<GROUPE DE TRAVAIL CRYPTOGRAPHIE POST-QUANTIQUE>

< GUIDE DE MIGRATION VERS LA CRYPTOGRAPHIE POST-QUANTIQUE >

CAMPUS CYBER 2026

< SOMMAIRE >

< INTRODUCTION >

L'arrivée d'un ordinateur quantique cryptographiquement pertinent (CRQC - Cryptographically Relevant Quantum Computer) représente une menace existentielle pour la sécurité de nos infrastructures numériques actuelles. Les algorithmes de cryptographie, surtout asymétriques (RSA, ECC, Diffie-Hellman), qui protègent aujourd'hui nos communications, nos transactions financières et nos données sensibles seront vulnérables face à la puissance de calcul d'un ordinateur quantique suffisamment mature.

Cette menace n'est pas uniquement future : elle est déjà présente. **Les attaques SNDL (Store Now, Decrypt Later)** sont déjà en cours ; des acteurs non légitimes collectent dès aujourd'hui, et a priori de façon massive, des données chiffrées avec l'intention de les déchiffrer ultérieurement lorsque des ordinateurs quantiques seront suffisamment matures. Cette menace est particulièrement critique pour les données à longue durée de confidentialité : secrets d'État, propriété intellectuelle, données médicales, dossiers personnels sensibles, secrets industriels et stratégiques. Elle l'est également pour les données à longue durée d'authenticité (contrats inter-banques, assurances-vie, testaments, etc.).

Face à cette menace imminente, il est impératif d'agir dès maintenant. La communauté internationale a déjà mobilisé des efforts considérables à plusieurs niveaux. Le NIST (National Institute of Standards and Technology) a publié en août 2024 les premiers standards PQC (FIPS 203, 204, 205) et a par la suite annoncé la standardisation de deux autres algorithmes : Falcon (FIPS 206) en développement et HQC, qui rejoint ML-KEM en tant que second schéma de chiffrement post-quantique. En Europe, des cadres réglementaires contraignants ont été adoptés : **le CRA (Cyber Resilience Act)** entré en vigueur en décembre 2024 avec des obligations applicables dès 2027, **DORA (Digital Operational Resilience Act)** effectif depuis janvier 2025 pour le secteur financier, et **NIS2** qui impose des mesures cryptographiques à l'état de l'art pour les infrastructures critiques.

En juin 2025, la Commission européenne a publié une recommandation sur une feuille de route coordonnée pour la transition vers la cryptographie post-quantique [1], établissant des jalons clairs : fin 2026 pour l'établissement des roadmaps nationales et le début des migrations pour les cas à haut risque, fin 2030 pour la finalisation de la transition des systèmes critiques, et fin 2035 pour la migration complète des systèmes à risque moyen et faible.

La transition vers la **cryptographie post-quantique (PQC)** n'est plus optionnelle : elle est devenue une nécessité stratégique et réglementaire [2]. Ce guide est donc proposé afin de vous accompagner dans cette transition. Ses objectifs sont :

- Présenter les risques posés par les ordinateurs quantiques aux infrastructures IT et aux systèmes d'information actuels ;
- Proposer des recommandations concrètes afin de construire graduellement une stratégie robuste face à la menace quantique ;

- Fournir une méthodologie de migration structurée avec des étapes clairement définies, des livrables identifiés et des jalons mesurables ;
- Simplifier et rendre compréhensible la migration PQC pour les RSSI et décideurs, en traduisant la complexité technique en actions opérationnelles.

Les travaux présentés dans ce document sont le fruit des contributions des participants au groupe de travail PQC du Campus Cyber. Ils présentent une feuille de route opérationnelle pour cette migration en quatre phases basée sur la feuille de route européenne de mise en œuvre coordonnée pour la transition vers la cryptographie post-quantique [1] et s'appuie sur les recommandations internationales.

Il est important de noter que **la date exacte d'arrivée d'un CRQC opérationnel reste incertaine**, les estimations varient entre 2030 et 2040 selon les sources. Cette incertitude renforce l'importance de se préparer dès maintenant et de construire une capacité d'accélération de la transition si l'évolution technologique devait être plus rapide que prévue.

