secure channel. Thus, the crypto-agility consideration for SFTP are the same as the considerations for the underlying protocol securing it, which is most often SSH.

I.2.12.2 Discovery/Inventory

In order to be crypto-agile, an organization must at least be able to identify where its SSH keys are. Hence, it is a requirement that the organization must at least be in the ***Centralized Tracking*** state. This would mean that they would have a centralized inventory of SSH keys with the ability to discover new ones which may pop up. This discovery can be performed with currently available scanning tools or by monitoring connections to centralized SSH servers.

In terms of inventory, clients and servers could theoretically be any machines, and keys could exist anywhere on those machines, so a complete discovery may be very difficult. As the purpose of SSH is to establish access to the server, we will focus our attention on server-side SSH key discovery.

At minimum, an inventory must include the following details from server-side resources:

- Server metadata (e.g., server name, URL, IP address, network location, etc.);
- Server private-key metadata (e.g., algorithm, key length);
- For each user for which an SSH connection will be accepted:
    - Metadata of clients the user has used (e.g., client name, client version, operating system, IP address, network location, etc.);
    - User public keys or hash of public keys (including algorithm used);

    - User access level (e.g., root, user, permissions);
    - Latest time of access.
- In the case of SFTP, it may also be useful to list:
    - Landing zone location for files on the server.

This information can typically be obtained from current discovery tools.

Performing a scan and inventory on clients may be infeasible and so will not be listed as a requirement for being crypto-agile. However, even a partial list may be of value to an organization. If an organization does wish to have such an inventory, the following are recommended inclusions:

- Client metadata (e.g., machine name, IP address, network location, etc.);
- For each SSH key on this machine:
    - Directory location of SSH key;
    - Metadata of user associated with SSH key;
    - Public key;
    - Public-key metadata (e.g., algorithm, length).
- For SFTP, it may also be useful to list:
    - Landing zone location for files on the client.

It would additionally be useful to list the servers which will grant resource access to this client public key. However, this is usually not inherently available. It may be more feasible to cross-reference the client and server inventories to glean information such as this.

The traditional process of discovery involves scanning common locations in client and servers. It is theoretically possible to scan the network looking for SSH traffic, although this is more complicated and, for many organizations, infeasible.

I.2.12.3 Migration Considerations

When migrating to new algorithms, the main considerations are:

- It is assumed that the vendors or an appropriate industry working group will have made the appropriate standards modifications to the protocol, if necessary, to support the new algorithms.
- Clients and servers typically have a many-to-many relationship, where a client is often used to connect to multiple servers, and a server generally accepts connections from multiple clients. Moreover, a server in one SSH connection may be the client in another SSH connection.
- As a result of this interconnectedness, it is essential that, at least server-side, connections using old and new algorithms be allowed simultaneously so as not to disrupt business operations.

- The appropriate algorithm(s) which are to be supported must be chosen. The server may support multiple host key algorithms and provides a preferential order. The choice of which client authentication algorithms to accept is made server-side.
- Both the server and the client would need to be migrated to support the new types of cryptographic keys and algorithms. SSH is often performed through a vendor product and so the vendor would be responsible for the new product.
- Where the model used is the *Centralized Management* or *Centralized Operations* model, the central entity will need to be migrated for use in the new algorithms. In these situations, the onus on algorithm selection transfers from the servers to the central entity. The central entity will likewise need to be capable of creating the new SSH keys and, in the case of *Centralized Operations*, facilitating the new SSH connections.
- For SFTP, encryption of files is typically not persistent, so retention of old keys should not be an issue.

I.2.12.4 Cutover Strategy

The cutover strategy would depend on the maturity level, but in general, it should be server-focused. It is important to ensure that the servers are migrated first and can support both new and old connections. Upon upgrade of coding, this may simply involve re-instantiating the daemon which is accepting connections. A daemon in this context refers to code (i.e., software) that runs as a background process.

Once the servers have been migrated, the clients will be able to migrate at their own convenience. The organization would have to decide for how low long to allow backward compatibility with the old algorithm. There would presumably be a cutover date at which point the old algorithms would no longer be accepted by servers. It would additionally have to have a strategy to deal with clients whom cannot or will not migrate to the new algorithms.

When in the Centralized Management or Centralized Operations model, the central entity will obviously need to be upgrade and be simultaneously compatible with old and new algorithms. It can then be used to enforce the migration operations between clients and servers according to their readiness.

