Institut belge des services postaux et des télécommunications

Consultation concernant un projet de proposition de l'IBPT fixant des exigences et une roadmap pour la transition post-quantique dans le secteur des télécommunications

Comment réagir au présent document ?

Jusqu'au 03/11/2025
Uniquement par e-mail à consultation.sg@ibpt.be
Avec la référence CONSULT-2025-C3

Personne de contact : Reda Meftah, Ingénieur-Conseiller (+32 2 226 87 75)

Les réponses sont attendues uniquement par voie électronique à l'adresse précisée.

Merci de joindre ce formulaire de couverture à votre réponse.

Vos commentaires devraient se référer aux paragraphes et/ou sections auxquels ils se rapportent et indiquer clairement ce qui est confidentiel.

Institut belge des services postaux et des télécommunications
Boulevard du Roi Albert II 32 bte 10 | 1000 Bruxelles
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.ibpt.be**

TABLE DES MATIÈRES

1. Introduction

1. La protection des données et la sécurisation des communications sensibles sont au cœur des préoccupations européennes.

2. La **Communication** conjointe au Parlement européen et au Conseil du 16 décembre 2020[1] relative à « *La stratégie de cybersécurité de l'UE pour la décennie numérique* », indiquait déjà que la cybersécurité revêt une importance stratégique dans la construction d'une Europe numérique résiliente.

3. La **Décision** (UE) 2022/2481[2] du Parlement européen et du Conseil du 14 décembre 2022 *établissant le programme d'action pour la décennie numérique à l'horizon 2030*, évoque, en son article 4, paragraphe 1er, 2°, parmi les « cibles numériques » visées d'ici à 2030, *« des infrastructures numériques durables, sûres, résilientes et performantes »* (…).

4. Une étape supplémentaire en matière de cybersécurité est franchie avec l'adoption de la Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/11481 (directive SRI 2), ci-après « directive NIS2 ».

5. Cette directive a été transposée partiellement par la loi du 26 avril 2024[3] *établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.*, qui met notamment en place les autorités compétentes ainsi qu'une coopération entre ces dernières au niveau national.

6. L'article 21 fixe les mesures de gestion des risques en matière de cybersécurité comme suit :

   « 1. Les États membres veillent à ce que les entités essentielles et importantes prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services.
   Les mesures visées au premier alinéa garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, en tenant compte de l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre. Lors de l'évaluation de la proportionnalité de ces mesures, il convient de tenir dûment compte du degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques.
   (…) ».

[1] Communication conjointe du 16 décembre 2020 (JOIN (2020) 18 final)
[2] DÉCISION (UE) 2022/2481
[3] Loi du 26 avril 2024

7. Enfin, après l'adoption d'un livre blanc consacré au thème « Comment maîtriser les besoins de l'Europe en matière d'infrastructures numériques ?[4]», dans lequel elle évoque l'objectif d'atteindre un leadership dans le développement de nouvelles capacités dans des domaines tels que les communications quantiques et la cryptographie quantique résiliente, la Commission a adopté le 11 avril 2024 une Recommandation[5] relative à une **feuille de route** pour la mise en œuvre coordonnée de la transition vers la cryptographie post-quantique.

8. Cette Recommandation a pour objet de « *favoriser la transition vers la cryptographie post-quantique pour la protection des infrastructures et services numériques utilisés par les administrations publiques et d'autres infrastructures critiques dans l'Union en permettant aux États membres :*

1) de définir une «feuille de route pour la mise en œuvre coordonnée de la cryptographie post-quantique», afin de synchroniser les efforts qu'ils déploient pour concevoir et mettre en œuvre des plans de transition nationaux tout en assurant l'interopérabilité transfrontière;

2) de soutenir l'évaluation et la sélection d'algorithmes de cryptographie post-quantique de l'UE pertinents, avec l'aide d'experts en cybersécurité, et de poursuivre l'adoption de tels algorithmes sous la forme de normes de l'Union qui devraient être mises en œuvre dans toute l'Union dans le cadre de la feuille de route pour la mise en œuvre coordonnée de la cryptographie post-quantique;

3) de prendre des mesures appropriées et proportionnées pour se préparer à cette transition. ».

2. Cadre légal interne

9. Le présent document traduit les attentes européennes développées au point 1 au niveau national en définissant les exigences minimales de gestion des risques quantiques et de transition vers la cryptographie post-quantique, ainsi qu'en établissant le calendrier sectoriel des objectifs pour les opérateurs de télécommunications belges.

10. Suite à l'adoption de la loi du 26 avril 2024 *établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique*, l'IBPT a vu la portée de ses compétences évoluer puisque l'article 14, § 1er, dernier alinéa, de la loi du 17 janvier 2003 *relative au statut du régulateur des secteurs des postes et des télécommunications belge (ci-après « loi-statut)* a été modifié.

11. L'IBPT a ainsi été désigné en qualité d'autorité sectorielle, mais également comme service d'inspection sectoriel, pour le secteur d'infrastructure numérique[6], à l'exception des prestataires de services de confiance au sens de l'article 8, 24°, de la loi du 26 avril 2024 précitée.