Le tableau suivant résume les quatre phases avec les principaux objectifs et les livrables prioritaires de chaque phase. Ce tableau n'a pas pour vocation de fournir une liste exhaustive de tous les livrables attendus ; cette liste devrait être instanciée pour chaque entreprise selon sa taille, ses ressources et ses besoins.

Les prochaines sections détailleront ces phases et livrables.

Phase	Période	Objectif principal	Livrables clés
1. Préparation (2026)	Immédiat	Sensibilisation pour comprendre les enjeux du PQC, évaluer l'empreinte cryptographique et élaborer la stratégie de transition	1.1Programme de sensibilisation et formation 1.2 Gouvernance et structure de pilotage 1.3 Bilan de pré-évaluation : maturité cryptographique, risques et impacts organisationnels 1.4 Inventaire cryptographique complet 1.5 Stratégie PQC alignée à la stratégie nationale et à la conformité UE 1.6 Planification de la migration 1.7 Budget initial et allocation des ressources

Phase	Période	Objectif principal	Livrables clés
2. Démarrage du déploiement (2026 - 2027)	Court terme	Intégrer et tester les algorithmes PQC dans des environnements contrôlés (hybridation).	2.1 Déploiement pilote 2.2 Démarrage de la mise en place de l'agilité cryptographique 2.3 Lancement de la mise à jour des composants critiques
3. Migration des systèmes critiques (2028 - 2030)	Moyen terme	Migrer l'intégralité des systèmes à risque élevé pour respecter l'échéance 2030.	3.1 Migration hybride/ PQC terminée pour les systèmes à risque élevé 3.2 Conformité PQC des nouveaux produits achetés
4. Généralisation et finalisation (2030 - 2035)	Long terme	Étendre la migration aux systèmes moins critiques et évaluer la transition vers la PQC seule.	4.1 Migration PQC/ hybridation terminée pour les systèmes à risque moyen 4.2 Migration achevée pour le risque faible 4.3 Passage aux algorithmes PQC seuls

< 1. PRÉPARATION (2026) >

1.1 PROGRAMME DE SENSIBILISATION ET FORMATION

La réussite de la migration PQC repose avant tout sur la compréhension de la menace quantique par l'ensemble des parties prenantes. Ce programme vise à sensibiliser les différents niveaux de l'organisation (direction générale, COMEX, équipes IT, développeurs, architectes) à l'urgence de la transition et aux enjeux spécifiques à leur périmètre. Il comprend des sessions de formation adaptées à chaque audience : présentation exécutive pour la direction (enjeux business et réglementaires), formations techniques pour les équipes IT (algorithmes PQC, implémentations), et ateliers pratiques pour les architectes (intégration dans l'existant). L'objectif est de poser des bases solides de compréhension commune qui faciliteront la prise de décisions stratégiques et techniques, l'adhésion aux changements et la collaboration tout au long du projet de migration sur la décennie à venir.

1.2 GOUVERNANCE ET STRUCTURE DE PILOTAGE

Une migration réussie présuppose une réflexion sur les différents chantiers à lancer afin de définir leur priorisation, ainsi que l'établissement d'une gouvernance propre et adéquate aux besoins de l'entreprise (en fonction des besoins métiers, de sa taille, sa maturité, etc.). Le contrôle régulier (via une comitologie établie) permet de suivre l'évolution de la migration et une prise de décision rapide selon les évolutions.

La gouvernance et la structure de pilotage du plan de migration reposent sur une organisation claire des rôles, des responsabilités et des circuits de décision.

Un comité de pilotage stratégique assure l'alignement avec les objectifs métier, valide les jalons clés et arbitre les priorités ; alors qu'une équipe projet opérationnelle coordonne l'exécution, le suivi de risques, la gestion des dépendances et la communication et synchronisation entre les parties prenantes. Ces deux structures permettront une gestion proactive des problématiques rencontrées, une adaptation continue des contraintes techniques, organisationnelles et budgétaires de la migration. N'étant pas à l'abri des évolutions et/ou des nouvelles contraintes règlementaires, la coordination de ces deux structures est un élément clé pour la réussite du projet afin d'être capable de prendre en compte, non seulement les évolutions techniques, mais aussi les besoins évolutifs de différents métiers.