For SFTP, it would be important to track any active file transfers which are in effect at the time of migration. If they are not halted or paused, then extra care should be taken to make sure they are not interrupted.

I.2.12.5 Governance

Governance, again, can only occur when the organization at least is doing Centralized Tracking. The centralized entity could either manually or automatically track the migration status of servers at a minimum.

The governance process would need to track the migration status of tracked clients and servers. It would also need to discover and deal with any "wild west" connections which may pop up. Finally, it will need to deal with SSH clients (and possibly servers) whose connections have gone dormant for long periods of time.

I.2.13 SAML or Other Federated Identity

I.2.13.1 Description

Security Assertion Markup Language (SAML) is a standardized set of protocol messages based on XML syntax which enables authorization of a user to access a particular service. It inherently verifies identity, authenticates users, and authorizes services. Depending on the version of SAML, some inherent elements may be encrypted.

Cryptographic security in SAML is most often provided by running the service over TLS channels. Important considerations for TLS are covered in Sections I.2.4 and I.2.5.

SAML relies on three major parties:

- User – the entity requesting access to a service;
- Identity Provider (IdP) – the entity which verifies the identity of the user;
- Service Provider (SP) – the entity providing the service.

The main asset is a SAML token provided by the Identity Provider which is verified by the Service Provider to allow the User to access the SP's resource.

Please note that the method of verification to authenticate the User to the IdP is out of the scope of this Annex.

An alternative SAML access flow can occur when the User performs an initial login to the IdP to get a SAML token and then is free to use the token with any SP. An example would be a User logging into their computer at the beginning of a workday and then accessing services throughout the day via Single Sign-On (SSO).

SAML also has several different methods of flow. They are:

- **Bearer** – the presence of any valid SAML token will grant access to the resource;
- **Holder of the Key** – similar to Bearer, but the SAML token is bound to the User and the User must verify to the SP that they are the entity identified in the SAML token;

- **Sender Vouches** – similar to Bearer, but there is an additional entity called an Intermediary which handles all processing on behalf of the User and additionally signs messages to the SP.

Other frameworks used to provide identity authentication, such as OpenID Connect, a commonly used extension of the OAuth 2.0 authorization standard, have certain differences but follow a similar theme. Therefore, many of the considerations for these frameworks would be similar.

I.2.13.2 Discovery/Inventory

Any inventory of SAML should start with a list of each different instance of a SAML network, usually with a unique IdP. For each IdP, the following information should be inventoried:

- SAML version used;
- IdP name and metadata (e.g. machines on which IdP resides);
- IdP vendor name and version or internal identifier if developed in-house;
- List of downstream SPs accepting tokens from this IdP;
- General list of user (actual list or generic information on types of system is too dynamic to keep track); this would include information as to what type of SAML is used (e.g. bearer, holder-of-the-key, sender-vouches).

I.2.13.3 Migration Considerations

While the SAML specification is maintained by OASIS, the cryptography available in SAML is inherited from XML, which is maintained by W3C. To migrate SAML for use with new algorithms, the expected path would be for an update to the XML encryption standard by W3C to include these algorithms.

From there, the following would be the major considerations:

- The vendor or in-house development team would have to update the coding of the IdP, SP, and user to accommodate the new SAML standard:
  - IdPs and SPs perform processing and would need coding changes in all cases;
  - Clients who perform holder-of-the-key would also need coding changes;
  - Clients who only do bearer or sender-vouches would need to ensure ancillary changes such as buffer sizes and storage are compatible with new data types and sizes.
- The appropriate algorithms would need to be selected.
- It would be vital for the product vendor or creator to give guidance on how their product changes would affect users, IdPs, and SPs whom have not migrated yet. This is critical for backwards compatibility.

I.2.13.4 Cutover Strategy

The cutover strategy is very dependent upon the considerations described in Section I.2.13.3. Migrated products for which backward compatibility is fully supported would require a different strategy from those which do not or have some issues with it. In any case, there is no way of knowing the effects of a migrated protocol at this point in time. Thus, we can state only some generic principles in terms of cutover strategy.