[4] Livre blanc
[5] Recommandation 2014 1101 feuille de route
[6] Pour être complet, on notera que l'IBPT a également été désigné en ces qualités pour le secteur des services postaux et d'expédition.

12. C'est en cette qualité que l'IBPT lance la présente consultation, en se basant notamment sur les travaux effectués par plusieurs instances ainsi que des lignes directrices[7] pour la gestion des risques quantiques dans le secteur des télécommunications émises par le GSMA.

13. Dans le cadre de l'exercice de ses compétences, l'IBPT dispose de plusieurs moyens d'action, évoqués à l'article 14, § 2, de la loi-statut, notamment la possibilité d'organiser de manière non discriminatoire toute forme d'enquêtes et de consultations publiques.

14. La présente consultation s'inscrit dans ce cadre et vise à assurer la prise en compte du point de vue des stakeholders concernés par la transition post-quantique dans le secteur des communications électroniques.

3. Proposition fixant des exigences et une roadmap pour la transition post-quantique pour le secteur des télécommunications

15. La proposition fixant des exigences et à une roadmap pour la transition post-quantique pour le secteur des télécommunications est annexée.

16. Des informations contextuelles supplémentaires sont fournies dans le texte proposé.

Bernardo Herman
Membre du Conseil

Peggy Valcke
Membre du Conseil

Stefaan Vyverman
Membre du Conseil

Michel Van Bellinghen
Président du Conseil

[7] « Guidelines for quantum risk management for telco v1.0, » 2023, disponible via ce lien direct.

Annexe : Proposition fixant des exigences et une roadmap pour la transition post-quantique dans le secteur des télécommunications

TABLE DES MATIÈRES

RÉSUMÉ

Le développement des ordinateurs quantiques menace de rendre obsolètes certains algorithmes cryptographiques utilisés pour sécuriser les réseaux de télécommunications.

Face aux risques de compromission rétroactive via des attaques "store now, decrypt later" et aux conséquences potentiellement sévères sur la confidentialité des clients et la continuité des services, afin d'assurer le respect de la Recommandation du 11 avril 2024, les Etats membres de l'UE œuvrent en vue d'assurer une transition coordonnée vers la cryptographie post-quantique.

Le présent document traduit les attentes européennes au niveau national en définissant les exigences minimales de gestion des risques quantiques et de transition vers la cryptographie post-quantique, ainsi qu'en établissant le calendrier sectoriel des objectifs pour les opérateurs de télécommunications belges.

La démarche de référence choisie est structurée en trois phases.

Elle comprend :

- l'inventaire des actifs cryptographiques et l'analyse de risques quantiques ;
- la planification de la migration avec désignation d'un responsable dédié et la coordination écosystémique ;
- l'exécution du déploiement progressif des solutions.

Le calendrier sectoriel fixe des objectifs qui s'échelonnent de la finalisation des inventaires dès publication du document à l'achèvement de la migration d'ici 2030 pour les systèmes les plus critiques, avec un dispositif de supervision prévu dans le cadre de la loi du 13 juin 2005 relative aux communications électroniques, ainsi que par les directives « NIS2 » et « CER » (directive (UE) 2022/2557 du 14 décembre 2022 sur la résilience des entités critiques), afin d'atteindre les objectifs de résilience quantique européenne d'ici 2035.

1. Introduction

1. Le développement des ordinateurs quantiques menace de rendre obsolètes de nombreux algorithmes cryptographiques actuels, en particulier les algorithmes asymétriques (qu'il s'agisse du « RSA »[1]ou de courbes elliptiques) utilisés pour sécuriser les réseaux de télécommunications. [1]

2. Des acteurs malveillants pourraient dès à présent exploiter cette menace via des attaques de type « store now, decrypt later », en interceptant et stockant des communications chiffrées pour les déchiffrer une fois qu'un ordinateur quantique suffisamment puissant sera disponible. [2] [3] L'intégrité et l'authenticité des données sont également en jeu, car la rupture des signatures numériques permettrait de falsifier des mises à jour logicielles ou des enregistrements critiques. [2]

3. Face à ces risques aux conséquences potentiellement sévères (atteinte à la confidentialité des clients, interruption de services, pertes financières) [2], une transition coordonnée vers la cryptographie post-quantique (ci-après « PQC » pour « Post Quantum Cryptography s'impose. [3]

4. Depuis maintenant plusieurs années, des efforts majeurs de standardisation de la PQC sont en cours. L'Institut National des Standards et de la Technologie (ci-après « NIST [2]» qui est l'abréviation anglaise du « National Institute of Standards and Technology) aux États-Unis a sélectionné de nouveaux algorithmes résistants aux ordinateurs quantiques (par ex. CRYSTALS-Kyber pour l'établissement de clés, CRYSTALS-Dilithium pour les signatures) et a publié en 2024 les premiers standards officiels de cryptographie post-quantique. [4]

5. Les avancées en matière de standardisation et de développement de solutions établissent les fondements techniques nécessaires à la transition. Il incombe également au secteur d'engager les efforts requis pour accompagner cette dynamique et se préparer à la menace quantique et à accueillir des solutions technologiques innovantes pour se prémunir contre cette menace. L'immaturité temporaire des solutions ne saurait justifier l'inaction.