Des mécanismes de reporting et des indicateurs permettant d'assurer la transparence, le suivi des délais et la qualité des livrables peuvent être mis en place si la taille de l'entreprise le permet (et le réclame).

1.3 BILAN DE PRÉ-ÉVALUATION : MATURITÉ CRYPTOGRAPHIQUE, RISQUES ET IMPACTS ORGANISATIONNELS

Avant de se lancer dans l'inventaire technique détaillé, l'organisation doit d'abord évaluer sa situation actuelle et identifier ses vulnérabilités face à la menace quantique. Ce bilan comprend trois volets :

- **Une évaluation de la maturité cryptographique de l'organisation** (exemple de méthode à suivre : le "Growth Model" TNO (8 aspects, 5 niveaux) [3]) permettant d'identifier les forces et faiblesses actuelles en matière de gouvernance cryptographique, d'agilité cryptographique et de gestion des actifs [4] ;
- **Une analyse préliminaire des risques quantiques** basée sur la sensibilité des données, leur durée de vie et l'exposition aux attaques « Store Now, Decrypt Later » ;
- **Une évaluation des impacts organisationnels anticipés** incluant les besoins en compétences, les changements de processus, les impacts sur les partenaires et fournisseurs et l'estimation de l'effort global requis pour la migration.

1.4 INVENTAIRE CRYPTOGRAPHIQUE COMPLET

L'inventaire cryptographique pour la migration PQC doit identifier **où, comment et par quels systèmes les algorithmes et protocoles cryptographiques sont utilisés**. Il doit également identifier les données traitées, leur sensibilité et leur durée de vie. L'objectif est de localiser toutes les instances de cryptographie (à clé publique et à clé secrète), y compris les dépendances cachées et les bibliothèques tierces.

Sans cette vue d'ensemble détaillée, l'organisation peut s'exposer à des risques de sécurité majeurs et à des échecs de migration coûteux car un inventaire précis assure que chaque composant vulnérable sera remplacé ou mis à jour. **La réussite de la migration PQC et la sécurité future de l'organisation dépendent de la qualité de cet inventaire initial**.

L'inventaire cryptographique étant la première étape clé pour la migration de la cryptographie actuelle à une cryptographie résistante aux ordinateurs quantiques, un plan d'action précis et strict doit être établi selon les besoins et la priorisation/criticité de chaque organisation. L'établissement d'un inventaire clair des actifs cryptographiques permettra à l'entreprise d'identifier de manière synthétique et proactive les risques et les défis posés par la transition vers la PQC, ainsi que d'être crypto-agile dans la planification des futurs changements des exigences cryptographiques. Cet inventaire est bien plus qu'une simple liste de certificats ; il cartographie l'ensemble du paysage cryptographique de l'organisation. L'inventaire permet d'identifier quelle cryptographie est utilisée par quelles applications et à quelles fins, ainsi que de cartographier l'utilisation de la cryptographie dans l'infrastructure. Il peut inclure des détails sur les mécanismes, les modes d'utilisation (ou toute autre méthode liée au mécanisme), les clés et leur stockage, les certificats et les versions de protocole.

Il est à noter que ce plan d'action ne considère pas l'usage de librairies obsolètes ou non maintenues, cela faisant partie de la gouvernance globale de la cybersécurité (et non uniquement de la cryptographie).

Le principe d'un inventaire est de :

- **Déterminer ce qu'on a** (algorithmes, clés, certificats etc.), où se trouvent ces éléments, quand ont-ils été créés, qui en est le propriétaire, et comment sont-ils utilisés dans le périmètre prédéfini ;
- **Déterminer ce qui est sous le contrôle de l'organisation** et doit être inventorié ;
- **Déterminer ce qui est en dehors du contrôle de l'organisation** et doit être documenté par les fournisseurs. Dans ce cas, des preuves doivent être demandées aux fournisseurs ;
- **Faciliter le suivi du patrimoine cryptographique d'une organisation** et donc les migrations quand un tel besoin apparait.