To cut over:

- There would first have to be an understanding of the new protocol, the way different products work, and the results of product testing.
- Each entity would have to generate new keys offline and have them distributed to the other entities, again offline
- When putting the new keys (and hence the migrated product) into service, there must be a strategy in place to turn on new capabilities in a certain order, observe behavior, and deal with entities which have been rendered inoperable or degraded.
- There must also be a strategy in place to deal with SPs which were previously untracked and unaccounted for and will be degraded or rendered inoperable.
- Beyond this, we cannot say much about a cutover strategy at this point.

I.2.13.5 Governance

More than any other use case, this one would appear to require the most inherent governance during cutover. It should consider not only all of the different entities which have been tracked, but also those that will be discovered during the migration. It will likely have to deal with entities becoming degraded or inoperable during cutover.

APPENDIX A: QUANTUM-READINESS MYTHS AND FAQs

	Myth	Reality
1	The Quantum Threat applies only to a small set of organizations within Canada.	The Quantum Threat is of national significance and impact. The risks to information security as well as health and safety, across domains including Critical Infrastructure, 5G, Cloud, AI/ML, and IoT, will require actions at a national scale, and efforts and actions from both government and organizations.
2	Quantum Threat: For my organization, that's an Information Technology (IT) problem ?	For the Organization, the threats and risks posed by Quantum Computing are, first and foremost, a BUSINESS problem.
3	The Information and Communications Technology (ICT) sector and related industry organizations will solve this. My organization / sector don't have to do anything… or not much ?	It is true that the vast array of quantum stakeholders, including standards organizations, ICT sector organizations, academia, and others are working diligently to try to address the threats posed by the future of quantum computing. However, at the end of the day, individual organizations and sectors are ultimately accountable for ensuring the confidentiality, integrity, and availability of all key data of value that is stored, processed, and transmitted.
4	This is not a pressing issue at this time. Getting prepared for Quantum … that can wait ?	The process of Quantum Risk Assessment and Quantum Migration may take many years, if not even longer. The timelines for organizations and sectors will depend on many factors, including but not limited to: numbers, types, complexities, and interdependencies (intra-org and inter-org) of products, systems, interfaces, and solutions employing various cryptographic systems; trusted supply chain of cryptographic systems (hardware & software); Skilled resources' availability; etc.

	Myth	Reality
5	NIST is still in the process of standardizing Post-Quantum Cryptography. Should one wait until that is done, before starting QSC prep ?	From a planning perspective, while standardized quantum-safe crypto is not yet available, there are NO direct dependencies on the outcomes of the NIST Post-Quantum Cryptography Standardization process that would prevent or delay an organization / sector from starting to assess and plan for the impacts of quantum technologies on cryptography. From an QSC migration perspective, the future implementations must be based on standards based and certified cryptographic algorithms and products and solutions.
6	The risk is low within the organization / sector, because cryptography usage is very low / low ?	Cryptography is pervasive and embedded across all aspects of Information and Communications Technology, to help ensure the confidentiality, Integrity of information that is stored, processed, and transmitted.
7	The confidentiality of current sensitive information is safe for now. Getting Quantum-Prepared can wait ?	One of the key threat scenarios is the capture of data today (including encrypted data as well as cryptographic information such as cryptographic key exchanges), and then decrypting the captured data in the future using quantum technologies.
8	Preparing for Quantum Readiness for my org / sector seems simple and straight forward. Getting Quantum-Prepared can wait ?	That depends. Quantum Readiness depends on may factors, including but not limited to : the amounts and types of data of values ; the requirements for keeping the data confidential and integral ; the number and types and systems that store, process and transmit the data ; the number and complexities of interfaces to other systems ; inter-organization dependencies ; A Quantum Readiness assessment may be required to understand the level of simplicity or complexity to prepare for Post-Quantum Cryptography.

	Myth	Reality
9	Preparing for Quantum-Readiness is as simple as some software upgrades to incorporate new crypto protocols. Right ?	This is DEFINITELY NOT like a “simple monthly software update”. A detailed technical review of current products, systems, infrastructure, and architectures that leverage cryptographic modules will help determine if any hardware upgrades, software upgrades, application upgrades, or even complete system replacements, may be required.
10	Preparing for Quantum-Readiness seems overwhelming ?	While the detailed technical aspects of Quantum threats and cryptographic aspects are beyond the skills of most, the vast majority of Quantum-Readiness steps are typically incremental steps on existing business as well as technical strategic and operational processes and procedures. Open source information, such as the Quantum-Readiness Best Practices guide, plus exemplars, are intended to help organizations and sectors start immediately.
11	For symmetric cryptography, all that needs to be done is to ensure that the key length is sufficiently large to provide QSC assurance ; it’s that simple, right ?	Strictly speaking, from the “narrow” perspective of symmetric cryptography, yes, if the ley length is sufficiently large, then the symmetric cryptography may be deemed safe. However, depending on the use case, in support of the symmetric cryptography, there may be also be a need for key exchange and key management of the symmetric keys, and those techniques typically require using asymmetric cryptography. So if this is the case, then the system will be vulnerable to Quantum based cryptographic attacks.
12	We implement some non-standards based cryptography. That’s OK, right ?	Using any proprietary or non-standard cryptography, or any algorithm that has not received substantial review is a big security risk.

