



LIGNES DIRECTRICES ET PRATIQUES EXEMPLAIRES nationales canadiennes pour la préparation en matière de technologie quantique

Version 01 – 7 juillet 2021



Préparé par :

Groupe de travail sur la préparation en matière de technologie quantique (GTPTQ)
du Forum canadien pour la résilience des infrastructures numériques (FCRIN)

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

Le contenu de ce document est **TLP : BLANC**

Sous réserve des règles usuelles en matière de droits d'auteur, les renseignements **TLP : BLANC** peuvent être diffusés sans restriction. La reproduction est autorisée à condition que la source soit mentionnée.



Contenu

Contenu	iii
Avant-propos	iiv
Remerciements	v
Quelques mots sur la cryptographie	vi
Historique des révisions	vii
1. Introduction	1
1.1 Objectif	2
1.2 La menace quantique	2
1.3 Pourquoi commencer à se préparer maintenant?	3
1.4 De combien de temps dispose-t-on?	5
1.5 À propos du présent document	8
2. Sources d'information	10
3. Pratiques exemplaires recommandées pour la préparation en matière de technologie quantique	11
3.0 Étape I – Préparation (phase 0)	14
3.1 Étape I – Découverte (phase 1)	15
3.2 Étape 1 – Évaluation des risques quantiques (phase 2)	18
3.3 Étape II – Phases de mise en œuvre 3, 4 et 5	22
4. Sensibilisation et perfectionnement des compétences	24
5. Mobilisation des fournisseurs	25
5.1 Questions recommandées pour mobiliser un fournisseur de CPQ	25
5.2 Clauses d'approvisionnement concernant la CPQ pour les demandes de renseignements (DDR) et les demandes de propositions (DDP)	25
6. Conclusion/principaux points à retenir	26
Annexe A : Glossaire	28
Annexe B : Cas d'utilisation recommandés de la cryptographie à découvrir et à documenter	29
Annexe C : Contenu nécessaire pour décrire les utilisations de la cryptographie par une organisation	30
Annexe D : Exemple de cas d'utilisation n° 1 – utilisation de Kerberos pour l'authentification	31
Annexe E : Exemple de cas d'utilisation n° 2 – ICP/AC	37
Annexe F : Exemple de cas d'utilisation n° 3 – sFTP	44
Appendice A : Mythes et FAQ concernant la préparation en matière de technologie quantique	49
Appendice B : Politiques, règlements et normes post-quantiques	52
B.1 Politiques post-quantiques	52
B.2 Réglementation post-quantique	52
B.3 Normes de sécurité post-quantique	52
Appendice C : Projet du NCCoE des É.-U. sur la migration vers la CPQ	53

Avant-propos

La Banque du Canada s'est engagée à collaborer avec ses partenaires des secteurs public et privé pour promouvoir et renforcer la résilience du secteur financier canadien face aux risques qui pèsent sur les opérations commerciales, notamment les cyberincidents.

C'est pourquoi nous avons été heureux de faire partie du Groupe de travail sur la préparation en matière de technologie quantique (GTPTQ) lancé en 2020 par le [Forum canadien pour la résilience des infrastructures numériques \(FCRIN\)](#). Une équipe d'experts en la matière provenant d'organisations responsables d'éléments fondamentaux de l'infrastructure financière essentielle du Canada a étudié ce qu'il faudrait faire pour que le Canada soit « prêt à évoluer dans l'univers quantique » dans les années à venir.

Le message clé que je veux vous transmettre est que nous devons tous commencer à nous préparer dès maintenant. Les technologies de chiffrement qui sécurisent aujourd'hui les systèmes financiers du Canada deviendront un jour désuets. Si nous ne faisons rien, les données financières sur lesquelles repose l'économie canadienne deviendront inévitablement plus vulnérables aux cybercriminels.

Si certains croient encore que la technologie quantique n'est pas pour demain, étant donné que cette technologie de chiffrement avancée n'est pas encore disponible, nous savons également qu'il faudra du temps pour élaborer et mettre en œuvre des systèmes de chiffrement post-quantique pour remplacer ceux dont nous disposons actuellement.

Les recommandations et les renseignements que vous trouverez dans le présent document ont été compilés et élaborés par des personnes chargées d'effectuer ce type de changements dans leurs propres institutions. Il s'agit de concepts fondamentaux – ils s'appliquent aussi bien aux petites qu'aux grandes organisations, tant dans le secteur public que dans le secteur privé.

Cela commence par l'évaluation de l'incidence possible de l'informatique quantique sur votre propre organisation. Outre les risques, l'informatique quantique peut également présenter des occasions. Mais quoi qu'il en soit, nous devons tous nous préparer à cette transition, ce qui comprend ma propre organisation, la Banque du Canada. La résilience du système financier canadien en dépend.

Nous tenons à remercier nos collègues qui ont pris part à ce premier projet pilote. Il reste encore beaucoup de chemin à parcourir, et la Banque du Canada sera aux côtés de ses partenaires à mesure que la question de l'informatique quantique évolue.

Hisham El-Bihbety

Dirigeant principal de la sécurité de l'information, Banque du Canada

Remerciements

Le contenu du présent document a été élaboré au cours des réunions du Groupe de travail sur la préparation en matière de technologie quantique du FCRIN entre juillet 2020 et juin 2021.

Les recommandations et les renseignements qu'il renferme sont le fruit de la participation active et de l'engagement d'experts en la matière provenant des organisations suivantes (énumérées par ordre alphabétique) :

Membres du FCRIN :

BlackBerry, CCC, CIRA, Google, IBM Canada, ISDE, Microsoft Canada, Quantum-Safe Canada

Participants au projet pilote de préparation en matière de technologie quantique :

Banque du Canada, BMO, Banque Scotia, CIBC, Desjardins, Manuvie, RBC, 2Keys

Intervenants de l'écosystème post-quantique :

Crypto4A, Entrust, evolutionQ, InfoSec Global, ISARA

Quelques mots sur la cryptographie

Dans le présent document, les termes « cryptographie » et « crypto » désignent la pratique de la cryptographie, qui comprend des concepts comme le chiffrement, les signatures numériques, le hachage, et plus encore. En particulier, le terme « crypto » ne fait pas référence à la cryptomonnaie, qui est une forme de monnaie numérique non réglementée qui utilise la cryptographie et souvent des technologies de chaîne de blocs.

Historique des révisions

Le tableau suivant décrit les dates des principales modifications apportées à ce document.

Auteurs	Date / Version	Notes
Participants au GTPTQ du FCRIN (juillet 2020 – juin 2021)	7 juillet 2021 / v.01	Version initiale des pratiques exemplaires recommandées, élaborées à partir du projet pilote du GTPTQ avec des membres du secteur des infrastructures essentielles des finances du Canada.

1. Introduction

Les technologies cryptographiques sont utilisées par les gouvernements et l'industrie pour authentifier la source des renseignements que nous communiquons et stockons et pour en protéger la confidentialité et l'intégrité. Les technologies cryptographiques comprennent un large éventail de protocoles, de systèmes et d'infrastructures¹.

Les ordinateurs quantiques perceront la cryptographie à clé publique actuellement déployée et affaibliront considérablement la cryptographie à clé symétrique, qui sont les piliers de la cybersécurité moderne. Ainsi, avant la construction d'ordinateurs quantiques à grande échelle, nous devons migrer nos systèmes et nos pratiques vers des systèmes qui ne peuvent pas être percés par des ordinateurs quantiques. Dans le cadre des systèmes qui visent à assurer une confidentialité à long terme, cette migration devrait se faire encore plus tôt.

[Cybersecurity in an era with quantum computers: will we be ready?](#)

Michele Mosca, novembre 2015

Les Canadiens s'appuient sur des systèmes cryptographiques pour sécuriser leurs applications et leurs sites Web, et pour protéger la confidentialité et l'intégrité de leurs données contre les cybermenaces nationales et internationales. Les ordinateurs quantiques, lorsqu'ils seront utilisés par des auteurs malveillants, seront en mesure de percer un grand nombre des systèmes cryptographiques actuels. Pour contrer cette menace, les systèmes numériques qui traitent, stockent ou transmettent des renseignements de nature délicate ou confidentiels devront être mis à niveau pour utiliser la nouvelle cryptographie post-quantique (CPQ).

Malheureusement, les solutions post-quantiques ne sont pas encore disponibles. Le National Institute of Standards and Technology (NIST) des États-Unis a commencé à travailler sur de nouvelles normes pour la CPQ en 2015, et espère publier des ébauches de normes pour commentaires publics en 2022-2023.

Si votre organisation stocke ou communique des renseignements de nature délicate, l'utilisation de la cryptographie post-quantique sera inévitable dans les prochaines années. Pour que cette transition se fasse en douceur, il existe des mesures pratiques que vous pouvez et devez prendre pour garantir la sécurité de vos renseignements de nature délicate, aujourd'hui et à l'avenir.

[Forbes magazine](#), 8 janvier 2021

¹ [Migration to Post-Quantum Cryptography](#), National Institute of Standards and Technology (NIST) des É.-U., juin 2021

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

La bonne nouvelle est que les entreprises et autres organisations canadiennes, y compris les propriétaires et exploitants d'infrastructures essentielles (IE), devaient avoir suffisamment de temps pour planifier une transition ordonnée et rentable vers la cryptographie post-quantique au cours des prochaines années, en utilisant les pratiques et les lignes directrices recommandées dans le présent document.

1.1 Objectif

L'objectif du présent document est de fournir un ensemble de pratiques et de directives recommandées :

- que les intervenants du secteur des infrastructures essentielles canadiennes et d'autres personnes peuvent utiliser dès maintenant pour planifier et préparer la façon dont ils feront la transition de leurs systèmes numériques afin d'utiliser les nouvelles technologies et solutions cryptographiques post-quantiques; et
- raccourcir les courbes d'apprentissage en offrant des conseils et des exemples concrets qui illustrent « comment » mettre en œuvre les recommandations formulées dans le présent document afin d'éviter que les organisations aient à « partir de zéro ».

Le présent document sera mis à jour chaque année afin de tenir compte des commentaires de l'industrie sur la mise en œuvre des pratiques exemplaires présentées ici, et de fournir des exemples supplémentaires de la « façon » d'opérationnaliser davantage les recommandations stratégiques décrites dans la section 3.

1.2 La menace quantique

La cryptographie asymétrique, ou cryptographie à clé publique, assure la confidentialité et l'intégrité des renseignements de nature délicate. Elle est largement utilisée par le gouvernement du Canada (GC) et par des organisations du secteur privé pour sécuriser et protéger les réseaux de communication, les clés cryptographiques pendant leur distribution, les données inactives, etc.

La plupart des organisations utilisent actuellement la cryptographie à clé publique pour sécuriser les éléments suivants :

- **signatures numériques** : utilisées pour fournir une authentification de la source et une authentification de l'intégrité, ainsi que pour prendre en charge la non-répudiation des messages, des documents ou des données stockées;
- **processus d'authentification de l'identité** : établir une séance de communication authentifiée ou l'autorisation d'effectuer une intervention particulière;

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

- **transport de clés symétriques** (p. ex. enveloppement de clés, chiffrement de données et clés d'authentification de messages) et d'autres matériels de chiffrement (p. ex. vecteurs d'initialisation);
- **processus d'autorisation de privilèges.**

La cryptographie asymétrique part du principe que deux parties ou plus échangent des clés publiques afin d'établir une clé secrète partagée pour chiffrer les données. La cryptographie symétrique, quant à elle, repose sur le principe selon lequel toutes les parties ont déjà partagé exactement la même clé avant de communiquer.

Une fois développés, les ordinateurs quantiques pourront utiliser la physique quantique pour traiter efficacement des renseignements et résoudre des problèmes impossibles à solutionner avec les technologies informatiques actuelles. Les ordinateurs quantiques seront capables de compromettre les algorithmes utilisés dans la cryptographie asymétrique.

Cela signifie que toutes les informations et communications classifiées, de nature délicate et/ou confidentielles qui ont été protégées à l'aide de la cryptographie à clé publique, en particulier celles ayant une valeur à moyen ou long terme sur le plan du renseignement ou un besoin proportionnel de confidentialité à long terme, seront vulnérables au déchiffrement par des adversaires ou des concurrents commerciaux disposant d'ordinateurs quantiques².

Répercussions de l'informatique quantique en matière de sécurité :

Les protocoles de chiffrement actuels, p. ex. Secure Socket Layer (SSL) et Transport Layer Security (TLS), basés sur des algorithmes à clé publique existants, sont en mesure de protéger les communications réseau contre les attaques d'ordinateurs classiques.

Toutefois, un ordinateur quantique insensible aux défaillances pourrait en quelques heures, voire quelques secondes, percer les codes mathématiques sur lesquels reposent ces protocoles et d'autres.

1.3 Pourquoi commencer à se préparer maintenant ?

Voici pourquoi il faut commencer dès maintenant à se préparer à faire face à la menace que les ordinateurs quantiques feront peser sur les systèmes de sécurité existants :

- a) les technologies cryptographiques sont intégrées dans la plupart des produits numériques couramment utilisés par les organisations pour mener leurs activités quotidiennes³;

² [Atténuation obligatoire des menaces liées à l'informatique quantique au GC obligatoire \(ITSB-127\) – Centre canadien pour la cybersécurité](#), mai 2019.

³ [Utiliser le chiffrement pour assurer la sécurité des données sensibles \(ITSAP.40.016\) Atténuation obligatoire des menaces liées à l'informatique quantique au GC obligatoire \(ITSB-127\) – Centre canadien pour la cybersécurité](#), mai 2021.

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

- b) certaines applications et certains systèmes utilisés dans les infrastructures énergétiques, financières, gouvernementales et de transport ont une durée de vie de 15 à 30 ans, et des exigences encore plus longues en matière de protection des données et de confidentialité;
- c) les ordinateurs quantiques insensibles aux défaillances, capables de percer les algorithmes de cryptage et les systèmes cryptographiques existants (p. ex. les infrastructures à clé publique), devraient bientôt être disponibles, comme mentionné plus haut;
- d) la migration des technologies cryptographiques installées (p. ex. SHA1) vers des technologies plus récentes peut s'échelonner sur plusieurs années⁴;
- e) le nombre de systèmes cryptographiques que les organisations devront faire migrer pour utiliser la nouvelle cryptographie « post-quantique » sera élevé;
- f) la plupart des organisations n'ont pas une vision claire des technologies cryptographiques utilisées par leurs systèmes existants de gestion de l'information (GI), de technologie de l'information (TI) et de technologie opérationnelle (TO); il sera donc difficile de déterminer et de classer en ordre de priorité les systèmes à mettre à niveau vers la cryptographie post-quantique⁵.

Les propriétaires d'entreprises et les exploitants de systèmes auront besoin de temps pour évaluer les efforts qu'ils devront déployer pour migrer leurs systèmes cryptographiques existants afin d'utiliser la nouvelle cryptographie post-quantique. La migration des systèmes cryptographiques d'une organisation vers la CPQ nécessitera des efforts importants. Les organisations devraient commencer à la planifier dès maintenant étant donné que :

- l'effort et le temps nécessaires (p. ex. pour étudier, analyser, planifier, acquérir, migrer et valider la nouvelle CPQ) seront importants et différents pour chaque organisation;
- il restera chaque jour moins de temps (avant que les auteurs malveillants puissent accéder à des ordinateurs quantiques suffisamment puissants pour percer la cryptographie existante).

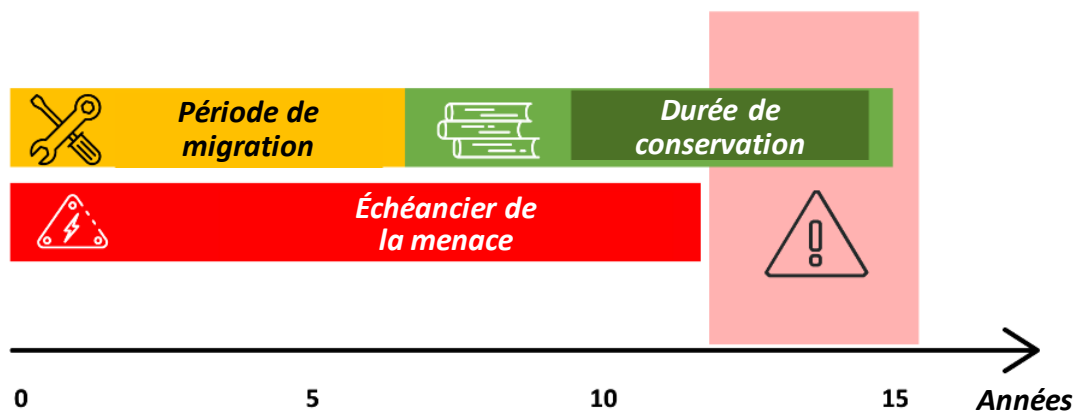
⁴ [The SHA1 hash function is now completely unsafe | Computerworld](#), février 2017.

⁵ [Getting Ready for Post-Quantum Cryptography: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms \(nist.gov\)](#), 28 avril 2021.

1.4 De combien de temps dispose-t-on?

Le temps qu'une organisation devra consacrer à la transition de ses systèmes pour utiliser la nouvelle cryptographie post-quantique (CPQ) dépend de trois facteurs :

- la **période de migration** : le nombre d'années dont l'organisation aura besoin pour faire migrer tous les systèmes qui traitent ses données importantes vers la nouvelle cryptographie post-quantique;
- la **durée de conservation des données** : le nombre d'années pendant lesquelles les renseignements importants et de grande valeur de l'organisation doivent être protégés;
- l'**échéancier de la menace** : le nombre d'années qui s'écouleront avant que les auteurs malveillants ne soient en mesure de percer la cryptographie existante de l'organisation, vulnérable à l'informatique quantique⁶.