Plusieurs paramètres doivent être pris en considération pour la création d'un inventaire pertinent. Dans ce qui suit, nous présenterons certains de ces paramètres - mais la liste n'est pas exhaustive :

- **Identification du contenu :** Un inventaire cryptographique doit couvrir tous les assets pertinents. En général, cela inclura un inventaire des mécanismes cryptographiques et des méthodes associées, ainsi que des clés telles qu'elles sont utilisées dans les applications et l'infrastructure. Les certificats peuvent aussi faire partie du même inventaire. Comme l'objectif d'un inventaire cryptographique est également de contrôler une politique cryptographique, l'inventaire doit être aussi détaillé que la politique en question.
- **Identification du périmètre :** Si des parties tierces sont utilisées, l'inventaire doit se focaliser sur les parties gérées et sous la responsabilité de l'entreprise en question. Par exemple, dans le cas des solutions SaaS où le fournisseur cloud s'occupe de la génération et gestion des clés, l'inventaire de ces clés serait impossible pour le client de ce service ; dans ce cas, des mesures contractuelles doivent être mises en place afin de garantir que les exigences actuelles en termes de sécurité sont prises en compte (voir aussi « Couverture/faisabilité »).
- **Identification d'outillage :** Un inventaire peut être manuel ou automatique. Un inventaire automatique correctement effectué a par défaut tendance à être plus complet et plus facilement maintenable et monitoré par rapport à un inventaire manuel. Cependant, si des inventaires manuels existent déjà pour le périmètre identifié, ceux-ci doivent être examinés afin d'identifier s'ils peuvent être étendus. Un scanning peut aussi être utilisé pour créer et maintenir un inventaire. Cependant, les outils de scan peuvent présenter des angles morts, ce qui peut limiter leur efficacité. Malgré ces limitations, le scan peut être un outil précieux pour valider les inventaires, détecter les changements et mettre en évidence les erreurs. L'outillage doit être choisi selon les besoins, les ressources et la maturité de chaque entreprise.

- **Couverture/faisabilité :** Si la cryptographie d'un outil est invisible ou gérée par un tiers, il faut la considérer comme une boîte noire. L'inventaire ne doit recenser que les éléments que l'organisation contrôle directement. Pour tout le reste, la sécurité repose sur des contrats et des procédures de gestion des tiers (TPRM) : le fournisseur a l'obligation de respecter l'état de l'art et reste responsable en cas de défaut technique sur sa partie.
- **Politique d'inventaire :** Une politique doit accompagner l'inventaire afin de préciser différentes caractéristiques, comme par exemple le périmètre visé (application, infrastructure etc) ainsi que la fréquence de répétition d'un inventaire. En effet, un inventaire doit être maintenu et monitoré. La fréquence de la réalisation d'un inventaire doit être identifié dans la politique de l'inventaire selon les besoins et les capacités de chaque entreprise. Un inventaire au niveau applicatif doit fournir des informations relatives au service de sécurité mis en œuvre en utilisant la cryptographie pour l'application. Toute cette cryptographie impliquera des méthodes et clés spécifiques dont les informations doivent être consignées dans un inventaire cryptographique efficace. Dans le même esprit, un inventaire au niveau de l'infrastructure doit fournir des informations relatives à l'utilisation des mécanismes cryptographiques au niveau de l'infrastructure. Chacun de ces éléments nécessite une infrastructure de clés et de certificats qui doit être incluse dans un inventaire cryptographique. Un scan des différents échanges peut donc être réalisé (par exemple via un analyseur de réseau) à des fins d'inventaire. L'inclusion du hardware dans un inventaire cryptographique est aussi un aspect important à considérer.