1.1 Objectif et portée du document

6. Le présent document propose un cadre normatif pour accompagner, encadrer et évaluer la transition post-quantique, ci-après « PQC » (abréviation de l'anglais « Post Quantum Cryptography »), des opérateurs de télécommunications belges désignés comme infrastructures critiques. Il constitue une base de référence pour les futurs contrôles et vise à garantir un niveau minimum homogène de sécurité quantique dans le secteur.

7. Ce document répond aux attentes européennes en définissant les exigences minimales pour l'évaluation, la planification et l'exécution de la transition, les critères de gouvernance des risques quantiques, et l'harmonisation avec le calendrier européen de résilience quantique (échéances 2026, 2030, 2035).

[1] Le RSA est l'abréviation du « Rivest–Shamir–Adleman ». Il s'agit du nom de l'algorithme cryptographique.
[2] « NIST » est l'abréviation anglaise utilisée pour désigner le « National Institute of Standards and Technology »

8. **Exclusions du périmètre d'application :**
Les technologies de distribution quantique de clés (en anglais « QKD » pour « Quantum Key Distribution ») et autres solutions de cryptographie quantique ne relèvent pas du présent document, qui se concentre exclusivement sur la migration vers les algorithmes cryptographiques post-quantiques standardisés.

2. Contexte télécom

9. Les opérateurs de réseaux de communications électroniques belges correspondent au Personna[3] adoptants urgents (Urgent Adopters) selon la taxonomie établie par le PQC Migration Handbook. [4] Ceci résulte de la criticité de leurs infrastructures, de la longévité opérationnelle de leurs équipements, et de leur exposition systémique à la menace quantique.

10. Ceci implique que les opérateurs doivent :

- Initier immédiatement les processus de migration post-quantique ;
- Mettre en place une gouvernance dédiée aux risques quantiques ;
- Établir un calendrier de transition contraignant ;
- Rapporter périodiquement l'avancement de la migration.

2.1 Vulnérabilité quantique dans les réseaux de télécommunications actuels

11. L'architecture cryptographique des réseaux télécoms présente une vulnérabilité stratifiée à la menace quantique. Comme l'illustre la figure 1, les couches inférieures de la pile réseau utilisent principalement le chiffrement symétrique sur des connexions statiques (par exemple, AES), tandis que les couches supérieures utilisent plus souvent le chiffrement asymétrique sur des connexions dynamiques pour la négociation de clés et/ou l'authentification (par exemple, TLS). La cryptographie symétrique déployée dans les couches inférieures pour le chiffrement des connexions statiques requiert une évaluation des tailles de clés et des mécanismes de distribution. Le chiffrement asymétrique, prédominante dans les couches supérieures (transport, application) pour l'établissement de clés et l'authentification, constitue une vulnérabilité critique nécessitant une migration prioritaire vers les standards post-quantiques. [5]

12. Les opérateurs doivent évaluer la vulnérabilité quantique de chaque domaine de sécurité de leur infrastructure :

12.1. **Plan de données :**
Transport des communications utilisateurs avec protection cryptographique de bout en bout. Risque de compromission rétroactive des données sensibles.

12.2. **Plan de contrôle :**

[3] Un « Personna » correspond à une catégorie d'organisations définies selon leurs besoins spécifiques en matière de migration post-quantique. [4]

Signalisation réseau et routage du trafic. Vulnérabilité critique pouvant compromettre l'intégrité opérationnelle globale du réseau.

12.3. **Plan de gestion :**
Configuration et supervision des ressources réseau. Exposition des systèmes de gestion via des protocoles d'administration non sécurisés face aux risques dus aux technologies quantiques.

12.4. **Interfaces d'exposition réseau :**
APIs de programmabilité réseau introduisant de nouvelles surfaces d'attaque. Ces APIs permettent à des applications externes de contrôler certaines fonctions du réseau de l'opérateur (allocation de bande passante, qualité de service, routage). Ces interfaces utilisent des mécanismes d'authentification cryptographique vulnérables aux attaques quantiques, risques amplifiés par l'ouverture croissante des architectures réseau.