Comme illustré ci-dessus :

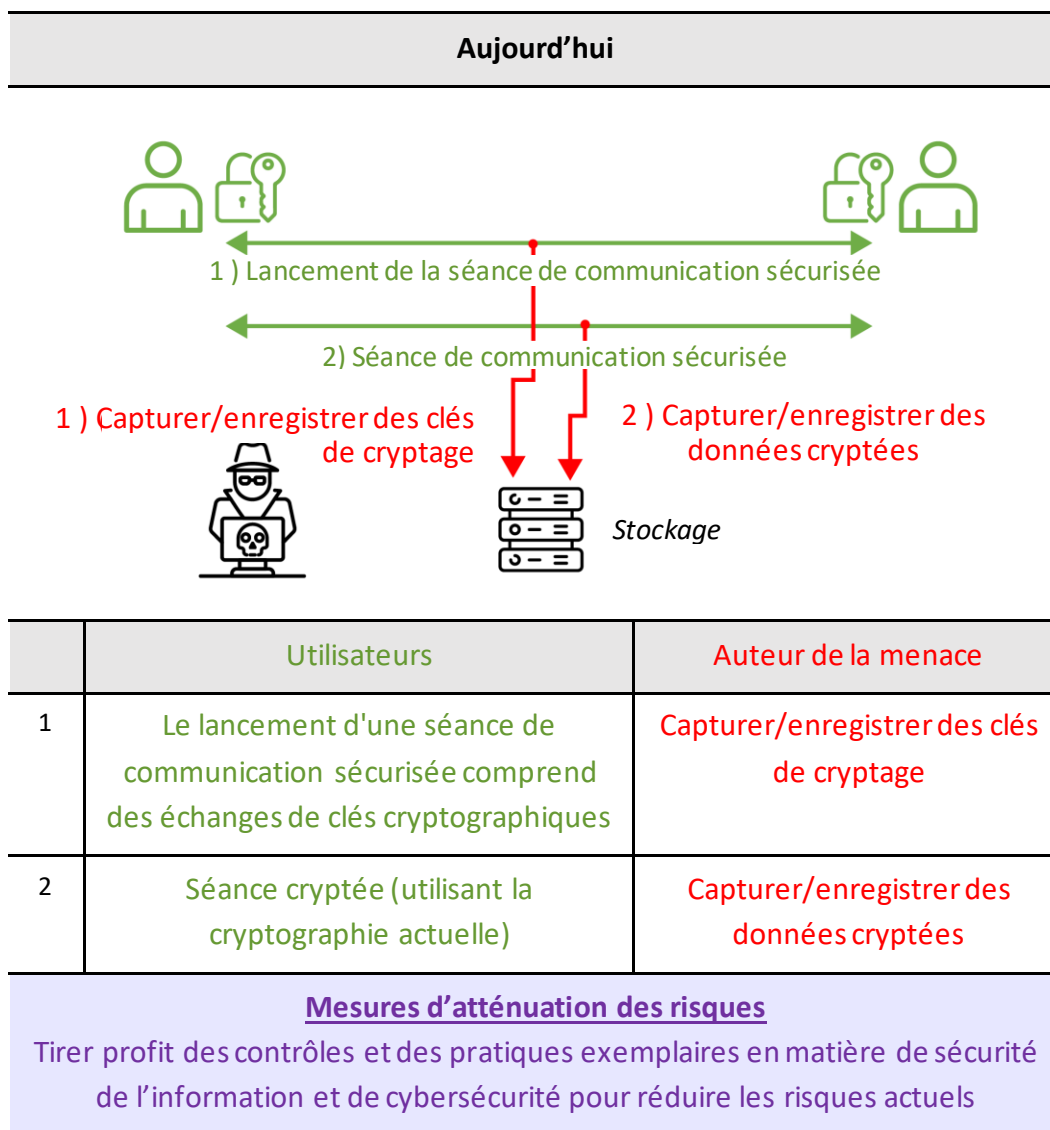
- les organisations peuvent avoir besoin de plusieurs années pour migrer vers la CPQ;
- de nombreuses organisations disposent de renseignements importants (p. ex. des secrets commerciaux, des données sur les clients, des plans d'affaires) qu'elles souhaitent garder confidentiels pendant une longue période.

Dans le pire des cas, un auteur malveillant sera en mesure d'utiliser un ordinateur quantique pour percer le chiffrement protégeant des renseignements importants avant que ces données ne soient protégées par la CPQ.

⁶ [Quantum Threat Timeline Report for 2020](#), Global Risk Institute, 27 janvier 2021.

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

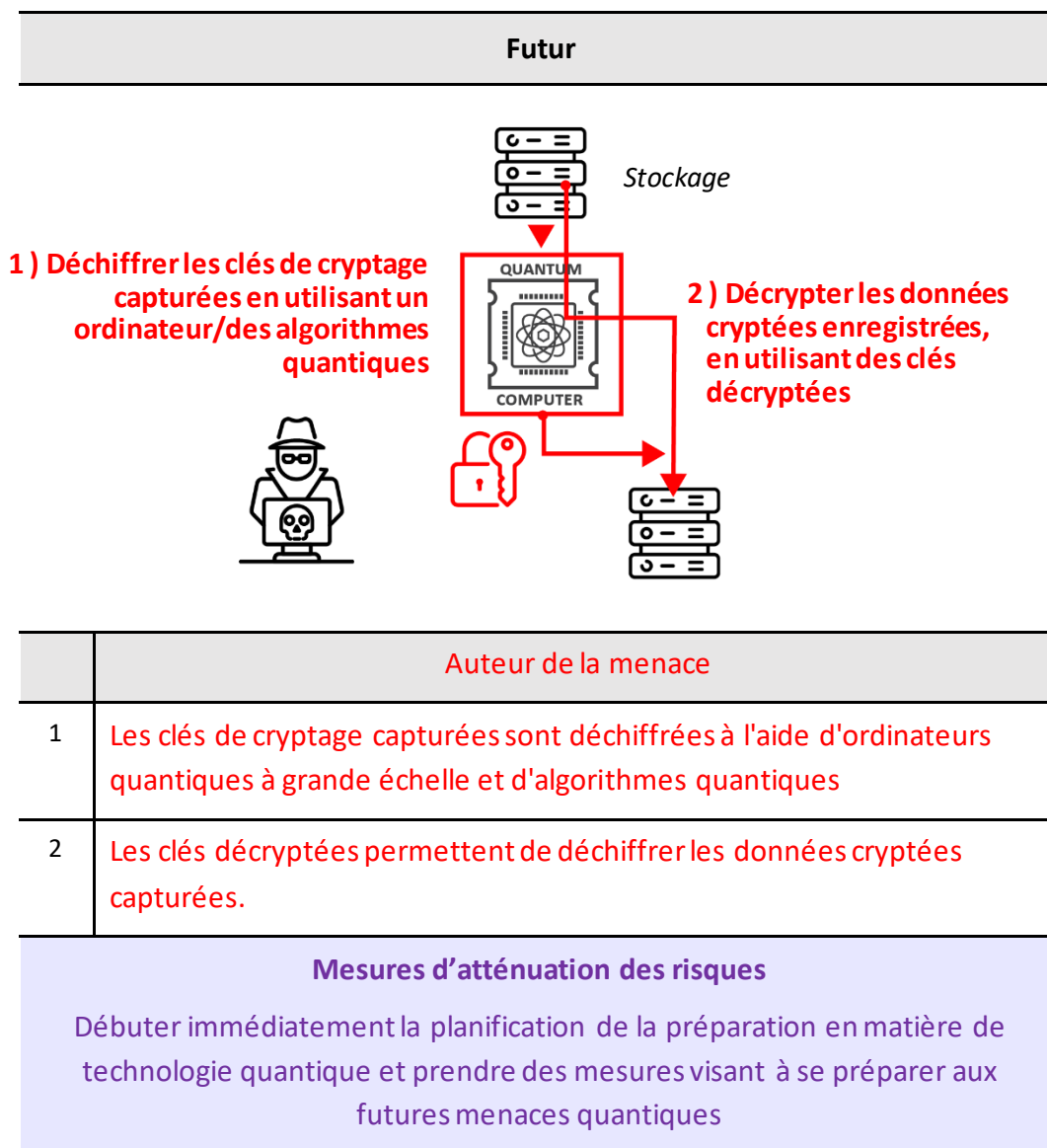
On sait que certains auteurs malveillants (p. ex. des adversaires au niveau des États-nations) récupèrent aujourd’hui des copies de renseignements cryptés et les stockent pour les décrypter plus tard. Ainsi, tout renseignement qui doit rester confidentiel pendant une longue période (plus de 10 ans, par exemple) peut déjà être exposé à des attaques du type « recueillir maintenant, déchiffrer plus tard ». Il convient de noter que la durée de conservation des données et renseignements essentiels, notamment les secrets commerciaux, peut dépasser 50 ans.



Dans le meilleur des cas, les organisations qui commencent à évaluer leur état de préparation en matière de technologie quantique auront le temps de faire migrer leurs systèmes les plus

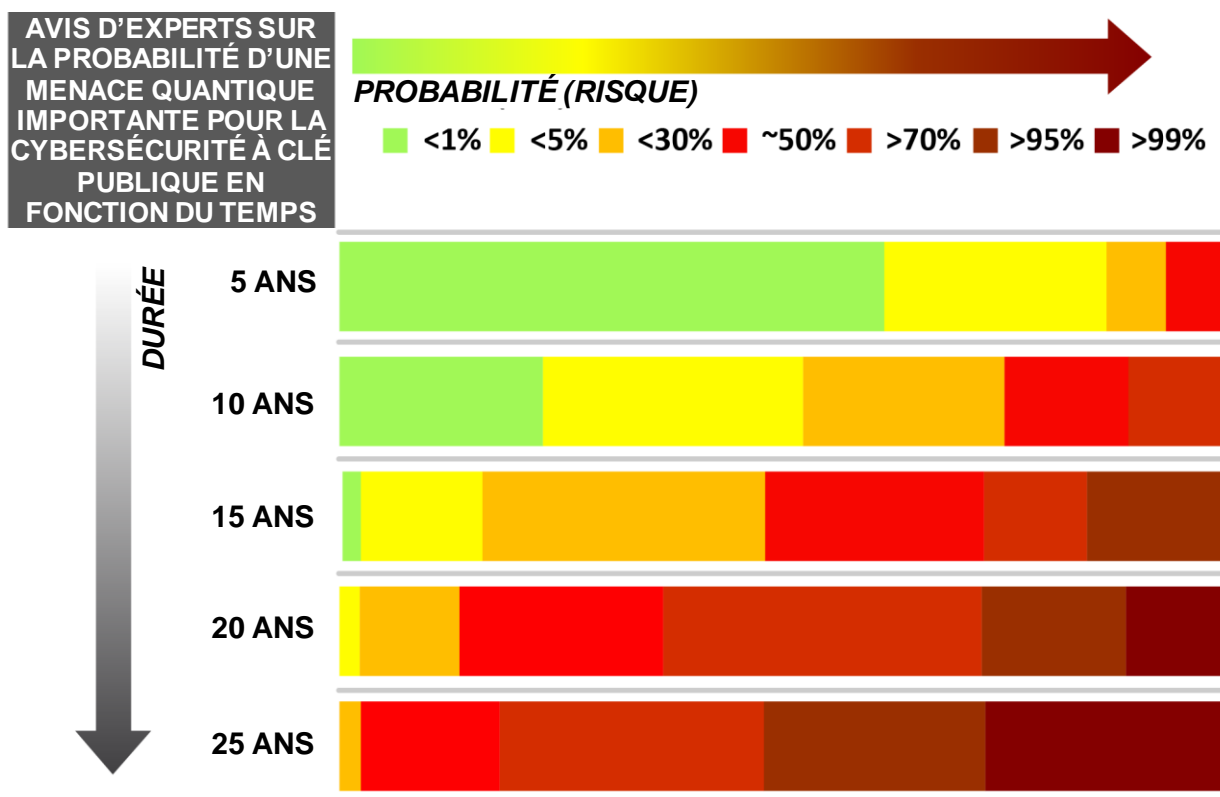
Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

importants pour utiliser une cryptographie post-quantique avant que les auteurs malveillants (et les concurrents commerciaux) n’obtiennent des ordinateurs quantiques.



En ce qui concerne l’échéancier de la menace, la figure ci-dessous résume les avis les plus récents de 44 experts mondiaux en matière d’informatique quantique. Chaque organisation devra examiner des renseignements de ce genre, puis évaluer le temps dont elle dispose, en fonction de sa propre tolérance au risque.

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique



Les chiffres reflètent le nombre d'experts (sur 44) qui ont attribué une certaine plage de probabilité.

[Quantum Threat Timeline Report 2020](#)

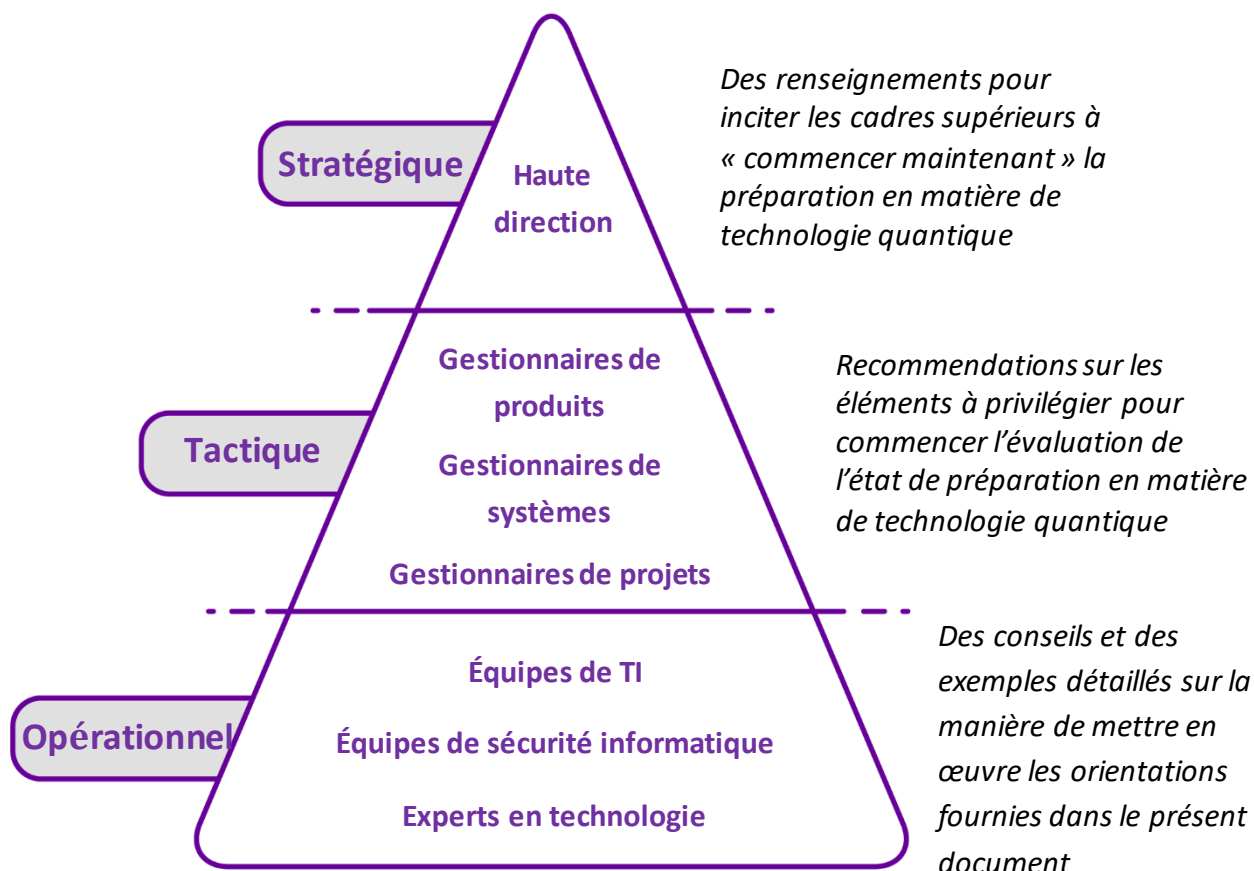
Global Risk Institute, 7 janvier 2021

1.5 À propos du présent document

En juin 2020, le [Forum canadien pour la résilience des infrastructures numériques \(FCRIN\)](#) a chargé son Groupe de travail sur la préparation en matière de technologie quantique (GTPTQ) de mener un projet pilote d'un an sur l'état de préparation en matière de technologie quantique avec des intervenants du secteur des infrastructures essentielles (IE) des finances du Canada. Ce projet comprenait des discussions, des découvertes et un examen approfondi d'un grand nombre de considérations clés dont les cadres supérieurs, leurs subalternes directs et leur personnel de GI, de TI et de TO devront tenir compte pour faire évoluer leurs systèmes cryptographiques existants afin qu'ils soient « post-quantiques » (c'est-à-dire sûrs sur le plan quantique) dans les années à venir.

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

Le présent document, ainsi que la série de diapositives qui l'accompagne, fournit des renseignements et du matériel de base qui peuvent être utilisés et adaptés par les organisations selon leurs besoins pour sensibiliser et informer les décideurs opérationnels et technologiques sur les raisons et les moyens d'entamer leur préparation en matière de technologie quantique.