La réalisation d'un inventaire « comporte » aussi plusieurs défis à prendre en considération :

- **Taux de couverture :** un inventaire cryptographique doit couvrir l'ensemble du périmètre donné. Par exemple, s'il s'agit d'un inventaire au niveau applicatif, l'ensemble du code de cette application doit être scanné et couvert par l'inventaire.
- **Accès aux vues :** La construction d'un inventaire nécessite la coopération de plusieurs parties prenantes au sein de l'organisation. L'accès peut être nécessaire au code, aux applications en cours d'exécution dans des environnements de test, aux systèmes de fichiers, etc. Un bon plan d'inventaire prendra en compte non seulement le « quoi » inventorié, mais également le « qui » doit participer à sa construction ainsi que « qui » a le droit de regarder les résultats.
- **Capacité de scan :** Des logiciels tiers peuvent être utilisés. La complétude de l'inventaire dépendra dans ce cas de la capacité à scanner le code source et/ou les bibliothèques appelées. Il est nécessaire d'avoir confiance dans les scanners utilisés, car les résultats doivent être fiables.
- **Efficacité :** Les faux positifs et les faux négatifs réduisent considérablement la valeur de l'inventaire, quel que soit le périmètre ou l'objectif de celui-ci. Ils peuvent entraîner une perte de temps sur des travaux de remédiation inutiles, des risques cryptographiques non détectés ou une non-conformité, ainsi qu'une priorisation erronée pour des projets de migration ou d'agilité.

- **Exploitation des résultats de l'inventaire :** L'inventaire a pour but d'identifier les éléments cryptographiques nécessitant une attention particulière. Lors de la réalisation d'un inventaire (surtout la première fois), plusieurs résultats non conformes sont attendus. Il est donc important de prioritiser les tâches de migration à effectuer, selon les priorités établies en interne et les capacités de l'entreprise. L'inventaire permet d'évaluer l'ampleur du travail, de planifier le remplacement et d'allouer les ressources nécessaires avec précision. Il doit permettre également d'identifier les dépendances de l'organisation considérée avec ses partenaires et fournisseurs, afin de se prémunir contre un risque de rupture d'interopérabilité.

Voici quelques exemples de tâches techniques à effectuer lors d'un inventaire (une liste plus complète est fournie dans l'Annexe 1) :

- **Définition du périmètre :** Identifier les systèmes, réseaux et applications dans le scope (interfaces publiques, VPN, systèmes internes, dispositifs IoT) et établir les exclusions.
- **Sélection des outils** : Choisir et déployer les outils de découverte : scanners de ports (e.g., Nmap), outils de découverte de certificats (e.g., ZGrab, crt.sh), solutions d'analyse statique du code (SAST) et solutions de gestion de clés/certificats (PKI/KMS). D'autres solutions CBOM et/ou SBOM peuvent être intégrées dans l'ensemble d'outillage utilisé pour l'inventaire.
- **Création du schéma de données :** Définir les attributs critiques à collecter pour chaque actif (algorithme, taille de clé, protocole et sa version, localisation, application associée, criticité métier, propriétaire, type de données protégées, sensibilité, durée de vie).

L'inventaire cryptographique est un socle stratégique pour la sécurité des SI. Il constitue un levier clé pour anticiper et piloter la transition vers des mécanismes PQC de manière maîtrisée et crypto-agile.

1.5 STRATÉGIE PQC ALIGNÉE SUR LA STRATÉGIE NATIONALE ET LA CONFORMITÉ UE

Dans cette section, on se focalise sur les recommandations émises au niveau européen (par la Commission européenne ou par des Etats membres) ainsi que sur l'étude de l'alignement des méthodes de migration par rapport à ces publications. Des feuilles de route publiées par des agences hors Union européenne sont présentées en Annexe 2.

1.5.1 Commission européenne

En juin 2025, les Etats membres de l'Union Européenne ont proposé une feuille de route pour la migration à la cryptographie post-quantique. Dans ce document, différents jalons sont définis et des éléments nécessaires pour les atteindre - le premier arrivant à son terme à la fin de 2026.