APPENDIX B: QUANTUM-SAFE POLICIES, REGULATIONS AND STANDARDS

B.1 QUANTUM-SAFE POLICIES

The Canadian Centre for Cyber Security introduced new guidance on preparing for Post-Quantum Cryptography (PQC) in the following document published during 2022:

- **Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information (Version 2)** ITSP.40.111, August 17, 2022, 28 pages

  This document identifies and describes recommended cryptographic algorithms and appropriate methods of use that organizations can implement to protect sensitive information.

  Section 12 Preparing for post quantum cryptography

  NIST is expecting to finalize standards (for PQC) by 2024. We will update the guidance in this document to address the quantum threat once standards are available. In the meantime, we recommend the following high-level steps:

  - *Evaluate the sensitivity of your organization's information and determine its lifespan to identify information that may be at risk (e.g., as part of on-going risk assessment processes).*
  - *Review your IT lifecycle management plan and budget for potentially significant software and hardware updates.*
  - *Educate your workforce on the quantum threat.*
  - *Consider using Stateful Hash-based Signature schemes if you meet the criteria in Section 5.4.*

  For more detailed information on how to prepare, see Preparing Your Organization for The Quantum Threat to Cryptography (ITSAP.00.017).

  Organizations should wait until standards for quantum-resistant public-key encryption and signature schemes are finalized before using any candidate algorithm to protect information or systems.

Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information
CCCS, August 17, 2022, Page 22

B.2 QUANTUM-SAFE REGULATIONS

Canada has not enacted any regulations related to quantum-readiness or quantum-safe cyber security to date.

B.3 QUANTUM-SAFE STANDARDS

The U.S. National Institute of Standards and Technology (NIST) began work on new standards for PQC in 2015. NIST's goals continue to include publishing a first set of PQC standards in 2024.

During the summer of 2022, NIST reported on the results of their third-round of evaluating and selecting candidate PQC algorithms for standardization, for public-key encryption/key-encapsulation mechanisms (KEMs) and for digital signatures, as follows:

- ***With the conclusion of the third round, NIST is pleased to announce the first public-key algorithms that will provide protection from quantum attacks to be standardized.***
- ***The primary algorithms NIST recommends for most use cases are CRYSTALS–KYBER (key-establishment) and CRYSTALS–Dilithium (digital signatures). In addition, the signature schemes FALCON and SPHINCS$^+$ will also be standardized*** *…* ***and*** *… (other)* ***candidates continue for further study in a fourth round of evaluation.***
- ***NIST will create new draft standards for these algorithms, with coordination of the submission teams to ensure that the standards are in agreement with the specifications.***
- ***As part of the drafting process, NIST will seek input on which specific parameter sets to include ... When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow. NIST hopes to publish the completed standard by 2024.***

Status Report on the Third Round of the NIST PQC Standardization Process - NIST IR 8413-upd1
NIST, July 2022 (including updates as of 09-26-2022), Page 52

APPENDIX C: U.S. NCCOE PROJECT ON MIGRATION TO PQC

On August 4, 2021, the U.S. National Cybersecurity Center of Excellence (NCCoE) within NIST announced the start of a new project on *Migration to Post-Quantum Cryptography*. [21]

The outputs of this project could input to the development of best practice recommendations for Section 3.4 - Migration to PQC (Phase 4).