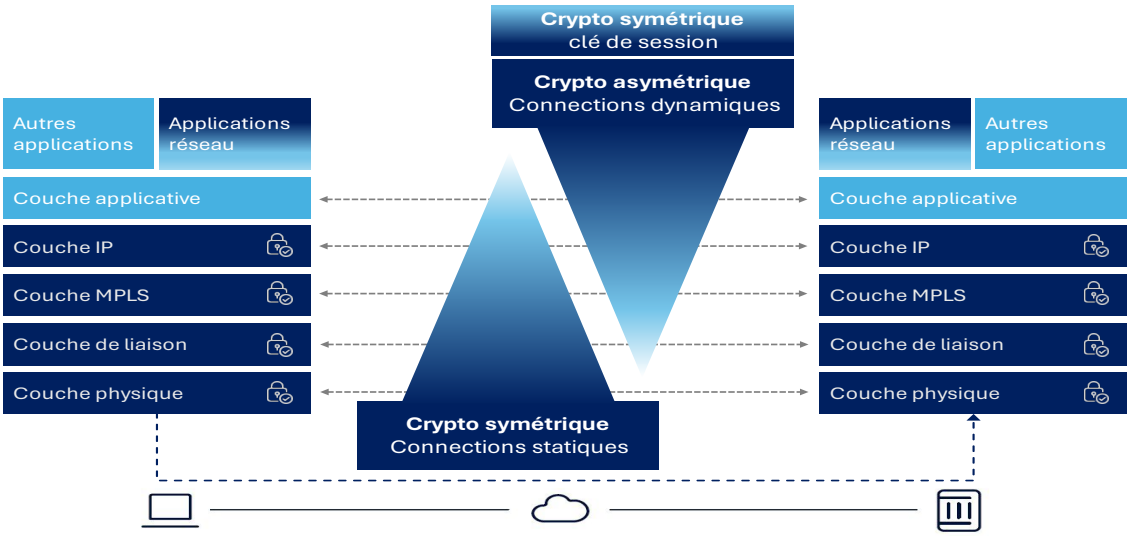

Figure 1: LA CRYPTOGRAPHIE SYMÉTRIQUE ET ASYMÉTRIQUE DANS LES DIFFÉRENTES COUCHES DU RÉSEAU [5]

2.2 Overview de l'écosystème télécom post-quantique

13. La transition post-quantique des opérateurs télécoms ne peut être envisagée de manière isolée. Les vulnérabilités mentionnées, et donc la transition PQC, s'inscrivent dans un écosystème complexe d'interdépendances cryptographiques qui amplifie les risques de propagation des vulnérabilités quantiques. La cartographie ci-dessous [2] illustre ces flux de dépendances qui conditionnent la réussite de la migration post-quantique.

14. Les opérateurs doivent établir une cartographie la plus complète possible de leurs chaînes de dépendances cryptographiques, évaluer les risques de défaillance en cascade, et coordonner leurs plans de migration avec l'ensemble des acteurs de leur écosystème technologique.

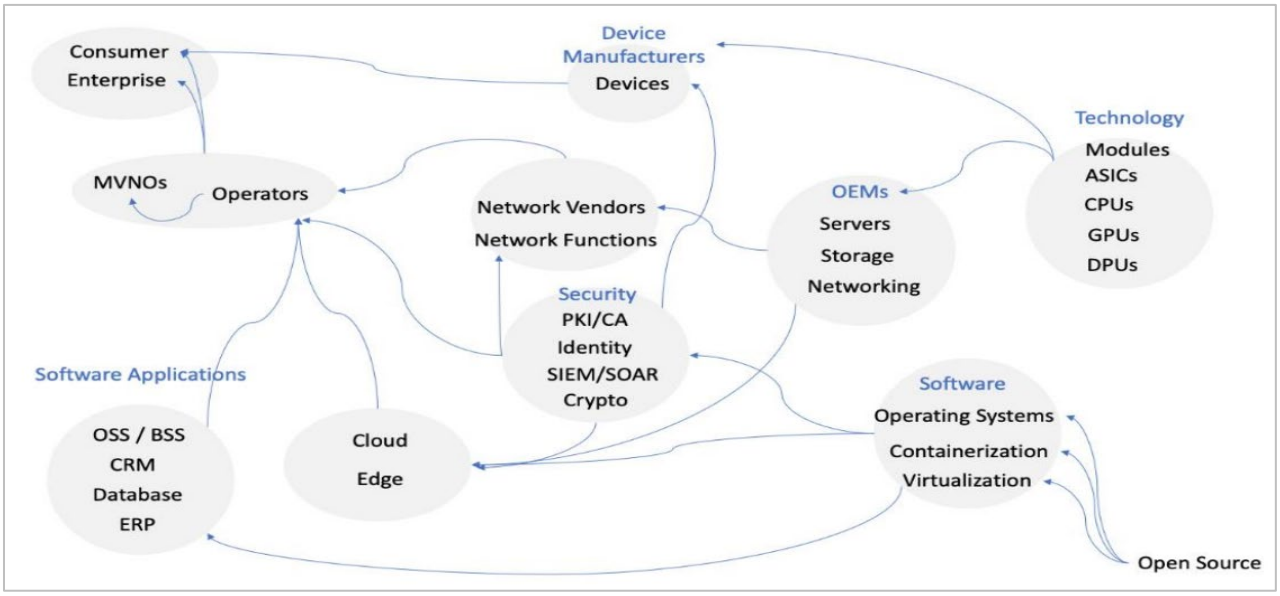

Figure 2: EXEMPLE DE STRUCTURE DE DÉPENDANCES DE L'ÉCOSYSTÈME POST-QUANTIQUE [2]

3. Migration PQC

15. Les opérateurs sont encouragés à adopter une démarche de migration structurée en trois phases conformément aux bonnes pratiques établies par l'ETSI " [6]" et du TNO[4] Migration Handbook [4]. Cette approche facilite une transition maîtrisée et vérifiable vers les crypto-systèmes post-quantiques.