Étapes	Objectifs principaux	Délais
• Identifier et impliquer les parties prenantes • Soutenir une gestion mature des assets cryptographique • Créer un tableau de dépendances • Effectuer une analyse du risque quantique • Inclure la chaine d'approvisionnement • Créer un programme national de communication et sensibilisation • Partager la connaissance et être impliqué dans le groupe de travail de NIS CG sur des sujets PQC • Développer une feuille de route et un plan d'implémentation	• Initier un plan de migration PQC et les pilotes associés pour des cas d'usage avec un risque moyen et haut • Etablir un plan initial de migration PQC par tous les états membres	31 décembre 2026
• Mettre en place de la crypto-agilité et de mécanismes d'actualisation à distance • Allouer des ressources pour la transition • Adapter les schémas de certification • Adapter les lois et réglementations nationales relativement à la menace quantique • Identifier des opportunités dans l'écosystème • Prendre en considération les activités transversales tout au long de la création et de l'implémentation de la feuille de route • Implémenter des cas d'usage pilotes et contribuer à des centres de tests	• Finaliser la transition PQC pour les cas d'usage à haut risque • Finaliser le plan de la transition PQC et les pilotes pour les cas d'usage à risque moyen • Activer par défaut les mécanismes de mise à jour résistants aux attaques quantiques pour les logiciels et les progiciels	31 décembre 2030
[Des étapes précises ne sont pas identifiées dans le document initial]	• Compléter la transition PQC pour les cas d'usage avec un risque intermédiaire • Compléter (dans la mesure du possible) la transition PQC pour les cas d'usage avec un risque faible	31 décembre 2035

Ces étapes sont détaillées dans le document initial [1].

Le présent document s'aligne globalement aux objectifs présentés dans la feuille de route européenne. Cependant, pour faciliter l'implémentation, certaines étapes sont découpées pour prioriser des actions importantes dans l'immédiat. Afin de donner également une vision à long terme, la feuille de route du présent document va au-delà de 2030 (date à laquelle la feuille de route européenne s'arrête) avec quelques étapes supplémentaires à garder en tête pour une migration complète.

1.5.2 Etats membres

En plus de la Commission Européenne, certaines agences nationales ont également publié des recommandations autour des sujets de la migration vers une cryptographie résistante à la quantique.

ANSSI (France) [5] :

- 2027 : Mise en place d'obligations PQC pour l'entrée en qualification de produits.
- 2030 : L'ANSSI indique qu'il ne sera pas raisonnable d'acheter des produits qui n'intègrent pas de la PQC après 2030.

BSI (Allemagne) [2] :

- 2030 : Interdiction d'utiliser uniquement de la cryptographie classique sur les échanges de clés pour les infrastructures critiques. Passage obligatoire sur de l'hybride ou du full PQC.
- 2031 : Extension de la règle précédente à tous les usages. Le classique seul devient donc obsolète partout.
- 2035 : Fin de l'usage des signatures numériques en utilisant uniquement de la cryptographie classique.

NCSC-FI (Finlande) [6]:

- 2026 : Tous les produits évalués doivent intégrer un KEM et des signatures hybrides/ full PQC avec une forte recommandation d'hybridation.
- 2030 : Interdiction d'utiliser uniquement de la cryptographie classique sur les échanges de clés et les signatures pour les infrastructures critiques. Passage obligatoire sur de l'hybride ou du full PQC.
- 2035 : Toute la cryptographie à clé publique doit être résistante aux technologies quantiques indépendamment de la criticité des systèmes.

NCSC-NL (Pays-Bas) [3]:

- Alignement sur la feuille de route européenne.

1.5.3 Cadre réglementaire sur la migration post-quantique

A l'échelle européenne, la prise en compte de la PQC s'intègre dans un environnement réglementaire en cours de consolidation via NIS 2, DORA et CRA qui imposent aux organisations concernées de maintenir un niveau de sécurité pour leur patrimoine cryptographique qui soit adapté à l'état de la menace, et également d'être crypto-agile. Cela implique désormais d'anticiper le risque quantique et de l'ajouter dans les analyses de risques.