Le présent document comprend des recommandations stratégiques et tactiques (dans les sections 3 à 5) et des conseils opérationnels (notamment des guides pratiques dans ses annexes).

2. Sources d'information

Les renseignements utilisés pour formuler les pratiques et les lignes directrices recommandées dans le présent document proviennent d'un large éventail de sources dans le domaine public, ainsi que des discussions et délibérations au sein du GTPTQ du FCRIN.

Les sources principales comprennent les suivantes :

- [publications du Centre canadien pour la cybersécurité \(CCC\)](#);
- [publications du Computer Security Resource Center du National Institute of Standards and Technology \(NIST\)](#) des États-Unis sur la sécurité post-quantique;
- les documents du [Groupe de travail sur la cryptographie post-quantique de l'Institut européen des normes de télécommunications \(ETSI\)](#);
- [Demande de commentaires de l'Internet Engineering Task Force \(IETF\)](#), le cas échéant.

S'il y a lieu, dans les sections ultérieures du présent document, des liens vers des publications particulières des sources ci-dessus peuvent être indiqués comme des « références normatives ». Les documents normatifs sont des publications qui doivent être lues pour comprendre ou mettre en œuvre les conseils fournis.

En revanche, d'autres sources mises en évidence dans le présent document sont qualifiées de « références informatives ». Les documents informatifs aident le lecteur à mieux comprendre un sujet en particulier.

Les sources d'information citées dans le présent document sont les suivantes :

- articles de magazines à code source ouvert, articles évalués par des pairs et actes de conférences;
- documents du Fonds monétaire international (FMI) et du Global Risk Institute ;
- webdiffusions de discussions de groupes d'experts et de présentations de conférences pertinentes;
- contenu de source ouverte (p. ex. livres blancs, études de cas, notes d'application) provenant d'entreprises du secteur privé membres du FCRIN, ainsi que d'autres membres de la chaîne d'approvisionnement des technologies de l'information et des communications (TIC) pour des solutions « post-quantiques ».

3. Pratiques exemplaires recommandées pour la préparation en matière de technologie quantique

On encourage les cadres à demander à leur organisation de commencer dès maintenant :

- à comprendre puis à gérer les risques associés aux progrès de l'informatique quantique ;
- à planifier la transition vers une cryptographie post-quantique cryptography.

Les mesures recommandées qui peuvent être mises en œuvre dès maintenant sont les suivantes⁷:

1. Mettre à jour et corriger fréquemment vos systèmes de gestion de l'information (GI), de technologie de l'information (TI) et de technologie opérationnelle (TO).
2. Veiller à ce que vos fournisseurs utilisent une cryptographie normalisée et validée (p. ex. Federal Information Processing Standards [FIPS]).
3. Évaluer la nature délicate des renseignements de votre organisation et déterminer leur durée de vie afin de recenser les renseignements susceptibles d'être à risque (p. ex. dans le cadre des processus d'évaluation continue des risques).
4. Sensibiliser vos équipes à la menace quantique émergente pour la cryptographie existante, ainsi qu'aux futures technologies quantiques.
5. Demander à vos fournisseurs s'ils prévoient de mettre en œuvre une cryptographie post-quantique (p. ex. vos fournisseurs prévoient-ils d'inclure une cryptographie post-quantique dans les futures mises à jour, ou devrez-vous acquérir du matériel ou des logiciels nouveaux?).
6. Prévoir dans votre budget des mises à jour logicielles et matérielles potentiellement importantes, à mesure que les remplacements nécessaires approchent.
7. Mettre à jour vos plans de gestion du cycle de vie de la GI, de la TI et de la TO pour décrire explicitement comment et quand votre organisation mettra en œuvre des algorithmes de cryptographie post-quantique pour protéger vos données et systèmes les plus importants à partir de 2024-2025, ou lorsque des modules cryptographiques validés seront disponibles (p. ex. un an plus tard).

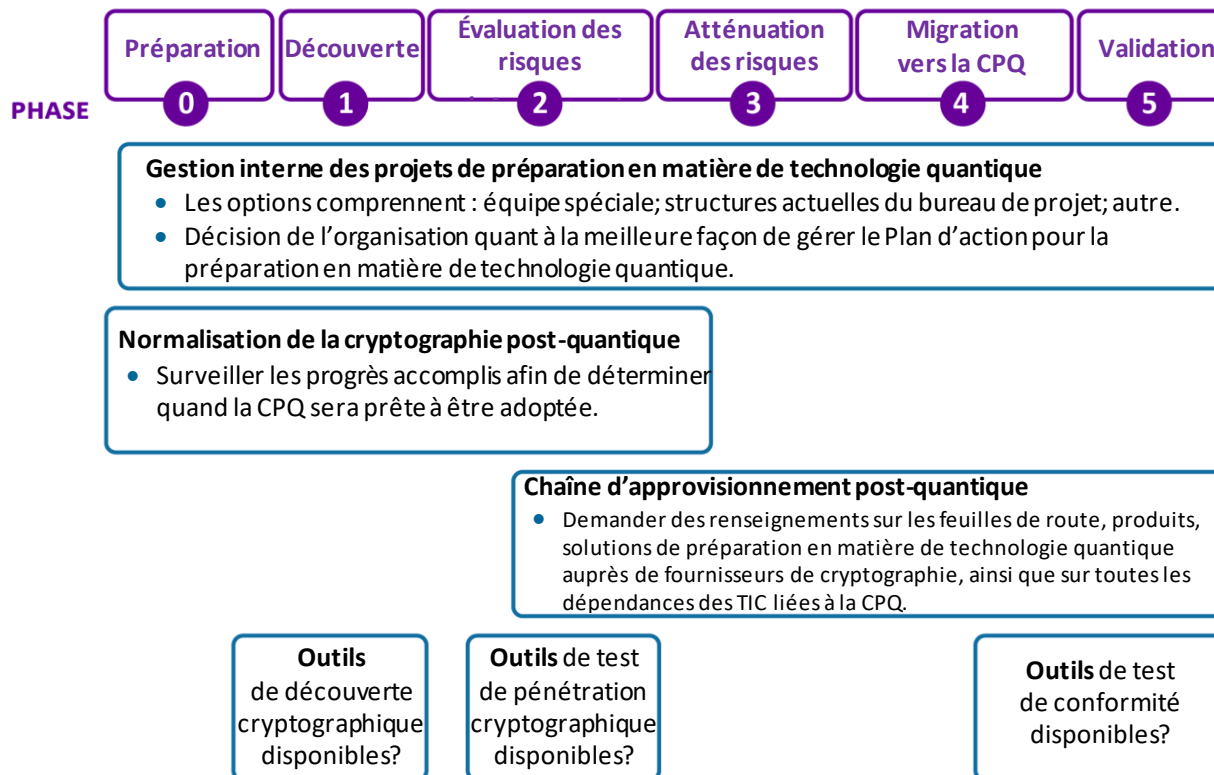
⁷ [Préparer votre organisation à la menace que pose l'informatique quantique pour la cryptographie \(ITSAP.00.017\) – Centre canadien pour la cybersécurité](#), février 2021

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

En ce qui concerne l'organisation des mesures recommandées dans le cadre d'un programme de préparation en matière de technologie quantique, on recommande d'élaborer un calendrier pluriannuel comportant plusieurs phases, comme décrit ci-dessous.

Éléments du programme de préparation en matière de technologie quantique

Quelques blocs fonctionnels conceptuels



Tout en reconnaissant que chaque entreprise est unique et qu'il n'existe pas de solution « universelle », le plan de travail de chaque organisation en matière de préparation en matière de technologie quantique doit suivre les **étapes** et les **phases** de projet suivantes :

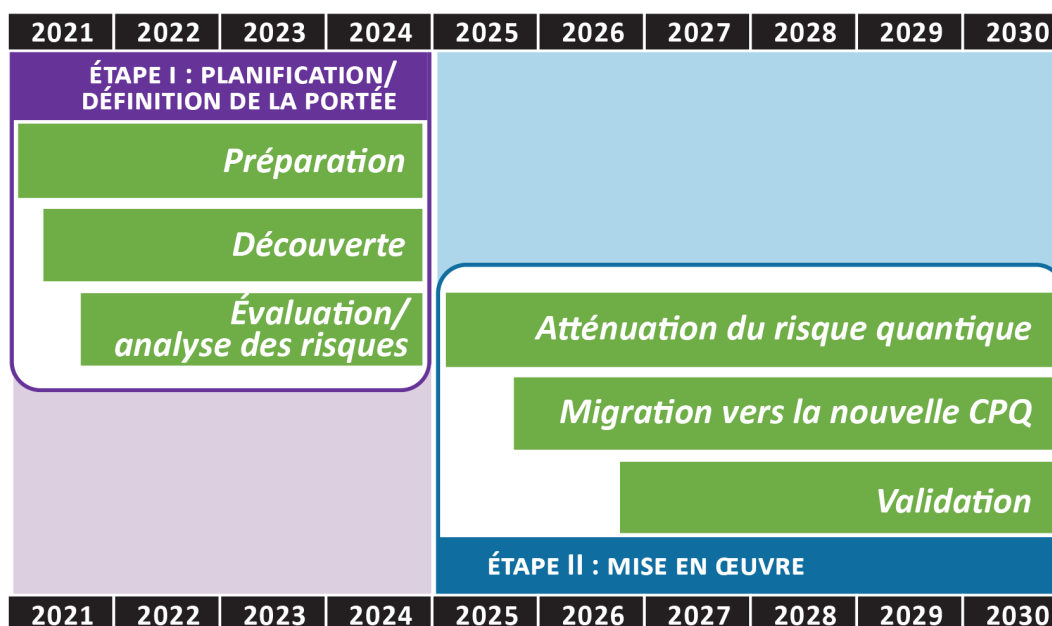
- **Étape I – Planification initiale et définition de la portée**, gérée comme trois phases de projet distinctes qui devraient toutes être bien avancées avant que les normes de la nouvelle cryptographie post-quantique (CPQ) ne soient achevées en 2024 :
 0. Préparation
 1. Découverte
 2. Évaluation des risques quantiques

Lignes directrices et pratiques exemplaires nationales canadiennes
pour la préparation en matière de technologie quantique

- **Étape II – Mise en œuvre**, à partir de 2025, comprenant également trois phases distinctes :
 3. Atténuation des risques quantiques
 4. Migration vers la nouvelle CPQ
 5. Validation

Les participants au projet pilote initial du GTPTQ du FCRIN recommandent d'utiliser le calendrier suivant pour définir les attentes concernant le temps nécessaire pour effectuer une préparation complète en matière de technologie quantique.

Calendrier du programme de préparation en matière de technologie quantique
Recommandations initiales à partir de juin 2021



La durée prévue (en années) pour chaque étape et phase indiquée ci-dessus est le point de vue consensuel des participants au projet pilote initial du GTPTQ du FCRIN avec des membres du secteur des IE des finances du Canada de juillet 2020 à juin 2021.

Dans les sections 3.0 à 3.2 du présent document, on recommande des mesures et des pratiques exemplaires de **planification et de définition de la portée** pour les trois premières phases. Elles décrivent ce qu’une organisation doit faire pour commencer à préparer ses systèmes de GI, de TI et de TO aux nouvelles technologies post-quantiques d’ici 2024.

Les futures versions du présent document offriront des conseils supplémentaires et recommanderont des pratiques exemplaires pour les phases de **mise en œuvre** après 2024.

3.0 Étape I – Préparation (phase 0)

(Recommandations à l'intention des membres de la haute direction)

1. Comprenez les menaces que l'informatique quantique fera peser sur votre infrastructure de TIC dans les années à venir. Demandez une séance d'information dans un délai de six mois.

Références normatives :

- **CCC** : [ITSE.00.017 – Préparer votre organisation à la menace que pose l'informatique quantique pour la cryptographie](#), mai 2020, 1 page
- **NIST**: [Cybersecurity White Paper - Getting Ready for PQC](#), avril 2021, 10 pages

Références informatives :

- NCCoE des États-Unis : [Post-Quantum Cryptography Challenges From a Customer Point of View](#), septembre 2020, webinaire de 18 minutes
- NCCoE des États-Unis : [The Long and Agile Transition – How Industry Needs to Prepare](#), septembre 2020, webinaire de 14 minutes

2. Demandez à un ou plusieurs membres de votre personnel de former une équipe chargée d'évaluer les efforts qu'il faudra déployer pour que votre organisation commence à utiliser une nouvelle cryptographie « post-quantique » dans les années à venir, et de déterminer les systèmes de GI, de TI et de TO qui devront être corrigés en premier.

Références normatives :

- **CCC** : [ITSE.00.017 – Préparer votre organisation à la menace que pose l'informatique quantique pour la cryptographie](#), février 2021, 2 pages
- **ETSI**: [TR 103 619 - V1.1.1 - CYBER; Migration strategies and recommendations to Quantum Safe schemes \(etsi.org\)](#) juillet 2020, 21 pages

Références informatives :

- CCC : [ITSB-127 Atténuation obligatoire des menaces liées à l'informatique quantique au GC \(cyber.gc.ca\)](#), mai 2019, 4 pages
- ETSI, IQC: [Quantum readiness and resilience of the digital economy | TelecomTV](#) octobre 2020, webinaire de 27 minutes en groupe d'experts

3. Demandez des rapports périodiques sur l'avancement du point no 2 (p. ex. tous les trimestres) et décidez quand passer à la phase 1 (découverte), comme décrit à la section 3.1 du présent document.

Référence informative :

- Internet Society: [Cryptography: CEO Questions for CTOs](#), mars 2018, 15 pages

4. Envoyez un courriel au [secrétariat du FCRIN](#) pour toute question sur les points abordés ci-dessus.

3.1 Étape I – Découverte (phase 1)

(Recommandations à l'intention des membres de la haute direction et de leurs subalternes directs)

5. Passez en revue les renseignements à recueillir au cours de cette phase, comme l'illustre le schéma à la page suivante.
 - L'objectif est de découvrir où et comment les produits, algorithmes et protocoles cryptographiques sont utilisés par votre organisation pour protéger la confidentialité et l'intégrité de ses données importantes et de ses systèmes numériques.
 - Les renseignements recueillis au cours de cette phase permettront d'évaluer les risques quantiques de votre organisation au cours de la phase 2.
6. Nommez une personne et autorisez-la à planifier et à effectuer une découverte détaillée de l'endroit et de la manière dont la cryptographie à clé publique est utilisée par votre organisation.

Référence informative :

- Forbes Technology Council: [Three Practical Steps To Prepare Your Business For The Quantum Threat](#) 8 janvier 2021, 5 pages

7. Vérifiez si l'utilisation d'outils automatisés faciliterait votre découverte cryptographique. Les organisations doivent trouver un juste équilibre entre leurs besoins en matière de sécurité et leurs besoins en matière de convivialité et de disponibilité lorsqu'elles envisagent d'utiliser de tels outils automatisés.

Références informatives :

- NIST: [Migration to Post-Quantum Cryptography - Project Description](#), juin 2021, pages 4-5
- NIST: [Guide to Enterprise Patch Management Technologies](#), juillet 2013, 26 pages
- Forbes Technology Council: [Building a Strong Cryptography Strategy \(Part I\): Securing Your Data Assets](#), 20 avril 2021, 3 pages

8. Dressez un inventaire des endroits et des façons dont votre organisation utilise la cryptographie à clé publique pour protéger ses données les plus importantes et ses systèmes de GI, de TI et de TO. Déterminez également tout système cryptographique existant utilisé.