Figure 3: MIGRATION STRUCTURÉE EN 3 PHASES

[4] « TNO » est l'abréviation pour désigner le "Toegepast Natuurwetenschappelijk Onderzoek".

16. Phase 1 : Évaluation et diagnostic des vulnérabilités quantiques

- Inventaire des actifs cryptographiques : Inventaire exhaustif de tous les composants, protocoles et implémentations cryptographiques déployés ;
- Analyse des risques quantiques : Évaluation de l'exposition de chaque actif à la menace quantique avec classification par criticité opérationnelle.

17. Les opérateurs doivent maintenir à jour de manière régulière leur inventaire cryptographique et leur analyse de risques quantiques. Cette obligation de révision périodique s'impose compte tenu de l'évolution constante des environnements informatiques et de l'émergence potentielle de nouvelles vulnérabilités quantiques. Cette démarche constitue par ailleurs une bonne pratique en matière de sécurité informatique au-delà des seuls enjeux quantiques.

18. Phase 2 : Planification de la migration

- Établissement d'un plan de migration avec échéances et jalons de contrôle ;
- Définition des priorités de migration basées sur l'analyse de risques ;
- Coordination avec l'écosystème de fournisseurs et partenaires technologiques.

19. Phase 3 : Exécution de la migration

- Déploiement graduel des solutions post-quantiques selon le plan établi ;
- Validation de conformité et tests d'interopérabilité ;
- Maintien de la continuité opérationnelle durant la transition.

20. Bien que la migration vers les algorithmes post-quantiques constitue une réponse nécessaire à la menace quantique, cette transition ne garantit pas une sécurité absolue. Les implémentations post-quantiques en conditions réelles présenteront probablement des vulnérabilités intrinsèques incluant des défauts algorithmiques, des choix sous-optimaux de paramètres de domaine, la génération de clés faibles, des bugs d'implémentation et des vulnérabilités aux attaques par canaux auxiliaires. Ces limitations soulignent l'importance critique de l'agilité cryptographique[5] comme mécanisme de résilience.

21. L'agilité cryptographique devrait permettre aux opérateurs de réagir rapidement aux découvertes de vulnérabilités, aux évolutions des recommandations de sécurité, et aux avancées cryptanalytiques. Cette capacité d'adaptation constitue un élément essentiel de la stratégie de sécurité post-quantique, faisant de cette migration un processus continu d'amélioration.

22. La réussite de la migration post-quantique repose donc sur la capacité organisationnelle à comprendre et gérer les enjeux techniques et stratégiques de cette transition.

[5] L'agilité cryptographique ou crypto-agilité désigne la capacité organisationnelle et technique permettant de substituer rapidement les algorithmes cryptographiques au sein des systèmes existants (protocoles, applications, équipements, infrastructures) sans devoir reconfigurer ou remplacer systématiquement l'ensemble des systèmes, tout en maintenant la sécurité et la continuité opérationnelle durant la transition.[9]

23. Les opérateurs doivent s'assurer que leurs équipes disposent des connaissances nécessaires pour conduire la migration et maintenir une veille technologique continue sur les évolutions des standards post-quantiques et des vulnérabilités émergentes.

3.1 Phase 1 : États des lieux et diagnostique face à la menace quantique

24. La phase d'évaluation et de diagnostic constitue le préalable indispensable à toute migration post-quantique. Cette étape vise à établir une connaissance précise de l'exposition aux risques quantiques et à structurer la démarche de transition. Les objectifs de cette phase sont :

- Identifier les actifs à migrer en priorité selon leur criticité opérationnelle et leur vulnérabilité quantique ;
- Cartographier les dépendances existantes au sein de l'écosystème technologique de l'opérateur ;
- Anticiper les impacts potentiels de la migration sur la continuité des services et les performances.

25. Les opérateurs peuvent adapter l'ordre et la granularité des activités d'évaluation à leurs contraintes opérationnelles. En pratique, plusieurs activités d'évaluation ou de collecte d'informations peuvent être menées en parallèle. Une approche progressive, débutant par l'analyse des systèmes les plus critiques, constitue une stratégie acceptable pour initier le processus tout en générant rapidement de la valeur.

3.1.1 Inventaire des actifs cryptographiques

26. Une démarche d'inventaire efficace s'appuie sur une stratégie de découverte/exploration structurée de ses assets couvrant l'ensemble des contextes d'usage cryptographique : le code source et les bibliothèques intégrées, les systèmes opérationnels et applications déployées, ainsi que le trafic réseau et les protocoles de communication.

27. La formalisation des résultats dans un format standardisé comme le Cryptographic Bill of Materials (en abrégé « CBOM ») facilite l'analyse, le partage et la maintenance de l'inventaire. L'automatisation de la découverte, lorsque techniquement possible, améliore la fiabilité et la complétude du processus tout en réduisant la charge opérationnelle.