CRA (Cyber Resilience Act) :

- Entrée en vigueur 10 décembre 2024, obligations principales applicables dès le 11 décembre 2027.
- Périmètre : Tous produits connectés (hardware, software, IoT) commercialisés sur le marché européen
- Obligations cryptographiques : Reconnaissant les développements récents comme la feuille de route européenne sur la transition PQC ([1]) les groupes de travail de standardisation CRA se dirigent vers un modèle «State-of-the-Art Cryptography» (SOTA) incluant la cryptographie post-quantique. Les produits conformes au CRA peuvent supporter d'autres mécanismes cryptographiques, mais seuls les algorithmes state-of-the-art sont autorisés comme configuration par défaut sécurisée pour les produits connectés à Internet.

DORA (Digital Operational Resilience Act) :

- Entrée en vigueur janvier 2025
- Périmètre : Secteur financier européen (21 types d'entités dont banques, assurances, prestataires d'investissement, infrastructures de marché)
- Obligations cryptographiques :

(1) Développement d'une politique formelle de chiffrement et contrôles cryptographiques
(2) Création et maintien d'un inventaire cryptographique exhaustif
(3) Crypto-agilité obligatoire : capacité de remplacement rapide des algorithmes vulnérables
(4) Documentation justifiant l'usage de cryptographie classique (legacy systems) avec une évaluation annuelle de risques
(5) Référence explicite aux menaces quantiques dans les standards techniques réglementaires (RTS)

NIS 2

NIS 2 oblige à prendre les mesures de sécurité nécessaires et qui sont à l'état de l'art concernant la cryptographie.

- Périmètre : Infrastructures critiques, services essentiels, services numériques (cloud, DNS, datacenters)
- Le texte introduit de nouvelles obligations liées à la cryptographie comme notamment la crypto-agilité, un alignement sur les normes internationales, et la production d'une documentation obligatoire qui permettra de démontrer sa conformité.

Hors territoire européen, aux Etats Unis, le mémorandum présidentiel NSM-10 impose aux agences fédérales de migrer vers la PQC. Le mémorandum a été décliné en loi américaine 117-260 (12/21/2022), le « Quantum Computing Cybersecurity Preparedness Act » [7].

1.6 PLANIFICATION DE LA MIGRATION

Les étapes préliminaires : sensibilisation des équipes (Section 1.1), mise en place de la gouvernance (Section 1.2), évaluation de la maturité cryptographique et des risques (Section 1.3) ont permis à l'organisation de prendre la mesure de son exposition et de poser les fondations nécessaires à une transition maîtrisée. Sur cette base, il est déjà possible d'amorcer une première version du plan de migration. Il est important de noter que la planification ne nécessite pas d'attendre la complétion d'un inventaire exhaustif (Section 1.4). Un inventaire préliminaire est suffisant pour identifier les priorités évidentes, structurer les premières décisions et mobiliser les ressources. L'inventaire complet, complété avec des outils spécialisés et exhaustif, viendra ensuite affiner et consolider ce plan.

La présente section se décline en deux volets complémentaires (organisationnel et technique) et vise à **permettre à chaque organisation de dresser sa feuille de route de migration PQC,** un document vivant, destiné à évoluer à chaque fin de phase en fonction des retours d'expérience, des évolutions des standards et des contraintes réglementaires émergentes.

1.6.1 Planification organisationnelle

Étape 1 : Structurer la gouvernance et mobiliser les ressources

Nomination d'un responsable de migration. Nommer un profil à double compétence technique et organisationnelle, distinct du RSSI, disposant d'un accès direct aux instances de décision et travaillant en coordination étroite avec le comité de pilotage décrit en Section 1.2.

Budget initial et allocation des ressources. Un budget initial doit être formalisé dès cette phase. Les principales catégories à couvrir sont :

- Ressources humaines internes et expertises externes (cryptographes, architectes sécurité) ;
- Licences et outillage (scanners, PKI, outils SAST) ;
- Infrastructure de test et coûts de transition ;

Une estimation indicative est fournie en Section 1.7.