Références normatives :

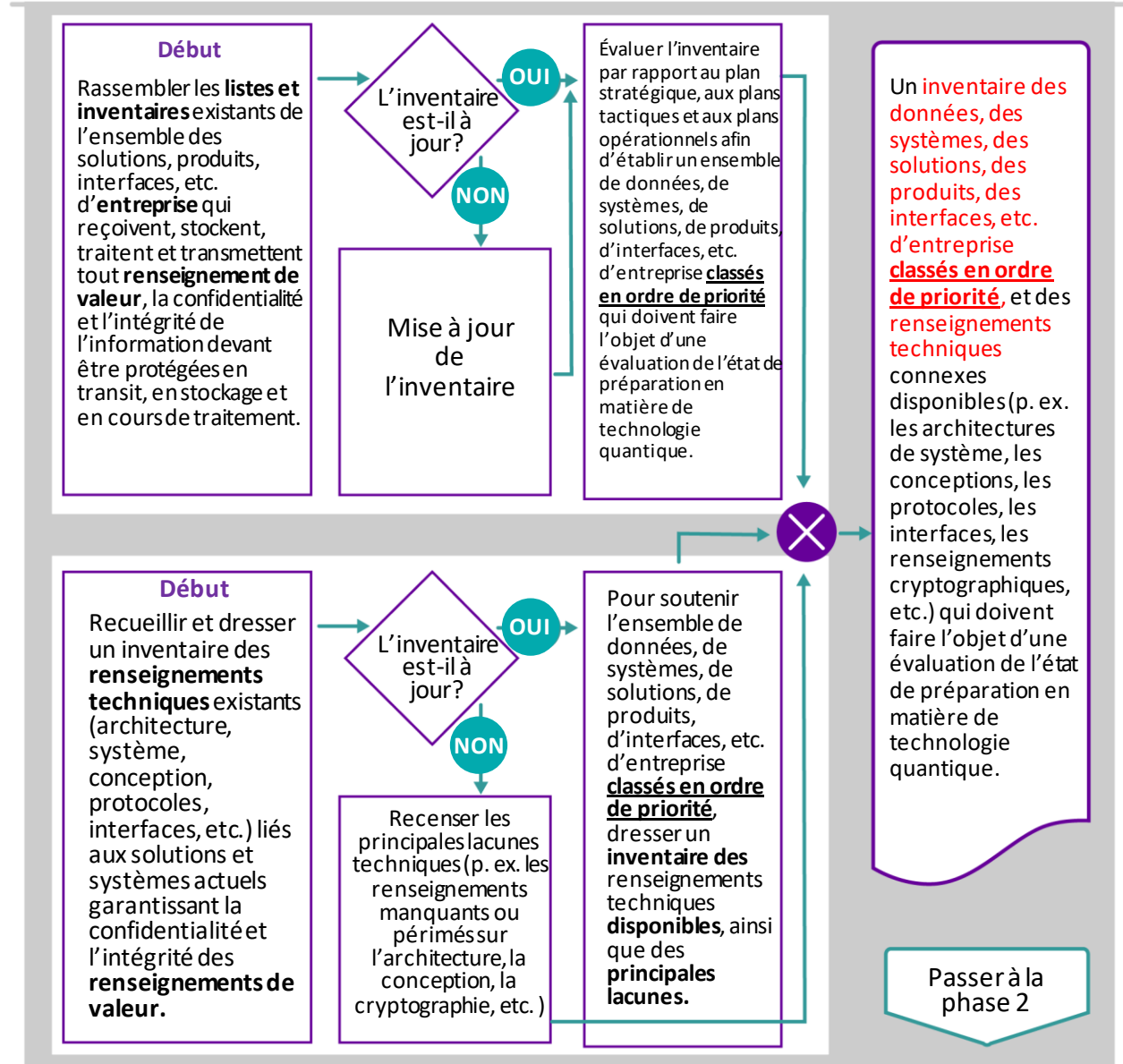
- **ETSI**: [TR 103 619 – V1.1.1 – CYBER; Migration strategies and recommendations to Quantum Safe schemes](#), juillet 2020, pages 7-10

Références informatives :

- Cryptosense Blog: [What is Cryptographic Inventory?](#), 2 août 2019
- Cryptosense Blog: [Cryptographic Inventory – Best Practice Tips](#), 3 juin 2020

Lignes directrices et pratiques exemplaires nationales canadiennes
pour la préparation en matière de technologie quantique

Phase 1 : Schéma de processus : découverte



9. Recensez les facteurs importants permettant de comprendre pourquoi la cryptographie à clé publique affecte le fonctionnement et la sécurité de vos systèmes et applications (p. ex. la taille des clés, les limites de latence et de débit, les protocoles actuels d'établissement des clés, la manière dont chaque processus cryptographique est invoqué, les dépendances).

Références normatives :

- **GTPTQ du FCRIN :** [Contenu nécessaire pour décrire les utilisations de la cryptographie par une organisation](#), annexe C du présent document

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

- **GTPTQ du FCRIN** : [Utilisation de Kerberos pour l'authentification](#), annexe D du présent document
- **GTPTQ du FCRIN** : [ICP/AC](#), annexe E du présent document
- **GTPTQ du FCRIN** : [sFTP](#), annexe F de présent document

Références informatives :

- NIST: [Getting Ready for Post-Quantum Cryptography](#) Cybersecurity White Paper, 28 avril 2021, page 5

10. Analysez les résultats des points 8 et 9 pour établir une liste de priorités des systèmes les plus importants de votre organisation qui sont vulnérables à l'informatique quantique et qui doivent être protégés.

Référence informative :

- CCC: [ITSE.00.017 – Préparer votre organisation à la menace que pose l'informatique quantique pour la cryptographie](#), février 2021, 2 pages

3.2 Étape 1 – Évaluation des risques quantiques (phase 2)

(Recommandations à l'intention des gestionnaires de la GI, de la TI et de la TO et de leurs subalternes directs)

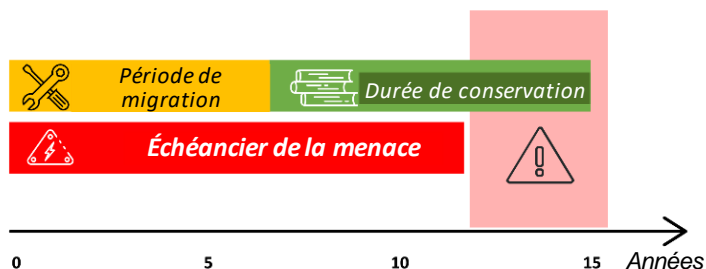
11. Passez en revue les objectifs de cette phase du processus de préparation en matière de technologie quantique, comme l'illustre le schéma à la page suivante.

Les objectifs sont les suivants :

- Évaluer la nature délicate des renseignements de votre organisation et déterminer leur durée de vie afin de recenser ceux qui peuvent être à risque (p. ex. dans le cadre des processus d'évaluation continue des risques).
- Vous informer et informer vos équipes sur les menaces que l'informatique quantique fera peser sur vos utilisations actuelles de la cryptographie.
- Demander à vos fournisseurs de systèmes de GT, de TI et de TO quels sont leurs plans et calendriers pour mettre en œuvre une cryptographie post-quantique et une cryptoagilité, afin de comprendre tout nouveau matériel ou logiciel qui sera nécessaire.
- Passer en revue vos plans de gestion du cycle de vie des TI et préparer un budget pour les mises à jour logicielles et matérielles potentiellement importantes.

12. Commencez votre évaluation des risques quantiques en examinant l'équation du risque quantique présentée à la section 1.4, ainsi que l'inventaire des renseignements découverts lors de la phase 1. Ces renseignements sont nécessaires pour déterminer les variables suivantes pour chacun des systèmes numériques qui traitent ou stockent les renseignements les plus délicats de votre organisation :

- la **durée de conservation** (mesurée en années) pendant laquelle vos données les plus importantes doivent être protégées;
- le **période de migration** (mesurée en années) dont votre organisation aura besoin pour mettre à niveau les systèmes qui traitent vos données à durée de vie la plus longue pour qu'ils soient à résistance quantique.

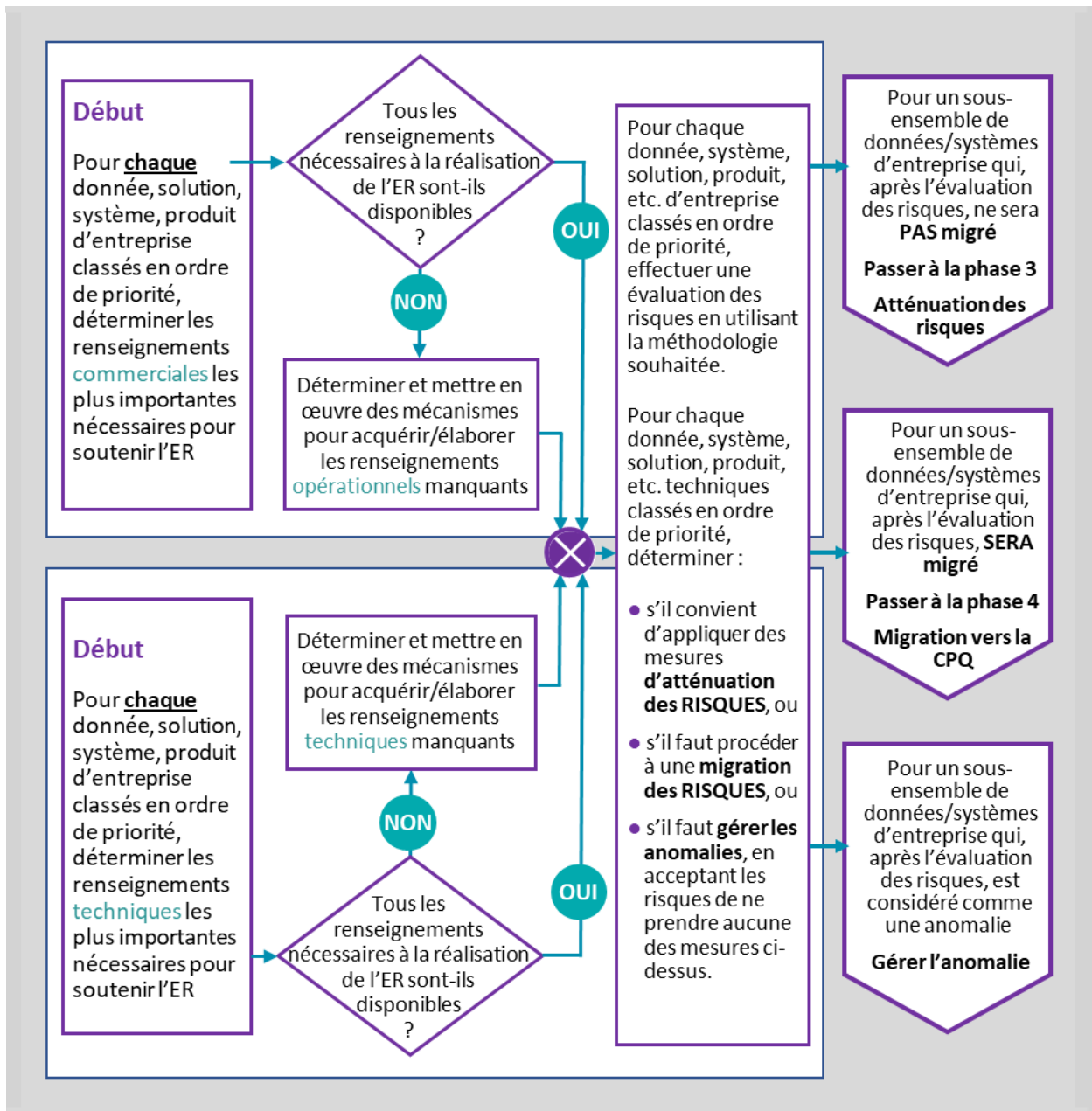


Référence normative :

- **evolutionQ**: [Managing the quantum risk to cybersecurity](#), 11 avril 2016, pages 16-20

Lignes directrices et pratiques exemplaires nationales canadiennes
pour la préparation en matière de technologie quantique

Phase 2 : Schéma de processus : évaluation des risques (ER)



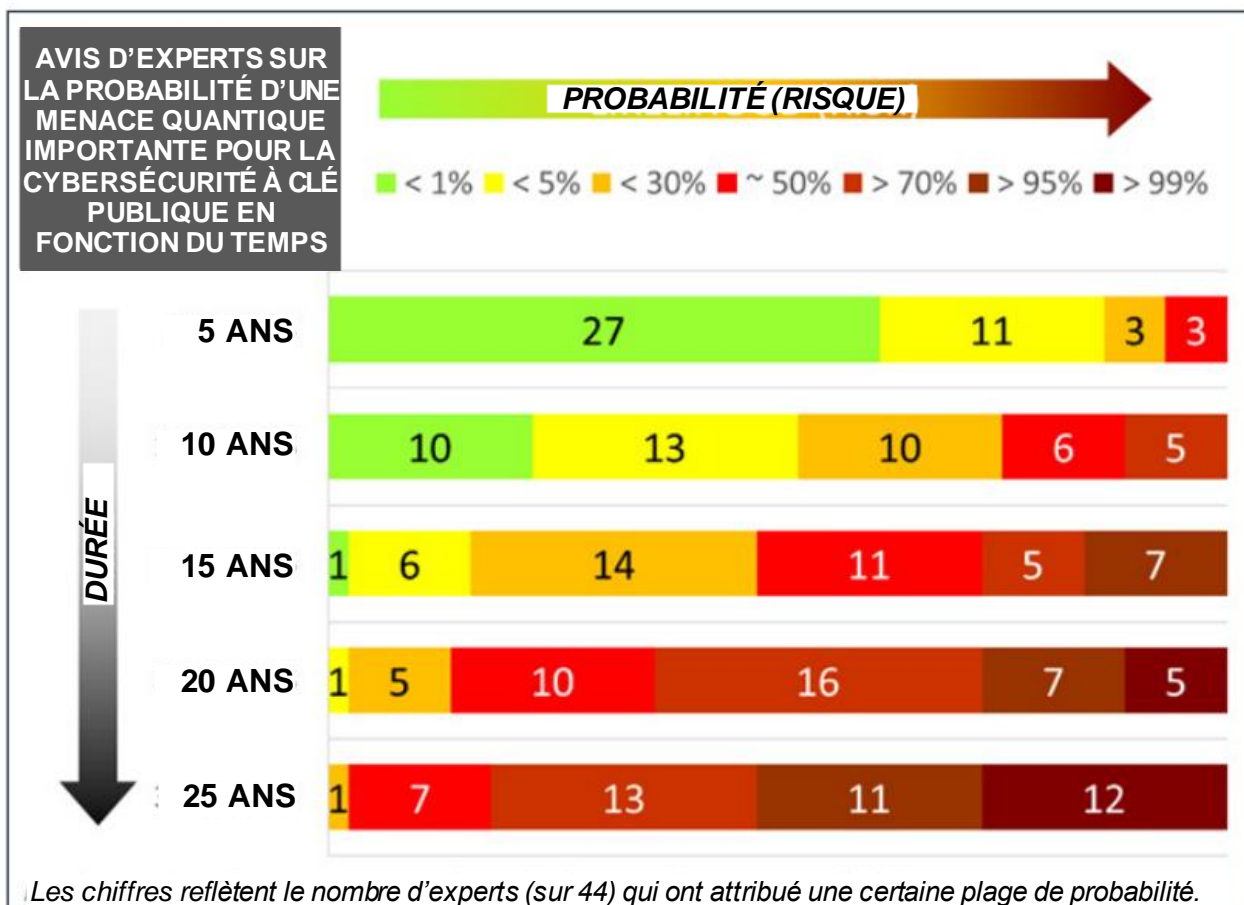
13. Déterminez comment l'**échancier de la menace** quantique actuellement prévu affecte la posture de risque de votre organisation. Pour ce faire, examinez les renseignements de

Lignes directrices et pratiques exemplaires nationales canadiennes
pour la préparation en matière de technologie quantique

source ouverte, notamment ceux qui suivent, puis déterminez votre échéancier de la menace en fonction de votre tolérance au risque.

Référence normative :

Global Risk Institute: [Quantum Threat Timeline Report 2020](#), janvier 2021, 52 pages



- Évaluez la nature délicate des renseignements de votre organisation et déterminez leur durée de vie (c'est-à-dire la **durée de conservation** de vos données les plus importantes qui doivent être protégées) afin de recenser ceux qui peuvent être à risque.

Référence normative :

- CCC: [ITSE.00.017 – Préparer votre organisation à la menace que pose l'informatique quantique pour la cryptographie](#), février 2021, page 2

- Passez en revue vos plans de gestion du cycle de vie technologique pour chacun des systèmes vulnérables à l'informatique quantique déterminés à l'étape 10 de la phase 1. Demandez à vos fournisseurs de systèmes de GI, de TI et de TO si leurs plans de développement de produits prévoient la prise en charge de la cryptoagilité et/ou de la

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

cryptographie post-quantique dans les futures mises à jour. Si tel est le cas, demandez quand ces capacités seront disponibles.

Référence normative :

- **CCC:** [ITSE.00.017 – Préparer votre organisation à la menace que pose l'informatique quantique pour la cryptographie](#), février 2021, page 2

16. À l'aide des renseignements du point 15, estimez la **période de migration** (mesurée en années) dont votre organisation aura besoin pour migrer chacun des systèmes qui traitent vos données ayant la plus longue durée de vie.

Référence informative :

- NIST: [Migration to Post-Quantum Cryptography - Project Description](#) juin 2021, page 6, lignes 197-216

17. Classez en ordre de priorité les systèmes qui nécessiteront l'attention la plus urgente, en énumérant tous les systèmes qui traitent des données importantes pour lesquels :

période de migration + durée de conservation > échéancier de la menace

Référence informative :

- Journal of Cybersecurity: [Crypto Agility Risk Assessment Framework](#) 30 avril 2021, pages 5-9

18. Pour chacun des ensembles de données, produits, systèmes ou solutions indiqués au point 17, déterminez :

- s'il faut procéder à l'atténuation des risques (selon la phase 3);
- s'il faut commencer la migration vers la CPQ (selon la phase 4); ou
- gérer les anomalies, en acceptant le risque quantique et en ne prenant aucune des mesures précédentes.