28. Pour les opérateurs télécoms, une approche par priorités permet de concentrer les efforts initiaux sur les composants les plus critiques : infrastructures de cœur de réseau, protocoles de signalisation, interfaces d'accès réseau, et systèmes de gestion exposés.

29. Les opérateurs doivent :

- Disposer d'une politique cryptographique formalisée définissant les règles de gouvernance des actifs cryptographiques ;
- Maintenir un inventaire complet et à jour de leurs actifs cryptographiques couvrant l'intégralité de leur infrastructure ;
- Documenter les dépendances cryptographiques avec leurs fournisseurs et partenaires technologiques ;
- Réviser périodiquement cet inventaire pour refléter les évolutions de leur environnement.

3.1.2 Analyse de risques quantiques

30. Une analyse structurée des risques quantiques s'appuie sur l'évaluation de plusieurs dimensions : la vulnérabilité intrinsèque des primitives cryptographiques face aux algorithmes quantiques, l'impact potentiel d'une compromission sur les opérations, et la complexité de migration vers des alternatives post-quantiques.

31. Des méthodologies comme celle développée par TNO [7] ou les guidelines sectoriels du GSMA [1] fournissent des critères d'évaluation et des outils d'aide à la décision pour une meilleure gestion des risques quantiques. L'utilisation de ces approches structurées permet de systématiser l'analyse et d'assurer la cohérence des évaluations dans la priorisation des actions de migration.

32. La collaboration avec des experts en cryptographie quantique et la consultation des recommandations des organismes de standardisation renforcent la qualité et la pertinence de l'analyse.

33. Les opérateurs doivent :

- Conduire une analyse de risques quantiques couvrant l'ensemble de leurs actifs cryptographiques inventoriés ;
- Établir une classification de criticité permettant de prioriser les actions de migration ;
- Documenter les raisons et les critères des décision prises ;
- Actualiser cette analyse en fonction de l'évolution de la menace quantique et des changements d'infrastructure.

3.2 Phase 2 : Planification de la migration

34. La planification de la migration structure la transition vers les systèmes cryptographiques post-quantiques en définissant les priorités, les ressources et les échéances. Cette phase détermine les stratégies de migration adaptées à chaque catégorie d'actifs et établit la coordination nécessaire avec l'écosystème technologique.

35. Une planification efficace s'appuie sur la constitution d'une équipe dédiée avec un responsable de migration identifié, l'allocation des ressources budgétaires et techniques nécessaires, et l'établissement d'un calendrier tenant compte des dépendances inter-systèmes [4]. La définition de stratégies de migration adaptées selon les spécificités de chaque composant (approche hybride, isolation temporaire, remplacement matériel) optimise l'efficacité du processus.

36. Les opérateurs doivent :

- Désigner formellement un responsable de migration post-quantique disposant d'une vision transversale de l'organisation ;
- Établir un plan de migration documenté définissant les priorités basées sur l'analyse de risques quantiques de la phase 1 ;
- Définir pour chaque actif critique une stratégie de migration (hybride[6], remplacement direct, isolation).

3.3 Phase 3 : Exécution de la migration

37. L'exécution de la migration met en œuvre les stratégies définies lors de la planification en privilégiant les approches qui minimisent les risques opérationnels. Cette phase requiert une attention particulière à la validation des solutions déployées et au maintien de la continuité des services.

38. Le processus de migration post-quantique doit maintenir et renforcer la résilience cryptographique durant toute la phase de transition. Cette résilience repose sur une défense en profondeur, la sécurité à long terme (anticipation des évolutions cryptanalytiques), et l'agilité cryptographique (substitution rapide des primitives selon les recommandations de sécurité).

39. Les opérateurs doivent :

- Respecter l'ordre de priorité établi lors de l'analyse de risques quantiques ;
- Maintenir un registre de traçabilité documentant chaque migration effectuée avec dates et versions ;
- Valider la conformité et l'interopérabilité avant mise en production de chaque solution post-quantique.

[6] Hybridation : Approche combinant simultanément des algorithmes post-quantiques avec des algorithmes cryptographiques classiques éprouvés pour atténuer les risques liés à la relative jeunesse des nouvelles primitives cryptographiques tout en assurant une protection contre la menace quantique. Recommandé notamment par l'ANSSI et la BS.

3.4 Mapping des recommandations GSMA et des exigences fixées par l'IBPT

40. Cette section fait le lien entre les recommandations faites par le GSMA dans le cadre de ses lignes directrices et les exigences minimales fixées par l'IBPT dans le présent document.