> ***The NIST National Cybersecurity Center of Excellence (NCCoE) is initiating the development of practices to ease the migration from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to quantum computer-based attacks.***
>
> ***The project will provide systematic approaches for migrating from vulnerable algorithms to quantum-resistant algorithms across the different types of assets and supporting underlying technology.***

The NCCoE's scope for this project includes investigating five demonstration scenarios that would be applicable to a broad range of organizations globally (including organizations in Canada). The scenarios are:

> ***Scenario 1: FIPS-140 validated hardware and software modules that employ quantum-vulnerable public-key cryptography;***
>
> ***Scenario 2: Cryptographic libraries that include quantum-vulnerable public-key cryptography;***
>
> ***Scenario 3: Cryptographic applications and cryptographic support applications that include or are focused on quantum-vulnerable public-key cryptography;***
>
> ***Scenario 4: Embedded quantum-vulnerable cryptographic code in computing platforms; and***
>
> ***Scenario 5: Communication protocols widely deployed in different industry sectors that leverage quantum-vulnerable cryptographic algorithms.***

A preliminary draft summary of initial findings from this project was released for public comments during the spring of 2023. [22]

---

[21] Migration to Post-Quantum Cryptography - Project Description NIST, August 2021, 16 Pages

[22] Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography, NIST Special Publication 1800-38A, May 2, 2023, 5 Pages

APPENDIX D: PQC CONSIDERATIONS FOR BLOCKCHAIN / DLT

This Appendix provides a brief introduction to the topic of blockchain and distributed ledger technology (DLT), in the context of Post-Quantum Cryptography (PQC) considerations.

The following assumes that the reader is generally familiar with the architectures and key characteristics of blockchains and distributed ledger technologies, in terms of the basics of.

Problem statement

The current implementations of blockchain and distributed ledger technology applications and solutions will be subject to increased risk with the appearance of quantum computers and quantum algorithms that are able to break the current suite of classical (non post-quantum cryptography) algorithms and implementations, especially asymmetric cryptography algorithms.

Cryptography is one of the key characteristics of the blockchain architecture.

Hashing, public-private key pairs, and the digital signatures together constitute the cryptographic foundations for the blockchain.

In a post-quantum environment, all of the cryptographic foundations are at increased risk, especially the digital signatures and public-private key pairs, which are based on asymmetric cryptographic algorithms.

Cryptocurrencies are one of the major applications of blockchain, where public-private key pairs are used to maintain addresses, and digital signatures are used to digitally sign transactions. Cryptocurrencies are therefore are at risk when cryptographically relevant quantum computers are available in the future.

The time to act is now

The standardization of post-quantum cryptographic algorithms is anticipated soon.

For applications of blockchain and distributed ledger technologies, such as cryptocurrencies and smart contracts, now is the time to review quantum related threats, vulnerabilities, impacts, and risks, and start researching, planning, and preparing for the mitigation and migration of those applications to post-quantum cryptographic based solutions.

References / resources

There is a growing set of publicly available resources focused on the topic of how quantum computers and post-quantum cryptography will impact blockchain and distributed ledger technologies, and the applications and solutions that use them, including for example digital currencies and smart contracts.

Below is a small non-exhaustive sample of some references on this topic.

Quantum-Proofing the Blockchain	Blockchain Research Institute, November 2017 Vlad Gheorghiu, Sergey Gorbunov, Michele Mosca, and Bill Munson University of Waterloo https://www.blockchainresearchinstitute.org/project/quantum-proofing-the-blockchain
Quantum-Resistance in Blockchain Networks	Inter-American Development Bank, June 2021 ITE Department & IDB Lab DISCUSSION PAPER No IDB-DP-00866 https://publications.iadb.org/publications/english/document/Quantum-Resistance-in-Blockchain-Networks.pdf
Vulnerability of blockchain technologies to quantum attacks	Joseph J. Kearney, Carlos A. Perez-Delgado, 23 April 2021 University of Kent, School of Computing Canterbury, Kent, UK https://www.sciencedirect.com/science/article/pii/S2590005621000138

APPENDIX E: QUESTIONS TO ASSESS THE PQC POSTURE OF A 3rd PARTY

This Appendix contains a series of questions to help an organization to begin assessing the PQC maturity or 'posture' of a 3rd Party organization that it may do business with. A 3rd Party in this context may be a technology partner or vendor, or a supplier of other products, goods, or services.

The intent/focus is to evaluate a 3rd Party's cryptography and PQC posture, to assist the organization that asks these questions, to determine the risk of doing business with the 3rd Party. This risk determination can and will vary in different organizations based on their risk tolerance associated to this topic.