Références informatives :

- **Boston Consulting Group:** [Ensuring Online Security in a Quantum Future](#), mars 2021, 11 pages
- NIST: [Migration to Post-Quantum Cryptography - Project Description](#), juin 2021, lignes 130-155

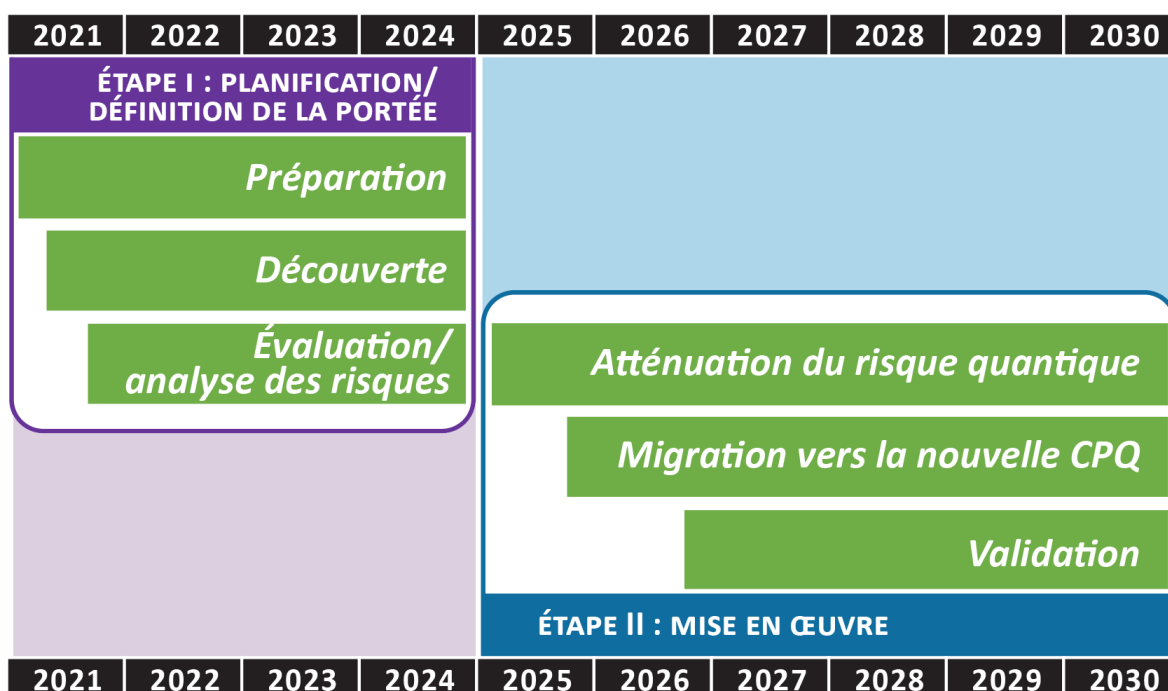
19. Déterminez également si votre personnel aura besoin d'une nouvelle formation ou de ressources supplémentaires (p. ex. des outils) pour migrer vos systèmes afin d'utiliser une cryptographie post-quantique sûre. Si tel est le cas, le temps nécessaire pour obtenir ces outils et/ou cette formation doit être pris en compte dans l'estimation de la période de migration par système établie au point 16.

3.3 Étape II – Phases de mise en œuvre 3, 4 et 5

Les futures versions du présent document offriront des conseils et des recommandations de pratiques exemplaires pour les trois phases de **mise en œuvre** après 2024, à savoir :

- atténuation des risques quantiques (phase 3);
- migration vers une nouvelle cryptographie post-quantique (phase 4);
- validation (phase 5)

Quantum-Readiness Program Timeline
Initial Recommendations as of June 2021



The Le deuxième projet d’une durée de 12 mois du GTPTQ du FCRIN, qui se déroulera de juillet 2021 à juin 2022, orientera la mise en œuvre des mesures ci-dessus, tout comme les initiatives pertinentes menées dans d’autres territoires. Par exemple, en juin 2021, le National Cybersecurity Center of Excellence (NCCoE) des États-Unis, au sein du NIST, a invité le public à commenter une ébauche de description de projet pour la **migration vers la cryptographie post-quantique**⁸. Voir l’annexe C pour de plus amples renseignements.

⁸ [Migration to Post-Quantum Cryptography – Project Description](#), NIST, 4 juin 2021, 16 pages

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

D'autres travaux seront pris en compte dans la prochaine version du présent document, notamment les publications de l'Agence de l'Union européenne pour la cybersécurité (ENISA) et de l'Internet Engineering Task Force (IETF).

En mai 2021, l'ENISA a mis à jour son rapport intitulé **Post-Quantum Cryptography – Current state and quantum mitigation**⁹ afin d'introduire deux options à court terme pour la mitigation quantique :

Si vous chiffrez des données qui doivent rester confidentielles pendant plus de 10 ans et qu'un auteur malveillant pourrait avoir accès au texte chiffré, vous devez prendre des mesures dès maintenant pour protéger vos données.

La première option serait d'effectuer dès maintenant une migration vers des applications dites hybrides qui utilisent une combinaison de schémas pré-quantiques et post-quantiques.

La deuxième option consiste à mettre en œuvre une mesure facile à concevoir, mais compliquée à organiser, c'est-à-dire intégrer des clés pré-partagées dans toutes les clés établies par cryptographie à clé publique.

En avril 2021, l'IETF a décidé de réorganiser l'un de ses groupes de travail, car les progrès récents dans le développement des ordinateurs quantiques constituent une menace pour les algorithmes à clé publique déployés à grande échelle¹⁰.

L'une des ébauches de norme Internet en cours d'élaboration au sein du groupe de travail LAMPS de l'IETF est particulièrement pertinente :

Pendant la transition vers la cryptographie post-quantique, la force des algorithmes cryptographiques suscitera de l'incertitude; nous ne ferons plus entièrement confiance à la cryptographie traditionnelle, p. ex. RSA, Diffie-Hellman, DSA et leurs variantes à courbe elliptique, mais nous ne ferons pas non plus entièrement confiance à leurs solutions post-quantiques de rechange tant qu'elles n'auront pas été suffisamment examinées.

Contrairement aux précédentes migrations d'algorithmes cryptographiques, le choix du moment de la migration et des algorithmes vers lesquels migrer n'est pas aussi clair. Même après la période de migration, il peut être avantageux pour l'identité cryptographique d'une entité d'être composée de plusieurs algorithmes à clé publique.

[Composite Keys and Signatures for Use In Internet PKI](#)

Groupe de travail LAMPS de l'IETF, janvier 2021

⁹ https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation/at_download/fullReport, mai 2021, pages 25-27.

¹⁰ [Charte du groupe de travail LAMPS de l'IETF, v.06](#), mai 2021, section 5

4. Sensibilisation et perfectionnement des compétences

Dans les années à venir, il sera important pour toutes les organisations qui utilisent la cryptographie, grandes ou petites, de créer un programme efficace de sensibilisation au risque quantique.

Le GTPTQ du FCRIN a élaboré une série de diapositives pour fournir des renseignements et du matériel de base qui peuvent être utilisés et adaptés par les organisations selon leurs besoins pour sensibiliser et informer les décideurs et le personnel sur les raisons et les moyens d'entamer leur préparation en matière de technologie quantique. Ces diapositives peuvent être obtenus en envoyant un e-mail au [Secrétariat du FCRIN](#).

	Contenu et objectif	Nombre de diapositives	Version et date
1	Introduction et contexte	5	Version 01 - 7 juillet 2021
2	Présentation principale	62	Version 01 - 7 juillet 2021
3	Sous-ensemble de la présentation principale exemple n° 1 – Guide du dirigeant	2	Version 01 - 7 juillet 2021
4	Sous-ensemble de la présentation principale exemple n° 2 – Aperçu général	8	Version 01 - 7 juillet 2021
5	Sous-ensemble exemple n°3 – Aperçu général avec diapos d'appoint	34	Version 01 - 7 juillet 2021
6	Sous-ensemble exemple n°4 – Aperçu détaillé pour les gestionnaires	32	Version 01 - 7 juillet 2021
7	Sous-ensemble exemple n°5 – Aperçu détaillé pour les gestionnaires avec diapos d'appoint	60	Version 01 - 7 juillet 2021
8	Sous-ensemble exemple n°6 – Aperçu détaillé pour les responsables de la mise en œuvre	56	Version 01 - 7 juillet 2021

5. Mobilisation des fournisseurs

Les prochaines versions du présent document offriront des conseils et des pratiques exemplaires pour les sous-sections énumérées ci-dessous.

5.1 Questions recommandées pour mobiliser un fournisseur de CPQ

5.2 Clauses d'approvisionnement concernant la CPQ pour les demandes de renseignements (DDR) et les demandes de propositions (DDP)

6. Conclusion/principaux points à retenir

- On conseille aux entreprises et aux organisations canadiennes, ainsi qu'aux propriétaires et aux exploitants d'infrastructures essentielles, de prendre des mesures dès maintenant, en utilisant les pratiques et les lignes directrices recommandées dans le présent document, afin de commencer à planifier une transition ordonnée et rentable vers la cryptographie post-quantique au cours des prochaines années pour gérer les risques que les ordinateurs quantiques leur feront courir.

Risques	
Menace de cyberattaque	<ul style="list-style-type: none">• Capturer maintenant; rejouer et décrypter plus tard• Données inactives/données en transit
Données clés en danger	<ul style="list-style-type: none">• Clés de cryptage; renseignements permettant d'identifier une personne (RIP); « bijoux » de l'entreprise; propriété intellectuelle
Portée du risque	<ul style="list-style-type: none">• Organisation; clients; chaîne d'approvisionnement; écosystèmes; dépendances/interdépendances

Évaluation des risques liés à la préparation en matière de technologie quantique de l'organisation pour aider à déterminer le risque

- Étant donné que chaque organisation est unique, il n'existe pas d'approche « universelle ».
- Il faut commencer dès maintenant la planification de la préparation en matière de technologie quantique, car la migration des systèmes vulnérables à l'informatique quantique d'une organisation vers l'utilisation d'une nouvelle CPQ s'échelonnera sur plusieurs années.
- La rétrocompatibilité et l'interopérabilité entre les plateformes, systèmes et solutions cryptographiques actuels et nouveaux seront essentielles pendant la transition pluriannuelle vers la CPQ.

Lignes directrices et pratiques exemplaires nationales canadiennes
pour la préparation en matière de technologie quantique

Cryptographie	
Découverte	<ul style="list-style-type: none"> • 1^{re} étape clé : obtenir une mise à jour précise de l'utilisation, des produits et des systèmes cryptographiques de l'organisation
Préparation en matière de technologie quantique	<ul style="list-style-type: none"> • Stratégies, plans et mesures pour mettre à niveau/remplacer les fonctions cryptographiques
Cryptoagilité	<ul style="list-style-type: none"> • Souplesse pour tirer profit des fonctions cryptographiques post-quantiques approuvées par des normes

Les organisations doivent se préparer à mettre à niveau ou à remplacer toutes les fonctions cryptographiques par une cryptographie post-quantique approuvée par des normes

- Les organisations doivent tirer profit de toutes les ressources d'information disponibles sur les sujets abordés plus haut, notamment les suivantes :
 - les recommandations présentées dans le présent document;
 - des experts commerciaux et techniques internes;
 - des renseignements de source ouverte
 - l'expertise et/ou les entreprises canadiennes et multinationales du secteur privé possédant une expérience et des compétences ou des produits liés à la préparation en matière de technologie quantique.

Ressources	
CFDIR Quantum-Readiness WG	<ul style="list-style-type: none"> • Quantum-Readiness Best Practices and Guidelines
CCC	<ul style="list-style-type: none"> • Publications du Centre canadien pour la cybersécurité
Chaîne d'approvisionnement cryptographique canadienne	<ul style="list-style-type: none"> • Chaîne d'approvisionnement canadienne en produits et services cryptographiques

Ressources canadiennes et mondiales disponibles pour aider les organisations à se préparer en matière de technologie quantique

Annexe A : Glossaire

- AC - Autorité de certification
- AFM - Authentification à facteurs multiples
- CCC - Centre canadien pour la cybersécurité
- CPQ - Cryptographie post-quantique
- DECT - Digital Enhanced Cordless Telecommunications (télécommunications numériques sans fil améliorées)
- ENISA - Agence de l'Union européenne pour la cybersécurité
- FCRIN - Forum canadien pour la résilience des infrastructures numériques
- FIPS - Federal Information Processing Standard (É.-U.)
- GI - Gestion de l'information
- GTPTQ - Groupe de travail sur la préparation en matière de technologie quantique
- HSM - Module de sécurité matériel
- ICP - Infrastructure à clés publiques
- IdO - Internet des objets
- IE - Infrastructure essentielle
- IETF - Internet Engineering Task Force
- IKE - Échange de clés Internet
- IPsec - Sécurité du protocole Internet
- ISO - Organisation internationale de normalisation
- Kerberos - Protocole d'authentification des réseaux informatiques permettant la communication entre serveurs sur un réseau non sécurisé
- LDAP - Protocole LDAP (Lightweight Directory Access Protocol)
- mTLS - Authentification mTLS (Mutual Transport Layer Security)
- NCCoE - National Cybersecurity Center of Excellence (É.-U.)
- NIST - National Institute of Standards and Technology (É.-U.)
- Oauth - Norme ouverte pour la délégation d'accès
- PGP - Logiciel Pretty Good Privacy
- RIP - Renseignements permettant d'identifier une personne
- S/MIME - Protocole MIME
- SAML - Security Assertion Markup Language
- sFTP - Protocole sFTP
- SHA1 - Algorithme de hachage sécurisé version 1
- SSH - Secure Shell
- TI - Technologie de l'information
- TLS - Protocole TLS
- TLP - Protocole TLP
- TO - Technologie opérationnelle

Annexe B : Cas d'utilisation recommandés de la cryptographie à découvrir et à documenter

La présente annexe contient une liste de protocoles technologiques et de cas d'utilisation plus généraux de la cryptographie de la GI/TI applicables à la plupart des organisations et entreprises publiques et privées du Canada.

Protocoles communs :

- | | |
|----------|----------------|
| 1) TLS | 10) Kerberos |
| 2) mTLS | 11) LDAPS |
| 3) sFTP | 12) PGP |
| 4) FTPS | 13) WiFi/WPA |
| 5) SSH | 14) S/MIME |
| 6) SAML | 15) DECT |
| 7) OAuth | 16) NEC mobile |
| 8) IPsec | 17) DNSsec |
| 9) IKE | |

Points dont il faut tenir compte dans les cas d'utilisation plus généraux de la cryptographie :

- A. Signature du code
- B. Authentification à facteurs multiples (AFM)
- C. Chiffrement des données inactives – peut être propre au fournisseur
- D. Chiffrement infonuagique
- E. Modules de sécurité matériel (HSM)
- F. Autorités de certification (AC)
- G. Chiffrement des données utiles de la couche d'application

Annexe C : Contenu nécessaire pour décrire les utilisations de la cryptographie par une organisation

La présente annexe fournit une liste des renseignements qui doivent être obtenus puis regroupés lorsqu'une organisation souhaite répertorier la cryptographie sur laquelle elle s'appuie pour l'un des cas d'utilisation énumérés à l'annexe B. Il convient d'élaborer ces renseignements au cours de la phase 1 – Découverte.

Le contenu à répertorier selon les points 1 à 10 (ci-dessous) décrira « l'état actuel » d'un ou de plusieurs systèmes de GI, TI et/ou TO existants d'une organisation.

1. Description du cas d'utilisation
2. Valeur opérationnelle
3. Données opérationnelles potentielles dans la portée/volume de ces données/durée de vie de ces données
4. Catégorie de cas d'utilisation (p. ex. données en transit, données inactives, données en cours de traitement, signature numérique)
5. Considérations techniques et menaces
6. Types de cryptographie actuellement utilisés
7. Composants techniques (p. ex. terminaux, réseaux, bases de données, serveurs de fichiers)
8. Emplacement des renseignements cryptographiques (p. ex. bibliothèque de liens dynamiques, matériel)
9. Dépendances techniques (p. ex. détails sur les composants de ce cas d'utilisation qui dépendent d'autres systèmes pour leur propre sécurité)
10. Capacité de prendre en charge simultanément des algorithmes cryptographiques (pré et post-quantiques)

Une fois les renseignements ci-dessus recueillis, leur analyse permettra de planifier « ce qu'il faut faire pour réduire le risque quantique » au cours des phases ultérieures du projet (p. ex. l'évaluation du risque quantique, l'atténuation du risque quantique, la migration vers une CPQ), notamment :

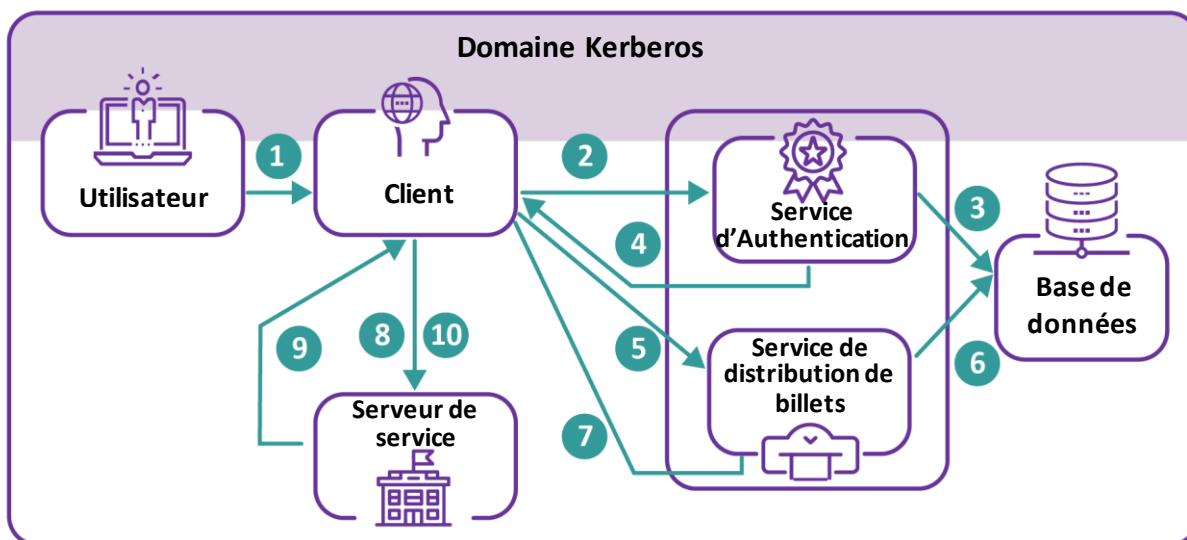
11. le meilleur algorithme à utiliser;
12. l'ordre dans lequel les éléments doivent être mis à niveau;
13. la voie à suivre pour l'adaptation quantique en ligne;
14. autres voies possibles pour l'adaptation quantique (p. ex. mise à niveau de l'ensemble du système, changement de paradigme).