	RECOMMENDATIONS GSMA [1]	EXIGENCES IBPT
GOUVERNANCE	Sensibilisation au niveau décisionnel : Établir la prise de conscience de la menace quantique au sein de la direction générale et du conseil d'administration	Les opérateurs doivent : ▪ Initier immédiatement le processus de migration. Tout retard dans l'engagement de cette démarche constitue un manquement aux obligations de sécurité, ▪ Mettre en place une gouvernance dédiée aux risques quantiques, ▪ Définir les rôles et responsabilités liés à la migration PQC et à sa préparation
	Processus de gouvernance organisationnel : Mettre en place un processus de gouvernance transversal pour la gestion des risques quantiques.	
	Responsabilité exécutive : Désigner formellement un responsable de migration post-quantique disposant d'une vision transversale de l'organisation	

	RECOMMENDATIONS GSMA [1]	EXIGENCES IBPT
CAPACITÉ ORGANISASTIONNELLE	Développement des compétences : Développer les capacités organisationnelles pour gérer les risques quantiques et la transition post-quantique	Les opérateurs doivent : ▪ S'assurer que leurs équipes disposent des connaissances nécessaires pour conduire la migration et maintenir une veille technologique continue sur les évolutions des standards post-quantiques et des vulnérabilités émergentes.
	Formation et sensibilisation : Actualiser les programmes de formation pour améliorer la compréhension des enjeux quantiques dans le contexte télécom	
	Veille technologique : Suivre le développement des outils facilitant la transition, particulièrement les solutions hybrides et les standards.	

	RECOMMENDATIONS GSMA [1]	EXIGENCES IBPT
GESTION DES RISQUES	Cadre de gestion des risques : Adapter la méthodologie de gestion des risques existante pour intégrer spécifiquement les risques quantiques Analyse de risques quantiques : Conduire une analyse de risques quantiques complète et rigoureuse couvrant l'ensemble des actifs cryptographiques inventoriés Gestion des risques résiduels : Identifier et gérer les risques résiduels pendant et après la transition	Les opérateurs doivent : ▪ Disposer d'une politique cryptographique formalisée définissant les règles de gouvernance des actifs cryptographiques, ▪ Conduire une analyse de risques quantiques couvrant l'ensemble de leurs actifs cryptographiques inventoriés, ▪ Réviser périodiquement cet inventaire pour refléter les évolutions de leur environnement, ▪ Actualiser cette analyse en fonction de l'évolution de la menace quantique et des changements d'infrastructure.

	RECOMMENDATIONS GSMA [1]	EXIGENCES IBPT
PLANIFICATION DE LA TRANSITION	Inventaire cryptographique : Maintenir un inventaire complet et à jour des actifs cryptographiques couvrant l'intégralité de l'infrastructure Classification des données : Documenter les dépendances cryptographiques avec les fournisseurs et partenaires technologiques, en identifiant les exigences de protection et la longévité des données Priorisation : Établir une classification de criticité permettant de prioriser les actions de migration basées sur l'analyse de risques quantiques Plan de transition : Établir un plan de migration documenté définissant les priorités, les stratégies de migration pour chaque actif critique, et respectant les échéances sectorielles définies	Les opérateurs doivent : ▪ Maintenir un inventaire complet et à jour de leurs actifs cryptographiques couvrant l'intégralité de leur infrastructure ; ▪ Réviser périodiquement cet inventaire pour refléter les évolutions de leur environnement ; ▪ Documenter les dépendances cryptographiques avec leurs fournisseurs et partenaires technologiques ; ▪ Établir une classification de criticité permettant de prioriser les actions de migration ; ▪ Actualiser les analyses et le cas échéant le plan de migration en fonction de l'évolution de la menace quantique et des changements d'infrastructure ; ▪ Documenter les raisons et les critères des décision prises.

4. Timeline

41. La transition post-quantique s'inscrit dans un calendrier européen coordonné.

42. La Recommandation (UE) 2024/1101 [8] et les travaux de l'EU PQC Workstream [3] fournissent un cadre de référence temporel pour structurer cette transition à l'échelle européenne, avec des objectifs d'élaboration de feuilles de route nationales d'ici 2026.

43. La timeline européenne élaborée par l'EU PQC Workstream [3] établit une progression en trois étapes majeures vers la résilience quantique.

    La phase d'initiation, déjà engagée conformément à la déclaration commune de 18 États membres « Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography », marque le début coordonné de la transition.

    D'ici 2026, la planification de la transition PQC et les projets pilotes pour les cas d'usage à haut risque et moyen risque doivent être lancés.

    L'étape cruciale de 2030 vise l'achèvement de la transition PQC pour les cas d'utilisation à haut risque, avec l'activation par défaut des mises à jour logicielles et firmware intégrant la sécurité quantique. Cette progression culmine en 2035 avec l'objectif d'une résilience quantique complète de l'infrastructure européenne.

44. Sur base de ce calendrier européen, les objectifs et échéances suivants ont été définis pour le secteur des télécommunications belges :

    - Échéance 1 - Évaluation (dès à présent) : Finalisation de l'inventaire cryptographique et de l'analyse de risques quantiques ;
    - Échéance 2 - Planification (2026-2027) : Élaboration et validation des plans de migration post-quantique ;
    - Échéance 3 - Mise en œuvre (2027-2030) : Déploiement progressif des solutions post-quantiques selon les priorités établies.

45. Ce calendrier sectoriel constitue la déclinaison des objectifs européens pour les infrastructures critiques de télécommunications, garantissant une transition coordonnée et harmonisée.