The questions in this Appendix can be used, wholly or partially, to generate insight into 3rd Party risk associated with the likelihood that the Quantum threat will affect business continuity. The responses by a 3rd Party to these questions may be used by the organization asking these questions, to evaluate risk to their organization, by defining a risk rating that is aligned to their organization's risk tolerance.

Different Questions for Different Time Periods

Three sets of assessment questions are provided below, to assist in determining a 3rd Party's maturity in cryptography and posture with respect to Post-Quantum cryptography migration. Each set of questions is designed for a different time period associated with the following stages of the Post-Quantum Cryptography migration:

A. Pre-Standardization (Today)

B. Post-Standardization (Starting 2024 or 2025)

C. Post-Quantum (Starting 2030 or later)

A) Questions for the Pre-Standardization Period (Today)

The following questions are for the period of time before quantum-safe algorithms and PQC standards are defined, and before government agencies decide on the set of standardized quantum-safe algorithms they will recommend be used.

The world is in the pre-standardization period now, and this is anticipated to continue until 2024 or 2025. This period is best characterized with planning for PQC migration.

3rd Party PQC Posture Assessment Questions (Pre-Standardization)

1. Have you (viz., the 3rd Party being asked) considered the future impacts of quantum computing in the cryptography used to deliver your services?
   Response Selection: Yes, No
2. Do you have a well-defined and up to date cryptographic management practice within your organization which includes:
   a. An approved cryptographic Policy and/or Standard?
      Response Selection: Yes, No, In progress
   b. An up to date inventory of cryptography usage (at rest and in transit)?
      Response Selection: Yes, No, In progress
   c. An up to date inventory of cryptographic artifacts, components, modules, and systems?
      Response Selection: Yes, No, In progress
   d. Do you have up to date operational processes and procedures for managing cryptographic technology?
      Response Selection: Yes, No, In progress
   e. Do you have a documented, up to date, and approved process for the upgrade and replacement of obsolete and deprecated cryptography?
      Response Selection: Yes, No, In progress
   f. Do you have cryptographic agility capabilities?
      Response Selection: Yes, No, In progress

B) Questions for the Post-Standardization Period (Starting 2024 or 2025)

In the face of shifting market demands, technological advances, and customer expectations, industry standards may be revised and enhanced. The questions proposed in this section will concentrate on the early stages of established standards.

These questions are for the period after quantum-safe algorithms and PQC standards have been fully defined. This period is best characterized as the time for organizations to start migrating their IM, IT and OT products and systems to PQC, and to complete their migration as soon as practical.

3rd Party PQC Posture Assessment Questions (Post-Standardization)

1. Do you (viz., the 3rd Party being asked) have a well-defined and up to date cryptographic management practice within your organization which includes:
    a. An approved cryptographic Policy and/or Standard?
        Response Selection: Yes, No, In progress
    b. An up to date inventory of cryptography usage (at rest and in transit)?
        Response Selection: Yes, No, In progress
    c. An up to date inventory of cryptographic artifacts, components, modules, and systems?
        Response Selection: Yes, No, In progress
    d. Do you have up to date operational processes and procedures for managing cryptographic technology?
        Response Selection: Yes, No, In progress
    e. Do you have a documented, up to date, and approved process for the upgrade and replacement of obsolete and deprecated cryptography?
        Response Selection: Yes, No, In progress
    f. Do you have cryptographic agility capabilities?
        Response Selection: Yes, No, In progress
2. Does your organization have an approved PQC migration strategy/plan?
    Response Selection: Yes, No, In progress
3. Do you have funding allocated for the PQC strategy/plan?
    Response Selection: Yes, No, In progress
4. Have you begun the migration?
    Response Selection: Yes, No, In progress
5. When do you expect your PQC migration to the completed?
    Response Selection: < 2 years, 2-5 years, more than 5 years

C) Questions for the Post-Quantum Period (Starting 2030 or later)

Whereas the focus of the questions up to this point has been on the risk posed by third parties, depending on their quantum posture. The questions in this section, however, can also be seen as guidance for third parties, which will need to be quantum-ready for their own purposes (notably business continuity) even if the haven't been pressed to do so by their customers or partners.

These questions are for the period of time after a quantum computer has successfully proven classical cryptography to be vulnerable. This period is best characterized with realized risk to classical cryptography.