Annexe D : Exemple de cas d'utilisation n° 1 – utilisation de Kerberos pour l'authentification

Section 1 : Description du cas d'utilisation

Kerberos est un protocole d'authentification sur les réseaux informatiques qui permet aux clients d'accéder aux services des fournisseurs. Pour ce faire, il s'appuie sur un service d'octroi de billets (Ticket-Granting Service ou TGS) d'un centre de distribution de clés (CDC) qui fournit des billets au demandeur du service afin qu'il les remette au fournisseur du service pour y accéder. Il est souvent l'élément principal de la fonctionnalité d'authentification unique (AU).

Voici un schéma générique de l'architecture du réseau dans lequel on utilise le protocole Kerberos.



- 1) L'utilisateur saisit ses justificatifs d'identité (nom d'utilisateur + mot de passe).
- 2) Envoyer KRB_AS_REQ.
- 3) Recherche de l'utilisateur (et du mot de passe) dans la base de données.
- 4) Envoyer KRB_AS_RSP.
- 5) Envoyer KRB_TGS_REQ.
- 6) Recherche du service (et du mot de passe) dans la base de données.
- 7) Envoyer KRB_TGS_RSP.
- 8) Envoyer KRB_AP_REQ.
- 9) Envoyer KRB_AP_RSP.
- 10) Envoyer une demande de service au serveur de service.

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

Il convient de mentionner que le contact initial et l'autorisation du client peuvent survenir sur un canal non sécurisé, ce qui, par conséquent, exigera une mesure de protection comme le protocole TLS. Ce canal ne fait pas partie de la portée de ce cas d'utilisation.

Section 2 : Valeur opérationnelle

Kerberos est principalement utilisé pour accorder aux utilisateurs et aux machines l'accès à différents services. Il s'agit souvent d'un élément essentiel dans les applications d'AU. Kerberos est également une des composantes de base de Microsoft Active Directory (AD).

Section 3 : Données opérationnelles potentielles dans la portée/la durée de vie

Les données utilisées par Kerberos se limitent souvent aux données d'accès des utilisateurs et/ou des machines ou aux données concernant le service auquel on accède. Il s'agit notamment des noms d'utilisateur et des mots de passe des utilisateurs, des adresses IP et, éventuellement, d'autres renseignements transitoires à usage limité. L'utilisation de la plupart de ces renseignements est restreinte et leur disponibilité est limitée dans le temps.

Les données auxquelles il est possible d'accéder en cas de compromission de Kerberos sont illimitées, car elles peuvent, en théorie, être utilisées pour accéder à n'importe quel service. Cependant, cela se ferait dans le cadre du service auquel on accède et ne serait pas directement lié à la mise en œuvre de Kerberos.

Section 4 : Catégorie de cas d'utilisation

Gestion des identités et contrôle d'accès.

Section 5a : Considérations techniques

Voici les points dont il faut tenir compte pour utiliser Kerberos dans le cadre de la mise en œuvre de la technologie post-quantique :

- 1) **Disponibilité** : un système utilisant le protocole Kerberos sera souvent accessible par de nombreux utilisateurs et services différents en même temps. Il y a toujours un risque de déni de service (DOS) dans toute modification.
- 2) **Compatibilité** : Kerberos peut être utilisé par de nombreux services différents, chacun ayant son propre codage. Tout changement doit être effectué de manière à être compatible avec les services qui utilisent ce protocole.
- 3) **Gestion des justificatifs d'identité** : Kerberos gère les justificatifs d'identité des utilisateurs et des services afin de les authentifier correctement. Les changements ne doivent pas les compromettre.

Kerberos est souvent intégré à d'autres produits. La plupart des organisations comptent sur leurs fournisseurs pour que le protocole Kerberos soit sûr sur le plan quantique. Toutefois, chaque

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

organisation doit effectuer un suivi et des tests pour s'assurer que tout changement ne cause pas de perturbations.

Section 5b : Menaces

Les applications de Kerberos servent souvent de point d'accès central pour faciliter l'interaction des utilisateurs avec les services d'une organisation. La compromission du système Kerberos peut avoir des conséquences allant d'un accès ponctuel et limité à un service à une défaillance complète et catastrophique du contrôle d'accès.

Il deviendrait alors une cible à la fois pour des initiés malveillants et pour des attaquants externes.

Il existe actuellement des attaques classiques contre Kerberos (p. ex. les attaques de type « pass-the-hash »).

Section 6 : Types de cryptographie

Kerberos repose habituellement sur une cryptographie à clé symétrique et n'est donc pas particulièrement vulnérable aux menaces quantiques. Cependant, il existe des extensions où la cryptographie asymétrique est utilisée pour l'authentification initiale (voir [RFC 4556](#)).

Il existe deux cas où la cryptographie asymétrique peut être utilisée dans le protocole Kerberos :

- 1) **Authentification de l'utilisateur** : le système Kerberos classique vérifie les utilisateurs au moyen de méthodes de contrôle d'accès traditionnelles, comme le nom d'utilisateur et le mot de passe. Toutefois, l'extension à clé publique de Kerberos permet à un utilisateur d'envoyer un certificat de client qui peut être vérifié par une autorité de certification fiable.
- 2) **Entente sur la clé de session** : le protocole Kerberos classique utilise les renseignements de l'utilisateur (p. ex. le mot de passe) pour calculer une clé de session entre le client et le centre de distribution de clés à des fins de chiffrement. L'extension de la clé publique permet l'utilisation d'une clé asymétrique, comme la clé Diffie-Hellman.

Section 7 : Composants techniques

Les principaux composants techniques de Kerberos sont les suivants :

- 1) **Client (demandeur de service)** : the l'utilisateur ou la machine qui demande le service.
- 2) **Fournisseur de service** : le service auquel on accède.
- 3) **Authentificateur du client** : l'entité responsable de l'authentification du client. Elle est souvent intégrée au CDC.
- 4) **Ticket-Granting Service (TGS)** : le service qui octroie au client un billet qui lui permettra d'accéder au service. Il fait souvent partie du CDC.

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

- 5) **Autorité de certification (AC)** : cette option est facultative pour les extensions qui font appel à une autorité de certification pour vérifier les certificats des clients.

Les contrôleurs de domaine sont un exemple de CDC, car ils mettent souvent en œuvre le protocole Kerberos.

Le réseau sur lequel la communication sera effectuée peut également être considéré comme un composant. Cependant, Kerberos n'étant pas un protocole de réseau, il ne fait pas partie de la portée de ce cas d'utilisation.

L'authentificateur du client et le TGS constituent le cœur du système Kerberos, souvent à l'intérieur même du CDC. Le client et le fournisseur de services utilisent des systèmes distincts qui doivent être compatibles avec le CDC du protocole Kerberos pour pouvoir fonctionner correctement.

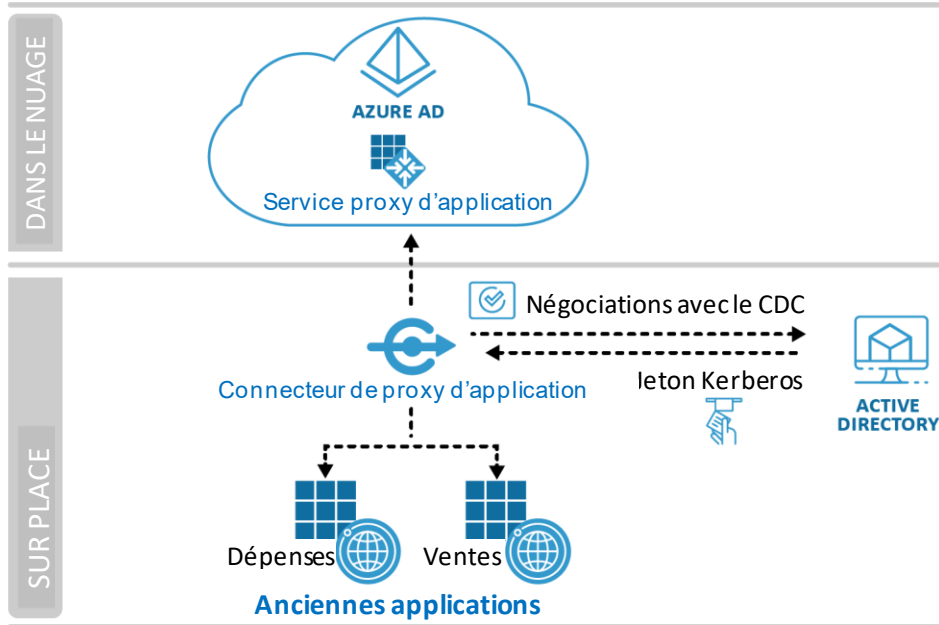
Section 8 : Emplacement des renseignements cryptographiques

Une application de Kerberos (c'est-à-dire le CDC) est généralement un système centralisé possédant son propre code cryptographique et/ou ses propres bibliothèques. Son emplacement exact dépend du produit. Il doit également être en mesure d'accéder à une autorité de certification appropriée pour vérifier un certificat de client lorsqu'il est utilisé pour l'extension de l'authentification initiale.

Il convient de prendre note que les clés asymétriques utilisées dans le CDC sont éphémères et n'ont donc pas besoin d'être stockées pendant une longue période. Les certificats des clients ne sont utilisés que pour l'authentification initiale et peuvent ensuite être éliminés, tandis que les clés asymétriques utilisées pour l'entente sur la clé peuvent être supprimées une fois la clé symétrique établie.

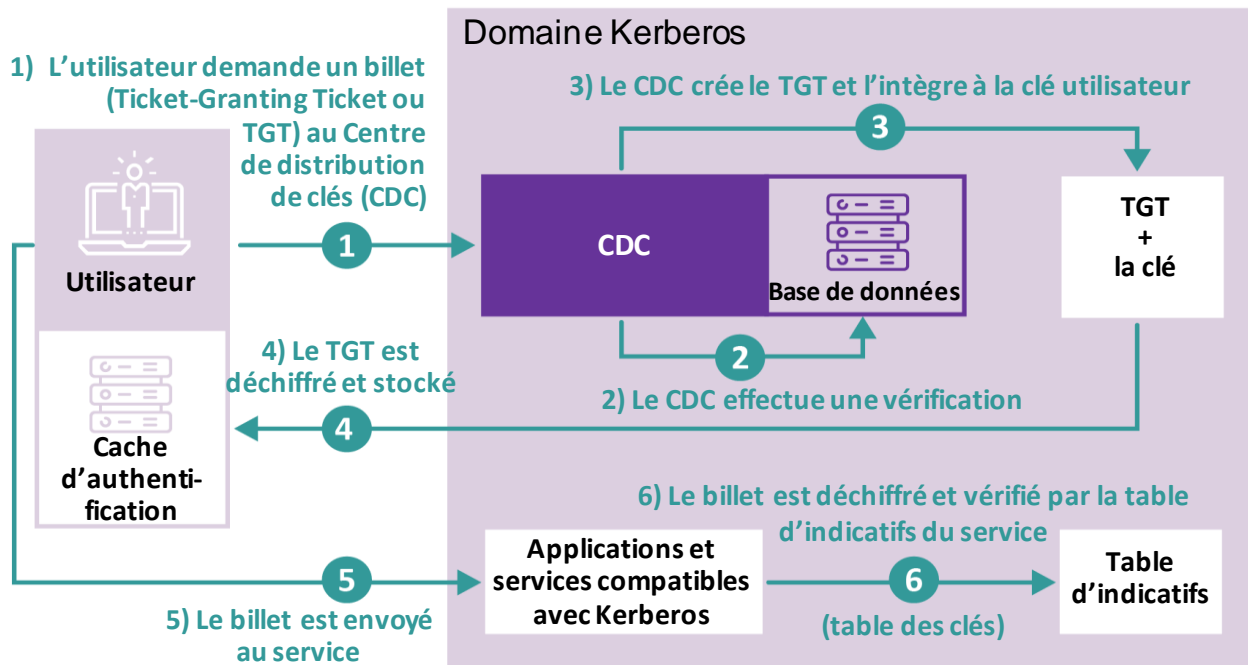
Le client et le fournisseur de services ont leur propre méthode de cryptographie et leur propre emplacement des renseignements cryptographiques. Là encore, tout dépend de l'application. Le client devra stocker la clé privée de son certificat. Cependant, les clés asymétriques nécessaires à l'entente sur la clé sont éphémères et leur stockage n'est pas nécessaire.

Lignes directrices et pratiques exemplaires nationales canadiennes
pour la préparation en matière de technologie quantique



L'application la plus courante de Kerberos se trouve dans Microsoft Active Directory (AD) (voir l'exemple ci-dessus).

Kerberos est également utilisé par Red Hat. Le schéma suivant montre sa structure.



Section 9 : Dépendances techniques

Les cas d'utilisation dépendants de Kerberos sont les suivants :

- Data Stockage des données – pour les clés privées des clients (si des certificats ont été utilisés pour établir l'authenticité des clés publiques);
- ICP/AC – (si des certificats ont été utilisés pour établir l'authenticité des clés publiques des clients);
- TLS – pour protéger l'authentification initiale du client.

Section 10 : Capacité de prendre en charge simultanément des algorithmes

Le CDC est la principale entité qui doit prendre en charge simultanément des algorithmes. Elle doit authentifier simultanément les demandes d'authentification de clés publiques post-quantiques et non post-quantiques des clients.

Si le CDC peut prendre en charge les deux simultanément, il serait logique qu'il soit mis à niveau en premier. Le client et le fournisseur de services devront prendre en charge la version du protocole mise en œuvre par le CDC. Ils peuvent donc être progressivement mis à niveau à leur propre rythme après le CDC. Ces mises à niveau sont indépendantes les unes des autres.

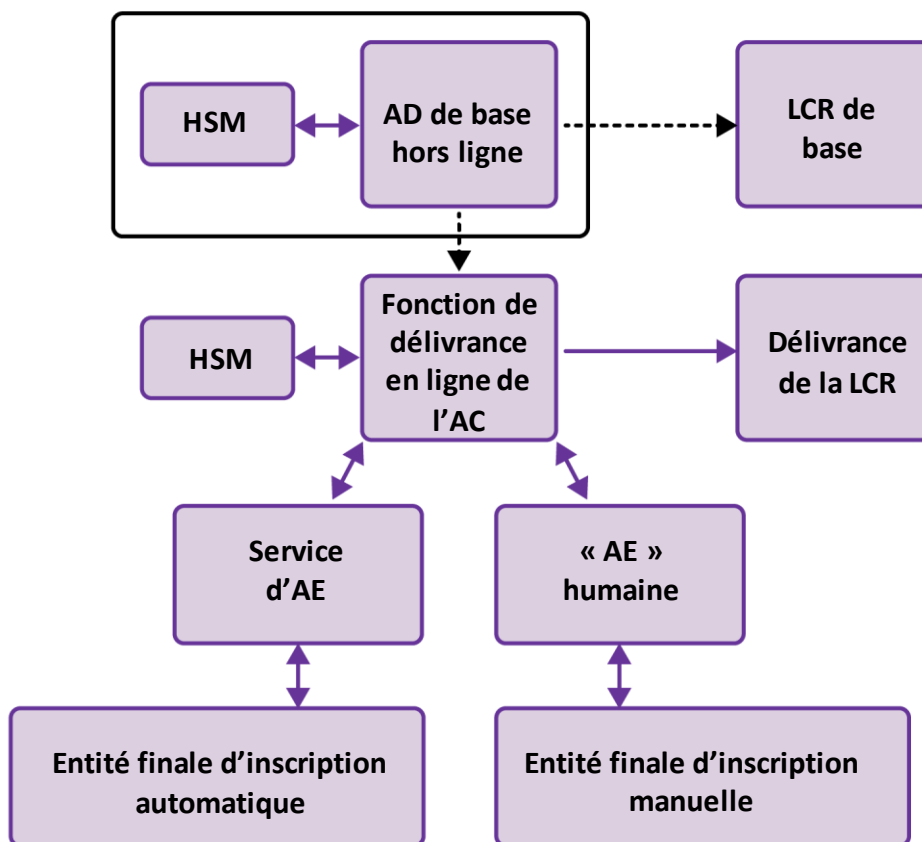
Annexe E : Exemple de cas d'utilisation n° 2 – ICP/AC

Section 1 : Description du cas d'utilisation

L'objectif d'une infrastructure à clés publiques (ICP) est de fournir la technologie et les processus permettant d'exploiter les certificats pour divers autres cas d'utilisation, p. ex. TLS, sFTP, IPSec, et bien d'autres.

Cela se fait par l'intermédiaire d'une autorité de certification (AC) qui a la capacité de délivrer des certificats dont les parties utilisatrices peuvent se servir pour authentifier des entités individuelles. Les certificats tirent profit de la cryptographie à clé publique pour l'authentification, ce qui la rend intrinsèquement vulnérable à l'informatique quantique.

Une autorité de certification a généralement une hiérarchie comme présentée dans le diagramme ci-dessous :



Les AC peuvent avoir plus ou moins de niveaux, mais elles ont la même structure de base.