4.1 Timeline de supervision

46. Pour garantir l'atteinte de ces objectifs, un dispositif de supervision est prévu. Ce calendrier de contrôle assure la convergence des efforts nationaux vers l'objectif commun de résilience quantique d'ici 2035.

47. 2026 - 2027 -- Vérification des fondations :

- Vérification de l'état des lieux de l'inventaire des actifs cryptographiques ;
- Validation de la qualité des analyses de risque quantique ;
- Évaluation des plans de migration établis.

48. 2028 - 2030 – Contrôle des systèmes de gestion des risques quantiques :

- Contrôle de la mise en œuvre des systèmes de gestion des risques quantiques ;
- Contrôle de l'avancement des migrations critiques ;
- Évaluation de la gouvernance post-quantique.

49. 2031 - 2035 -- Inspection des systèmes à haut risque :

- Contrôle ciblé : "Quantum-Secure or not ?" ;
- Vérification de la migration des actifs prioritaires.

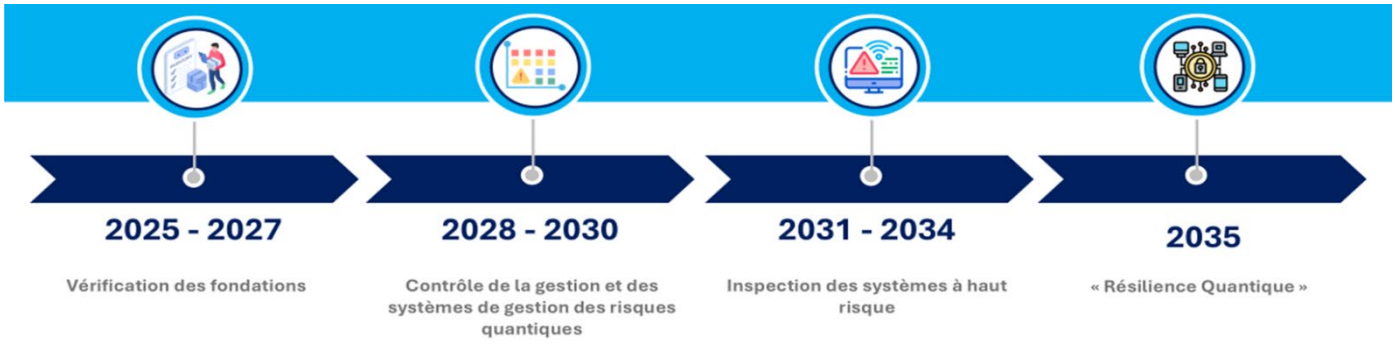

Figure 4: TIMELINE DE LA SUPERVISION

Références

[1] GSMA, «Guidelines for quantum risk management for telco v1.0,» 2023. Url: Guidelines for Quantum Risk Management for Telco

[2] GSMA, «Post quantum Telco Network Impact Assessment - Whitepaper Version 1.0,» 2023. Url: PQTN_1_Doc_006 PQTN White Paper

[3] NIS Cooperation Group, « A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography » 2025. (« NIS » est l'abréviation de « Network and Information Systems »;
Url: A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography | Shaping Europe's digital future

[4] AIVD-CWI-TNO, « The PQC Migration Handbook - guidelines for migrating to post-quantum cryptography » 2024. (« AIVD" désigne "Algemene Inlichtingen- en Veiligheidsdienst»; « CWI» désigne "Centrum Wiskunde & Informatica»; « TNO» désigne le « Toegepast Natuurwetenschappelijk Onderzoek») Url: TNO-2024-pqc-en.pdf

[5] W. Coomans, D. Schoinianakis, R. Sohn, S. Chenard, A. Banerjee et M. Charbonneau, *The road to quantum-safe networks,* Nokia Bell Labs, 2025. Url: Nokia: The road to quantum-safe networks

[6] ETSI, « Migration strategies and recommendations to Quantum Safe schemes », 2020.

Url: TR 103 619 - V1.1.1 - CYBER; Migration strategies and recommendations to Quantum Safe schemes

[7] TNO, Manon de Vries, Sven Bootsma, Vincent Dunning, and Marc van Vliet., « Quantum risicomethodologie,» 2024. Url: Quantum risicomethodologie voor cryptografie

[8] Recommandation 2024/1101 de la Commission du 11 avril 2024 relative à une feuille de route pour la mise en œuvre coordonnée de la transition vers la cryptographie post-quantique; Url: Recommandation 2014 1101 feuille de route

[9] Elaine Barker (NIST), Lily Chen (NIST), David Cooper (NIST), Dustin Moody (NIST), Andrew Regenscheid (NIST), Murugiah Souppaya (NIST), William Newhouse (NIST), Russ Housley (Vigil Security), Sean Turner (sn3rd), *Considerations for Achieving Cryptographic Agility: Strategies and Practices,* 2025. Url: NIST CSWP 39 second public draft, Considerations for Achieving Crypto Agility: Strategies and Practices