3rd Party PQC Posture Assessment Questions (Post-Quantum)

1. Do you (viz., the 3rd Party being asked) have a well-defined and up to date cryptographic management practice within your organization which includes:
    a. An approved cryptographic Policy and/or Standard?
        Response Selection: Yes, No, In progress
    b. An up to date inventory of cryptography usage (at rest and in transit)?
        Response Selection: Yes, No, In progress
    c. An up to date inventory of cryptographic artifacts, components, modules, and systems?
        Response Selection: Yes, No, In progress
    d. Are you aware of any cryptography within your organization which should not be used in light of the quantum computing threat?
        Response Selection: Yes, No, In progress
    e. Do you have up to date operational processes and procedures for managing cryptographic technology?
        Response Selection: Yes, No, In progress
    f. Do you have a documented, up to date, and approved process for the upgrade and replacement of obsolete and deprecated cryptography?
        Response Selection: Yes, No, In progress
    g. Do you have cryptographic agility capabilities?
        Response Selection: Yes, No, In progress
    h. Is your organization fully migrated to Post-Quantum Cryptography?
        Response Selection: Yes, No, In progress
2. If the answer to 1h is “No” or “In Progress” :
    a. Does your organization have an approved PQC migration strategy/plan?
        Response Selection: Yes, No, In progress

b. Do you have funding allocated for your PQC strategy/plan?
Response Selection: Yes, No, In progress

c. When do you expect your PQC migration to the completed?
Response Selection: < 2 years, 2-5 years, more than 5 years

3. If the answer to 2c is "2-5 years" or "more than 5 years" :

a. Does your organization (viz., the 3rd Party being asked this question) have crisis-management capacity, as it may be necessary given your circumstances?
Response Selection: Yes, No, In progress

APPENDIX F: TEMPLATE TO CATALOG TECHNOLOGY VENDOR/ SUPPLIER PQC CAPABILITIES

This Appendix contains a template that an organization could use to begin compiling a view of the PQC roadmaps (e.g., PQC features, capabilities, compliance to standards, and anticipated timelines for commercial availability) for each of the technology vendors and/or suppliers it deals with.

This template, or a customized version of it, can be used to canvas a technology vendor or supplier to gather information needed to inform your PQC migration planning, by gathering relevant information about that vendor or supplier's products manufactured by that vendor as used within your organization. Note that the development of an organization's timeline (and project plan) for migrating to PQC may gated by the PQC implementation timelines of its technology vendors and suppliers.

The column headings shown below can be used as a starting point to canvas suppliers for information needed to develop an organization's PQC migration project plan and schedule. This template can also be used as part of the RFP process during acquisition of new products.

When using this template for an existing vendor/supplier, prior to sending, insert a description of the vendor's products and versions (of those products) currently used within your organization.

Technology Vendor/Supplier: *Add Vendor Name Here*

To assist in Post-Quantum Cryptography migration planning, complete the following table for all technology products/services, including current targets on release of a Quantum-Safe version and the supported algorithms.

#	Product (Name, #, Identifier)	Current Version	Quantum-Safe Version	Release/Target Date	PQC Algorithms Supported
Ex1	*Product with no cryptography (example)*	*v1.2.0*	*NA*	*01 March 2015*	*NA - No cryptography present*
Ex2	*Product with cryptography - (future release example)*	*v1.0.0*	*Future - v2.1.1*	*Q1 2024*	*Kyber, Dilithium*
Ex3	*Product with cryptography - (quantum safe example)*	*v2.5.1*	*V3.2.x*	*2022-02-01*	*Kyber, Dilithium*

#	Product (Name, #, Identifier)	Current Version	Quantum-Safe Version	Release/Target Date	PQC Algorithms Supported

Note that the column headings in this template may and should be revised as appropriate to gather relevant information for your organization. For example, additional columns may be added to:

- denote your organization's use of the vendor's product (e.g. secure data transfer, file storage, user authentication, signing and digital signatures, key establishment, certificate management);
- ask for more information about the PQC algorithms supported (e.g., which standard(s) do the PQC algorithms comply with?);
- ask about plans for certification (e.g. FIPS 140), when such certification supports PQC;
- ask if products support cryptographic agility;
- ask about software and firmware upgrade policies and procedures for any necessary or large agility updates; and
- more . . .

Technology Vendor Product PQC Catalogue:

This template can be used to canvas technology vendor/supplier to gather PQC migration information associated to technology products used within your organization. This will assist in your Post Quantum Migration planning. It can also be used as part of RFP process during acquisition of new products.