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

En ce qui a trait à la portée, ce cas d'utilisation ne concerne que la structure de l'AC elle-même. Il ne s'applique pas à l'utilisation des certificats dans des protocoles comme TLS et sFTP, qui feront l'objet de cas d'utilisation distincts.

Le cas d'utilisation de l'AC/ICP sera subdivisé en plusieurs sous-cas d'utilisation :

1. AC publiques – AC qui délivrent des certificats publics ou universellement reconnus (p. ex. Entrust, DigiCert);
2. AC internes sur place – AC établies et gérées par une organisation interne (p. ex. ICP de Microsoft, KeyFactor);
3. AC internes gérées – AC qui ne sont fiables que pour une organisation interne, mais qui sont gérées par une entité externe;
4. AC à usage spécial – AC qui sont généralement propres à une application dans un domaine bien défini (p. ex. les AC IdO pour les appareils mobiles);
5. AC d'inspection – AC utilisées pour intercepter le trafic dans un scénario d'attaque de l'intercepteur et inspecter le contenu (p. ex. filtrage du contenu Web et inspection du protocole).

Bien qu'elles soient similaires, ces AC ont toutes leurs propres caractéristiques, qui seront indiquées lorsqu'elles sont différentes.

Section 2 : Valeur opérationnelle

Les ICP font généralement partie des infrastructures technologiques. Leur valeur réside dans leur rôle d'élément clé de la sécurité opérationnelle des activités essentielles. Ainsi, elles héritent essentiellement de la valeur opérationnelle de toute application qui en dépend. Comme la plupart des applications qui utilisent un réseau exigent un certain niveau de sécurité, les ICP sont omniprésentes dans la plupart des applications de faible ou grande valeur.

Section 3: Données opérationnelles potentielles dans la portée/la durée de vie

Si les ICP jouent un rôle dans la protection des données opérationnelles, elles ne les protègent généralement pas directement. Cette tâche revient souvent à des certificats d'entités finales dans des cas d'utilisation comme les protocoles TLS, sFTP, etc. Cela ne fait pas partie de la portée de ce cas d'utilisation.

En outre, les certificats d'AC sont généralement utilisés pour la signature, et non pour le chiffrement ou l'entente sur la clé. Il n'y a donc pas de risque d'attaque de type « collecte et déchiffrement » pour les certificats d'AC.

Les seules données présentes au sein d'une ICP sont des données d'infrastructure comme les noms de domaine complets (FQDN) ou les informations de routage. Avec l'avènement de la

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

transparence des certificats (TC), la plupart de ces renseignements sont désormais accessibles au public. Il est donc très important de les protéger du point de vue de l'intégrité et de l'authenticité.

Section 4 : Catégorie de cas d'utilisation

Authentification des entités pour les infrastructures essentielles.

Section 5a : Considérations techniques

Voici des points dont il faut tenir compte pour l'ICP dans le cadre de la mise en œuvre de la technologie post-quantique :

- 1) **Taille du certificat** : les applications peuvent avoir des limitations de taille, notamment des contraintes liées à l'appareil ou au canal ou le codage fixe de la taille de la mémoire tampon.
- 2) **Rendement en matière de signature** : certaines applications exigent une AC à haut débit pour des capacités de signature à grand volume ou à grande vitesse. Les AC d'inspection en sont un bon exemple, car elles doivent créer de nouveaux certificats à la volée avec un impact minime ou nul sur la navigation des utilisateurs.
- 3) **Rendement en matière de vérification** : certaines applications comme l'IdO ou les serveurs à grand volume peuvent restreindre le rendement de la vérification, car les dispositifs peuvent être limités ou traiter de grandes quantités de vérifications.

Il faut prendre note que les considérations techniques de la vérification de la chaîne de l'AC pour les applications ne font pas partie de la portée, car elles sont abordées dans les cas d'utilisation des certificats.

Section 5b : Menaces

L'AC est souvent la racine centrale de confiance d'un grand nombre de systèmes. La compromission de la clé privée d'une AC pourrait se traduire par la création d'une grande quantité de certificats et de connexions frauduleux et, par conséquent, de transactions non autorisées. La fraude potentielle dépend directement des capacités des applications qui exploitent ces certificats.

Il faut prendre en considération les points suivants supplémentaires pour chaque cas d'utilisation :

- 1) Les AC publiques sont universellement acceptées, de sorte qu'un compromis pourrait être catastrophique à l'échelle mondiale.
- 2) Les AC sur place n'ont des répercussions que sur l'organisation. Étant donné qu'elles sont hébergées à l'interne, il faudrait probablement accéder au réseau interne de l'organisation pour trouver les certificats d'AC et mener des activités malveillantes.

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

- 3) Les AC gérées sont similaires aux AC sur place en ce sens qu'il faut avoir accès à l'organisation pour effectuer la fraude. Il existe un vecteur de menace supplémentaire dans la mesure où la compromission d'un fournisseur d'AC gérées pourrait affecter de nombreuses organisations différentes.
- 4) Les AC à usage spécial sont propres à l'application à laquelle elles s'appliquent. L'une des menaces à prendre en compte est la découverte de ces AC. Très souvent, ces AC sont intégrées dans des produits et ne sont pas connues des utilisateurs et des administrateurs.
- 5) Les AC d'inspection sont similaires aux AC sur place, sauf que la compromission serait probablement limitée aux applications par un navigateur auxquelles accèdent les utilisateurs internes.

Section 6 : Types de cryptographie

La cryptographie asymétrique est principalement utilisée dans les cas suivants :

- 1) signature des certificats intermédiaires de l'AC;
- 2) signature de certificats d'entités finales;
- 3) signature des listes des certificats révoqués (LCR);
- 4) authentification des justificatifs d'identité de l'autorité d'enregistrement (AE).

Il convient de noter que la signature des certificats racine est automatique. Cependant, la signature a souvent peu de valeur, car les applications accepteront un certificat s'il fait partie de leur liste de certificats racine approuvés.

Les certificats utilisent également une fonction de hachage dans le cadre de la signature et de la vérification de l'empreinte du pouce.

L'ICP fera également appel à la génération de nombres aléatoires afin de créer des paires de clés publiques/privées et de produire des signatures.

Section 7 : Composants techniques

Les composantes techniques de la mise en œuvre de l'AC dépendent du type d'AC. Plusieurs types d'AC sont répertoriés ici :

A) AC de base

Les AC de base sont généralement hors ligne et ne sont utilisées que pour signer les AC intermédiaires et les LCR. Les composants sont généralement les suivants :

- module de sécurité matériel hors ligne (HSM) et périphériques connexes;
- machine hors ligne pour faciliter la signature (p. ex. un ordinateur portable, un ordinateur de bureau, une sorte de dispositif);
- logiciel pour faciliter les fonctions de l'AC;

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

- dispositif de stockage sécurisé hors ligne pour stocker les renseignements de la clé privée.

B) AC intermédiaires (en réseau)

Les AC intermédiaires sont généralement utilisées pour délivrer des certificats.

- HSM en réseau en ligne et périphériques connexes;
- Serveur en ligne, machine virtuelle, ou l'équivalent;
- Logiciel pour faciliter les fonctions de délivrance de l'AC, p. ex. :
 - Validation et approbation de la demande de signature de certificat (DSC).
 - Protocole OCSP ou compatibilité équivalente.
 - Génération et signature de LCR.
 - Vérification des titres d'AE.
 - Génération d'une paire de clés publiques/privées (pour certains cas d'utilisation où l'AC génère le certificat de l'entité finale)
- Recherche en ligne de fichiers accessibles pour les LCR.
- Fonctionnalité de contrôle d'accès.
- Systèmes de sauvegarde pour stocker les journaux et les données.

C) AE (soit manuelle ou automatisée)

Les AE doivent avoir la capacité technique d'accepter les demandes de certificat et d'effectuer la vérification de la demande et la validation de l'entité. Elles comprennent généralement les éléments suivants :

- une machine (p. ex. un ordinateur portable ou un serveur) pour exécuter le logiciel de l'AE;
- un portail ou une liste de contrôle d'accès (LCA) pour fournir les renseignements à valider;
- les justificatifs d'identité de l'AE (généralement un certificat d'AE).

D) AC d'inspection

Les AC d'inspection sont généralement intégrées dans une sorte d'appareil et disposent de leurs propres capacités de protection de la clé privée, comme une carte cryptographique intégrée.

E) AC à usage spécial

Les composants d'une AC à usage spécial dépendent du type d'application pour laquelle elle est utilisée. Par exemple, une AC destinée à gérer l'enregistrement de caméras de surveillance aurait des composants très différents de ceux d'un logiciel de conférence. Cependant, elle comprend :

- une machine pour gérer l'enregistrement, la signature et la délivrance des certificats à usage spécial.

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

F) Entités finales

Bien que les entités finales ne fassent généralement pas partie de la portée de ce cas d'utilisation, nous incluons particulièrement pour l'entité finale la fonction de création d'une DSC et d'installation d'un certificat. Pour ce faire, les composants de l'entité finale seront les suivants :

- l'entité finale elle-même;
- le logiciel utilisé pour créer la DSC et installer le certificat;
- l'emplacement de stockage de la clé privée, ainsi que tout mécanisme de protection connexe.

Section 8 : Emplacement des renseignements cryptographiques

1) AC de base et intermédiaires

Les renseignements cryptographiques sont principalement conservés dans les HSM. Cela dépend beaucoup du type de HSM et du fabricant. Il peut y avoir une certaine fonctionnalité cryptographique résiduelle du logiciel qui est destinée à faciliter la fonctionnalité de l'AC ou à effectuer la signature du protocole OCSP et la vérification des justificatifs d'identité de l'AE.

2) AE

Dans le cas des AE, il s'agira probablement du logiciel qui facilite la connexion des AE.

3) AC d'inspection

Les AC d'inspection s'appuient principalement sur la carte cryptographique qu'elles utilisent pour la génération des certificats, ainsi que sur le logiciel correspondant. Ces éléments sont généralement regroupés dans un même appareil.

4) AC à usage spécial

L'emplacement dépend entièrement de l'application et est propre au fournisseur.

5) Entités finales

Les renseignements sont intégrés dans le logiciel de création des DSC de l'entité, p. ex. OpenSSL.

Pour la majorité des cas d'utilisation, il n'y a généralement pas de renseignements cryptographiques de l'AC en dehors du HSM. La cryptographie pour les HSM est traitée dans le cas d'utilisation du HSM.

Lorsqu'une application uniquement logicielle est utilisée, les clés privées sont habituellement stockées localement sur la machine qui effectue la signature. Le code est intégré dans le logiciel utilisé.

Pour la création de clés privées et de DSC, l'utilitaire de ligne de commande `req` d'OpenSSL représente une application courante. Le code requis se trouve dans les binaires OpenSSL et les clés et les DSC sont envoyées dans un fichier spécifié dans la ligne de commande.

Section 9 : Dépendances techniques

Les cas d'utilisation suivants en sont des dépendances :

- stockage des données
- HSM.

En outre, il peut être nécessaire de tenir compte de certaines considérations relatives à d'autres cas d'utilisation pour lesquels ce cas d'utilisation est une dépendance, afin d'assurer la compatibilité.

Section 10 : Capacité de prendre en charge simultanément des algorithmes

Il existe des propositions visant à jumeler la technologie post-quantique à des méthodes existantes pour prendre en charge les deux, sous forme d'hybride, comme indiqué ici :

- [draft-ietf-lamps-cmp-algorithms-06 - Certificate Management Protocol \(CMP\) Algorithms](#)
- [draft-ounsworth-pq-composite-sigs-04 - Composite Keys and Signatures For Use In Internet PKI \(ietf.org\)](#)

Ce qu'il reste à faire consiste donc à inciter les AC et les entités finales à les mettre en œuvre. Les HSM et tous les logiciels des AC doivent être en mesure de les prendre en charge, tout comme les applications.

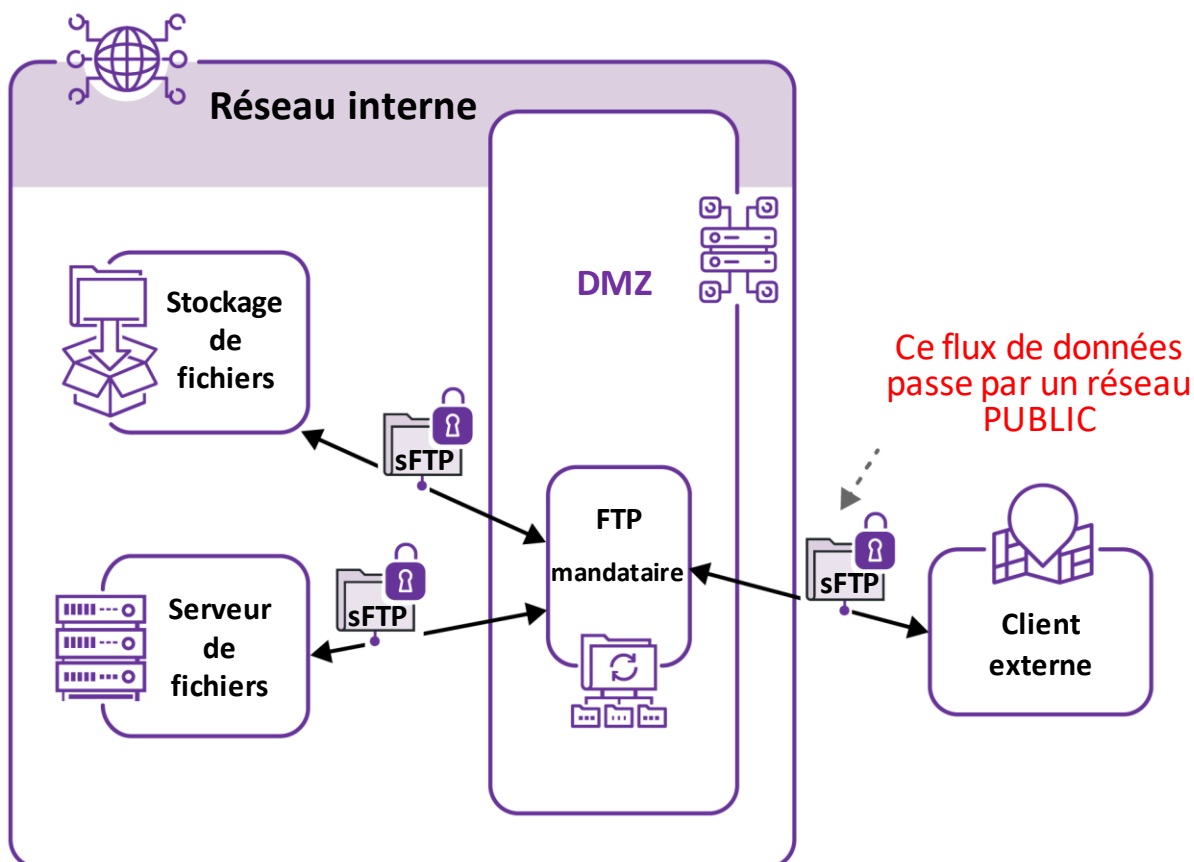
Annexe F : Exemple de cas d'utilisation n° 3 – sFTP

Section 1 : Description du cas d'utilisation

Le protocole sFTP (Secure File Transfer Protocole) (à ne pas confondre avec le Simple File Transfer Protocol) est un protocole réseau qui s'appuie sur l'authentification SSH pour transmettre et gérer des fichiers en toute sécurité entre deux terminaux.

Le protocole SSH constitue en fait un cas d'utilisation et ne sera donc pas examiné de manière générale. Cependant, à des fins de définition de la portée, étant donné que le sFTP est largement utilisé et qu'il présente une grande valeur opérationnelle, dans ce cas d'utilisation, on présumera que l'utilisation de SSH est liée au protocole sFTP et les deux seront donc considérés comme étant un seul et même concept. Un cas d'utilisation de SSH distinct sera créé pour l'utilisation de protocoles autres que sFTP.

Voici un schéma générique de l'architecture réseau dans laquelle le protocole sFTP est utilisé.



Section 2 : Valeur opérationnelle

De nombreuses organisations utilisent des serveurs sFTP pour échanger des fichiers et d'autres documents commerciaux essentiels avec leurs partenaires d'affaires. Ces serveurs ne sont habituellement pas utilisés pour les systèmes transactionnels à faible latence et conviennent davantage aux transferts de fichiers par lots ou en masse. Comme ces types de transferts de fichiers sont omniprésents dans la mise en œuvre technique des systèmes commerciaux, un serveur sFTP pourrait avoir sa place dans n'importe quel système commercial.

Section 3 : Données opérationnelles potentielles dans la portée/la durée de vie

On peut utiliser un serveur sFTP pour transférer tout type de données, à condition qu'elles soient sous forme de fichier. Par conséquent, il n'y a essentiellement aucune limite à la valeur des données qui sont transférées. Les données elles-mêmes dépendront largement de l'utilisation commerciale prévue de l'application qui a recours au serveur sFTP.

Section 4 : Catégorie de cas d'utilisation

Protection des données en transit – (fichiers).