When using for an existing vendor/supplier, prior to sending add the vendor products and current versions used within the organization.

Technology Vendor/Supplier: *Add Vendor Name*

To assist in Post Quantum Cryptography migration planning, complete the following table for all technology products/services, including current targets on release of a Quantum Safe version and the supported algorithms.

#	Product (Name, #, Identifier)	Current Version	Quantum Safe Version	Release/Target Date	PQC Algorithms Supported
Ex1	*Product with no cryptography (example)*	*v1.2.0*	*V1.0.1 or greater*	*01 March 2015*	*NA - No cryptography present*
Ex2	*Product with cryptography - (future release example)*	*v1.0.0*	*Future - v2.1.1*	*Q1 2024*	*Kyber, Dilithium*
Ex3	*Product with cryptography - (quantum safe example)*	*v2.5.1*	*V3.2.x*	*2022-02-01*	*Kyber, Dilithium*

APPENDIX G: PQC ROADMAP QUESTIONS TO ASK VENDORS

This Appendix contains eight "PQC Roadmap" questions that have been developed for owners and operators of critical infrastructure (CI) to send to their vendors of Information or Communications Technology (ICT) products or services.

Background / Overview

From January to March 2023, the CFDIR Quantum-Readiness Working Group (QRWG) drafted an initial set of "PQC Roadmap" questions to seek information from vendors that will be needed by CI owners and operators to inform their Post-Quantum Cryptography (PQC) adoption/migration planning.

The QRWG "alpha tested" the utility of the questions in this Appendix by asking several organizational members of the CFDIR to answer them during April and May 2023. That process led to the revision of some questions to clarify the information being sought. The revised questions were vetted through additional testing and are presented below.

"PQC Roadmap" questions for vendors of ICT products and/or services

Q1: What can you share about your roadmap for including post-quantum cryptography (PQC) in your [**Product / Service**], such as a timeline for when PQC support will be available to customers for all quantum-vulnerable public key cryptography usage by your [**Product / Service**] ?

Q2: Will support for PQC in your [**Product / Service**] be made available through patches or updates under existing contracts and purchases?

Q3: Will your [**Product / Service**] require customers to replace existing hardware or make system architecture changes to support the PQC migration?

Q4: How will your [**Product / Service**] support cryptographic agility to allow flexible administration of configurations for planned cryptographic migration, or an unplanned and immediate migration to remediate a weakness in an algorithm?

Q5: What operational/configuration guidance will you be providing customers on how to migrate your [**Product / Service**] to utilize PQC?

Q6: When your [**Product / Service**] is updated to support PQC, will you ensure the cryptography is independently validated for implementation assurance, for example FIPS 140-3 certification under the Cryptographic Module Validation Program (CMVP)?

Q7: Are your 3rd party suppliers aware of and addressing the quantum computing threat, and are you evaluating how their PQC posture may impact your business operations and your customers?

Note: Appendix E of the CFDIR *Quantum-Readiness Best Practices v.02* provides questions an organization may use to assess the PQC posture of a third-party : https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2022/cfdir-quantum-readiness-best-practices-v02-en.pdf .

Q8: Can you nominate a contact person for any follow-up questions on your answers to questions 1 to 7 ?

How to use the [Product / Service] field that appears on some of the questions

The first six questions include a field denoted by square brackets: [**Product / Service**].

This field is a placeholder to identify the spot, in each question, where the name of a vendor's product or service should be inserted before sending the questions to that vendor.

In situations where a CI owner or operator uses more than one product or service from the same vendor, it is important to consider that the PQC roadmaps for the different products and services may not be identical. As a result, we recommend CI owners or operators ask their vendors to answer all eight PQC Roadmap questions for each of the products and/or services of interest that are provided by those vendors.

One way to ask a vendor about their PQC Roadmaps for different products or services is to send multiple copies of the questions to the vendor, and to write the name of a different [**Product or Service**] into each set of questions.

The contents of this document were developed
during the course of CFDIR QRWG meetings and workshops
between July 2020 and June 2023.

This document will be updated annually,
to reflect industry feedback from implementing
the best practices described herein.

TLP : CLEAR

Version 03 - June 12, 2023

Prepared by the Quantum-Readiness Working Group
of the Canadian Forum for Digital Infrastructure Resilience