Section 5a : Considérations techniques

Il faut tenir compte des points suivants pour l'ICP dans le cadre de la mise en œuvre de la technologie post-quantique :

- 1) **Taille des fichiers** : un serveur sFTP peut être utilisé pour transférer des fichiers de taille arbitraire. La seule limite pourrait très bien être la limite technique du matériel et du logiciel sous-jacent utilisant ce serveur.
- 2) **Débit** : un serveur sFTP n'est généralement pas utilisé pour des applications transactionnelles à faible latence, de sorte que le débit en temps réel n'est PAS un facteur dont il faut tenir compte. Cependant, certaines applications commerciales dépendent d'un serveur sFTP pour transmettre de grandes quantités de données au cours d'une période restreinte. Le débit devient alors un facteur à prendre en considération.
- 3) **Gestion des justificatifs d'identité** : le protocole sous-jacent permettant l'authentification sFTP (généralement au moyen du SSH) exige que les justificatifs d'identité, comme les clés privées, soient stockés correctement et en toute sécurité sur les terminaux facilitant la connexion sFTP.
- 4) **Prise en charge de la technologie sous-jacente** : les terminaux facilitant la connexion sFTP doivent disposer des capacités appropriées (p. ex. système d'exploitation, connexions réseau, logiciel cryptographique) pour mettre en œuvre la connexion sFTP.

Section 5b : Menaces

Les serveurs sFTP sont devenus une cible de choix pour les pirates, ce qui les expose au risque d'une coûteuse atteinte à la protection des données.

(<https://www.goanywhere.com/blog/2018/01/23/10-essential-tips-for-securing-ftp-and-sftp-servers>).

Les menaces précises qui pèsent sur les serveurs sFTP dépendent de l'environnement de sécurité dans lequel ceux-ci sont utilisés. Par exemple, les connexions sFTP externes sur un réseau public sont intrinsèquement plus vulnérables aux attaques que celles qui s'effectuent à l'intérieur d'une organisation. Des mesures de contrôle supplémentaires, comme la journalisation et la surveillance, peuvent abaisser le niveau de menace global.

Étant donné qu'un serveur sFTP utilise la cryptographie asymétrique pour l'authentification et l'entente sur la clé, il existe une menace quantique inhérente de compromission de la connexion, ainsi qu'un risque d'attaque de type « collecte et déchiffrement » pour les données opérationnelles transmises.

Section 6 : Types de cryptographie

Un serveur sFTP utilise principalement la cryptographie symétrique et asymétrique pour protéger les données des fichiers qui sont transmis.

La cryptographie asymétrique est utilisée par le protocole SSH sous-jacent pour établir une authentification et une entente sur la clé entre les deux terminaux. Les fichiers sont ensuite protégés par la cryptographie symétrique pendant la transmission.

Section 7 : Composants techniques

Les principaux composants techniques sont les suivants :

- 1) les terminaux : les deux terminaux participant à la séance et leur technologie sous-jacente;
- 2) le réseau : le réseau sur lequel la transmission s'effectue.

Il faut prendre note que le réseau peut avoir plusieurs sauts entre les points de connexion. Cependant, dans le cadre de ce cas d'utilisation, il s'agit de passages transparents et il n'est donc pas nécessaire d'en tenir compte.

Les terminaux doivent satisfaire aux exigences qui suivent :

- 1) disposer des capacités requises pour prendre en charge le logiciel sFTP, y compris les fonctions cryptographiques requises;
- 2) disposer des capacités requises pour prendre en charge le logiciel d'authentification sous-jacent (SSH);

Lignes directrices et pratiques exemplaires nationales canadiennes pour la préparation en matière de technologie quantique

- 3) être en mesure de stocker ou d'envoyer ou de recevoir les fichiers transmis;
- 4) être en mesure de stocker et de gérer les justificatifs d'identité du logiciel d'authentification sous-jacent (p. ex. les clés privées);
- 5) avoir accès au réseau approprié sur lequel la communication doit s'effectuer.

Le réseau doit être en mesure de prendre en charge le protocole d'authentification, ainsi que le transfert de fichiers.

Section 8 : Emplacement des renseignements cryptographiques

Le protocole sFTP tirera profit de la cryptographie intégrée dans son propre logiciel lorsqu'il aura été installé ou qu'il exploitera les bibliothèques cryptographiques sous-jacentes de la machine sur laquelle il est utilisé.

Toute modification de la cryptographie utilisée dans le protocole sFTP équivaut à une modification du code cryptographique dans l'un de ces emplacements. Il est important de prendre note qu'il faut tenir compte de considérations supplémentaires avant d'effectuer toute modification de ce type :

- 1) l'emplacement de toute clé cryptographique doit être pris en compte;
- 2) il faut s'assurer que les protocoles connexes sont compatibles avec toute modification de la taille de la mémoire tampon, du débit ou des étapes du protocole.

Il importe de noter que certaines applications sFTP peuvent être regroupées avec un SSH ou être séparées de façon modulaire. Dans de telles situations, il faudra peut-être prendre en considération la cryptographie et les emplacements cryptographiques des deux protocoles simultanément plutôt que séparément. Lorsque l'on envisage de modifier la cryptographie d'une application, il convient de tenir compte du fait que les applications sFTP et SSH sont liées ou non.

De nombreuses applications sFTP courantes fonctionnent de manière similaire en ce qui concerne l'emplacement des renseignements cryptographiques. Le code cryptographique est intégré dans le code source et les binaires du produit. Les clés privées ou les certificats sont généralement stockés localement dans des fichiers .pem ou .ppk.

Section 9 : Dependencies techniques

Les cas d'utilisation dépendants du protocole sFTP sont les suivants :

- stockage de données;
- ICP/AC – (si des certificats ont été utilisés pour établir l'authenticité des clés publiques).

De plus, on devrait normalement considérer le SSH comme un cas d'utilisation dépendant, mais nous l'avons lié au protocole sFTP pour les besoins de ce cas d'utilisation.

Section 10 : Capacité de prendre en charge simultanément des algorithmes

De par sa nature même, un terminal sFTP établit une connexion sFTP individuelle avec un nombre quelconque d'autres terminaux. Chaque connexion utilise des algorithmes cryptographiques fixes et établis pour la durée de vie de cette connexion. Toutefois, les connexions entre les différents terminaux sont en théorie indépendantes les unes des autres. Par conséquent, tout terminal sFTP peut théoriquement mettre en œuvre différents algorithmes cryptographiques pour différentes connexions. Ainsi, toute migration vers de nouveaux algorithmes peut être effectuée connexion par connexion au moment où l'autre terminal est prêt.

La possibilité de prendre en charge simultanément différents algorithmes dépend donc de la programmation du produit sFTP en question pour cette fonctionnalité. Il serait bon d'encourager les fournisseurs de produits sFTP à offrir cette fonctionnalité.

Appendice A : Mythes et FAQ concernant la préparation en matière de technologie quantique

	Mythe	Réalité
1	La menace quantique ne s'applique qu'à un petit groupe d'organisations au Canada.	La menace quantique est importante et a des répercussions dans tout le pays. En raison des risques pour la sécurité de l'information, ainsi que pour la santé et la sécurité, dans des domaines comme les infrastructures essentielles, le réseau 5G, l'infonuagique, l'intelligence artificielle/apprentissage automatique et l'IdO, il faudra des efforts et des mesures à l'échelle nationale, notamment de la part du gouvernement et des organisations.
2	La menace quantique : pour mon organisation, n'est-ce pas un problème de technologie de l'information (TI)?	Pour l'organisation, les menaces et les risques posés par l'informatique quantique sont, avant tout, un problème d'ordre OPÉRATIONNEL.
3	Le secteur des technologies de l'information et des communications (TIC) et les organisations industrielles connexes vont résoudre ce problème. Mon organisation/secteur ne doit rien faire... ou n'a pas grand-chose à faire, n'est-ce pas?	Il est vrai qu'un large éventail d'intervenants du domaine de l'informatique quantique, notamment les organismes de normalisation, les organisations du secteur des TIC, le milieu universitaire et d'autres, travaillent avec diligence pour tenter de faire face aux menaces posées par l'avenir de l'informatique quantique. Cependant, en fin de compte, ce sont les organisations et les secteurs individuels qui sont responsables de la confidentialité, de l'intégrité et de la disponibilité de toutes les données clés de valeur qu'ils stockent, traitent et transmettent.
4	Ce n'est pas un problème urgent pour le moment. Se préparer à l'avènement de l'informatique quantique... ça peut attendre, n'est-ce pas?	Le processus d'évaluation des risques quantiques et de migration quantique peut s'échelonner sur plusieurs, voire de nombreuses années. Les délais pour les organisations et les secteurs dépendront de nombreux facteurs, notamment les suivants : le nombre, les types, la complexité et les interdépendances (intra et interorganisationnels) des produits, systèmes, interfaces et solutions employant divers systèmes cryptographiques; une chaîne d'approvisionnement fiable des systèmes cryptographiques (matériel et logiciels); la disponibilité de ressources qualifiées; etc.

Lignes directrices et pratiques exemplaires nationales canadiennes
pour la préparation en matière de technologie quantique

	Mythe	Réalité
5	Le NIST est toujours en train de normaliser la cryptographie post-quantique. Faut-il attendre que cela soit fait avant de commencer à se préparer à la CPQ?	<p>Du point de vue de la planification, bien que la cryptographie quantique normalisée ne soit pas encore disponible, il n'existe AUCUNE dépendance directe à l'égard des résultats du processus de normalisation de la cryptographie post-quantique du NIST qui empêcherait une organisation ou un secteur de commencer à évaluer et à planifier les répercussions des technologies quantiques sur la cryptographie.</p> <p>Du point de vue de la migration vers la CPQ, les futures mises en œuvre doivent être fondées sur des algorithmes et des produits et solutions cryptographiques reposant sur des normes et des certifications.</p>
6	Le risque est faible au sein de l'organisation/du secteur, car la cryptographie est peu ou très peu utilisée, n'est-ce pas ?	La cryptographie est omniprésente et intégrée dans tous les aspects des technologies de l'information et des communications afin de garantir la confidentialité et l'intégrité des renseignements stockés, traités et transmis.
7	<p>La confidentialité des renseignements de nature délicate actuels est assurée pour le moment.</p> <p>La préparation en matière de technologie quantique peut donc attendre, n'est-ce pas?</p>	L'un des principaux scénarios de menace consiste à capturer des données aujourd'hui (y compris des données chiffrées et des renseignements cryptographiques, comme des échanges de clés cryptographiques), puis à déchiffrer les données capturées plus tard en utilisant des technologies quantiques.
8	La préparation en matière de technologie quantique semble simple et directe pour mon organisation ou mon secteur. Cette préparation peut donc attendre, n'est-ce pas?	<p>Cela dépend. La préparation en matière de technologie quantique dépend de nombreux facteurs, notamment : les quantités et les types de données de valeur; les exigences en matière de confidentialité et d'intégrité des données; le nombre et les types de systèmes qui stockent, traitent et transmettent les données; le nombre et la complexité des interfaces avec d'autres systèmes; les dépendances interorganisationnelles.</p> <p>Il peut être nécessaire d'effectuer une évaluation de la préparation en matière de technologie quantique pour comprendre le niveau de simplicité ou de complexité de la préparation à la cryptographie post-quantique..</p>

Lignes directrices et pratiques exemplaires nationales canadiennes
pour la préparation en matière de technologie quantique

	Mythe	Réalité
9	Pour se préparer à la technologie quantique, il suffit de mettre à jour certains logiciels pour intégrer les nouveaux protocoles de chiffrement, n'est-ce pas?	Il ne s'agit ABSOLUMENT PAS d'une « simple mise à jour logicielle mensuelle ». Un examen technique détaillé des produits, systèmes, infrastructures et architectures actuels qui utilisent des modules cryptographiques permettra de déterminer si des mises à niveau matérielles, logicielles ou applicatives, voire des remplacements complets de systèmes, sont nécessaires.
10	La préparation en matière de technologie quantique vous semble-t-elle fastidieuse?	Si les aspects techniques détaillés des menaces quantiques et les aspects cryptographiques dépassent les compétences de la plupart des gens, la grande majorité des étapes de la préparation en matière de technologie quantique sont généralement des étapes progressives de procédures et processus stratégiques et opérationnels existants, tant sur le plan opérationnel que technique. Les renseignements de source ouverte, comme le guide des pratiques exemplaires pour la préparation en matière de technologie quantique, ainsi que les exemples, ont pour but d'aider les organisations et les secteurs à commencer immédiatement leur préparation.
11	Pour la cryptographie symétrique, il suffit de s'assurer que la clé est suffisamment longue pour fournir une assurance concernant la CPQ; c'est aussi simple que cela, n'est-ce pas ?	À proprement parler, du « simple » point de vue de la cryptographie symétrique, oui, si la clé est suffisamment longue, alors la cryptographie symétrique peut être considérée comme étant sûre. Cependant, en fonction du cas d'utilisation, à l'appui de la cryptographie symétrique, il peut être nécessaire d'échanger et de gérer les clés symétriques, et ces techniques exigent généralement l'utilisation de la cryptographie asymétrique. Si c'est le cas, le système sera vulnérable aux attaques cryptographiques de type quantique.
12	Nous mettons en œuvre une cryptographie non normalisée. C'est correct, n'est-ce pas?	L'utilisation d'une cryptographie exclusive ou non normalisée, ou d'un algorithme qui n'a pas fait l'objet d'un examen approfondi, représente un risque important pour la sécurité.

Appendice B : Politiques, règlements et normes post-quantiques

B.1 Politiques post-quantiques

Le Centre canadien pour la cybersécurité a publié une directive (ITSB-127) concernant l'informatique quantique :

- **Atténuation obligatoire des menaces liées à l'informatique quantique au GC** (ITSB-127)

L'ITSB s'applique aux réseaux de communications du gouvernement du Canada (GC), aux systèmes de sécurité nationale et aux utilisateurs du GC qui traitent, manipulent ou conservent l'information et les données classifiées du GC, ou d'autre information.

[Centre canadien pour la cybersécurité - mai 2019](#)

B.2 Réglementation post-quantique

Jusqu'à présent, le Canada n'a pas adopté de réglementation relative à la préparation en matière de technologie quantique ou à la cybersécurité post-quantique.

B.3 Normes de sécurité post-quantique

Le National Institute of Standards and Technology des États-Unis a commencé à travailler sur de nouvelles normes pour la CPQ en 2015. Il a notamment pour objectifs de publier des ébauches de normes pour commentaires publics en 2022-2023, et de recommander des normes en matière de CPQ en 2024. Le NIST prévoit également :

- *recenser tous les cas où les normes FIPS (Federal Information Processing Standards) du NIST, les Special Publications (SP) de la série 800 et d'autres orientations devront être mises à jour ou remplacées;*
- *recenser les normes de l'ISO/CEI, de l'IEEE, de groupes industriels comme le Trusted Computing Group et d'autres organisations d'élaboration de normes qui devront être mises à jour ou remplacées;*
- *recenser les RFC (Request for Comments) de l'IETF (Internet Engineering Task Force) et autres normes de protocoles de réseaux qui devront être mis à jour ou remplacés.*

[Migration to Post-Quantum Cryptography - Project Description](#)

NIST, 4 juin, 2021, 16 pages

Appendice C : Projet du NCCoE des É.-U. sur la migration vers la CPQ

Le 4 juin 2021, le National Cybersecurity Center of Excellence (NCCoE) des États-Unis, au sein du NIST, a invité le public à commenter une ébauche de description de projet pour la *migration vers la cryptographie post-quantique*¹¹.

Si cette ébauche est approuvée sans modification, les résultats du projet du NCCoE pourraient contribuer à l'élaboration de recommandations de pratiques exemplaires pour la section 3.4 – Migration vers la CPQ (phase 4).

Le National Cybersecurity Center of Excellence (NCCoE) du NIST a entrepris l'élaboration de pratiques pour faciliter la migration de l'ensemble actuel d'algorithmes cryptographiques à clé publique vers des algorithmes de remplacement résistants aux attaques par ordinateur quantique.

Le projet fournira des approches systématiques pour remplacer les algorithmes vulnérables par des algorithmes résistants à l'informatique quantique dans les différents types de biens et de technologies sous-jacentes.

La portée proposée par le NCCoE pour ce projet comprend l'étude de cinq scénarios de démonstration qui seraient applicables à un large éventail d'organisations à l'échelle mondiale (y compris les organisations au Canada). Ces scénarios sont les suivants :

Scénario n° 1 : modules matériels et logiciels validés par la norme FIPS-140 qui utilisent une cryptographie à clé publique vulnérable à l'informatique quantique;

Scénario n° 2 : bibliothèques cryptographiques comprenant une cryptographie à clé publique vulnérable à l'informatique quantique;

Scénario n° 3 : applications cryptographiques et applications de soutien cryptographique qui comprennent la cryptographie à clé publique vulnérable à l'informatique quantique ou qui reposent sur cette technologie;

Scénario n° 4 : intégration d'un code cryptographique vulnérable à l'informatique quantique dans les plateformes informatiques;

Scénario n° 5 : protocoles de communication déployés à grande échelle dans différents secteurs industriels qui exploitent des algorithmes cryptographiques vulnérables à l'informatique quantique.

¹¹[Migration to Post-Quantum Cryptography – Project Description](#), NIST, 4 juin 2021, 16 pages



Le contenu du présent document a été élaboré au cours des réunions
du GTPTQ du FCRIN entre juillet 2020 et juin 2021.

Il sera mis à jour chaque année afin de tenir compte des commentaires
de l'industrie sur la mise en œuvre des pratiques exemplaires qui y sont décrites.

Version 01 – 7 juillet 2021

Préparé par le Groupe de travail sur la préparation
en matière de technologie quantique du Forum canadien
pour la résilience des infrastructures numériques

La reproduction est autorisée à condition que la source soit mentionnée.