Coordination avec l'écosystème. La migration implique d'engager l'ensemble des partenaires (qui produisent ou consomment des opérations cryptographiques) en amont:

- Fournisseurs SaaS/Cloud : obtenir leurs feuilles de route PQC et exiger un CBOM (Cryptographic Bill of Materials) ;
- Partenaires partageant des canaux chiffrés : coordonner les calendriers pour éviter toute rupture d'interopérabilité ;
- Prestataires de confiance (IGC, HSM) : vérifier leur support des algorithmes standardisés (ex : ML-KEM, ML-DSA, SLH-DSA) dans les délais requis.

Étape 2 : Aligner sur les jalons réglementaires européens et définir les KPIs

Jalons réglementaires européens [1]. Le plan doit être ancré sur les échéances de la feuille de route européenne, qui constituent des engagements et non des objectifs indicatifs (voir aussi Section 1.5) :

- Fin 2026 : plan de migration finalisé, pilotes lancés pour les cas à risque élevé ;
- Fin 2030 : migration PQC/hybride achevée pour tous les systèmes à risque élevé ;
- Fin 2035 : généralisation aux systèmes à risque moyen et faible.

Indicateurs de pilotage (KPIs). Un tableau de bord doit être mis en place dès le lancement du programme. Les indicateurs recommandés couvrent a minima : le taux de couverture de l'inventaire, le nombre d'actifs pour lesquels une décision de migration a été formalisée, le pourcentage de systèmes à risque élevé en mode hybride, le nombre de fournisseurs ayant confirmé leur roadmap PQC, et le respect des enveloppes budgétaires par phase.

1.6.2 Planification technique

Étape 3 : Prioriser les actifs à migrer

À partir des données de l'inventaire, chaque actif est classé selon trois critères : la durée de vie des données qu'il protège (priorité aux systèmes exposés à la menace SNDL), son niveau d'exposition, et ses dépendances vis-à-vis d'autres composants (IGC racine, HSM, bibliothèques).

Classification par niveau de risques :

Etapes	Objectifs principaux	Délais
Elevé	Systèmes exposés sur Internet, PKI/IGC, signatures de code, VPN	Fin 2030
Moyen	Systèmes internes à données sensibles (RH, juridique, R&D)	Fin 2035
Faible	Systèmes internes à faible criticité, données à durée de vie courte	Fin 2035

Évaluation des dépendances : identifier les systèmes qui ne peuvent migrer qu'après la mise à jour d'un fournisseur tiers ou d'une bibliothèque spécifique.

Étape 4 : Formaliser une décision par actif

Pour chaque actif vulnérable, une décision est documentée dans le registre cryptographique avec son justificatif, son responsable et son échéance :

- Migrer : remplacement des algorithmes vulnérables, en mode hybride par défaut ;
- Décommissionner : retrait de l'actif si sa fin de vie coïncide avec la migration ;
- Maintenir temporairement : si la migration n'est pas immédiatement réalisable, définir des mesures compensatoires (isolation réseau, réduction de durée de vie des certificats, surveillance renforcée) et une fiche de risque avec échéance de traitement définitif.

Étape 5 : Sélectionner les solutions et les fournisseurs

Le choix des solutions doit s'appuyer sur les critères suivants :

- Conformité aux standards finalisés (ex : FIPS 203/ML-KEM, FIPS 204/ML-DSA, FIPS 205/SLH-DSA) et aux obligations réglementaires ;
- Agilité native : capacité à mettre à jour les algorithmes sans refonte architecturale ;
- Disponibilité d'un CBOM et transparence sur la roadmap d'évolution ;
- Compatibilité matérielle (HSM, équipements réseau, terminaux contraints).

Pour les cas d'usage sans solution commerciale conforme disponible, initier un développement interne en parallèle avec une veille marché régulière. Pour l'outillage, se référer au Panorama produit par le GT Cryptographie post-quantique du Campus Cyber.

Étape 6 : Définir la stratégie de déploiement

L'hybridation constitue le mode de transition par défaut : elle combine un algorithme classique et un algorithme post-quantique au sein d'un même protocole, garantissant la sécurité tant qu'au moins l'un des deux résiste. Le déploiement suit ensuite une logique de vagues successives :

- Systèmes à risque élevé traités en priorité, par lots fonctionnels cohérents ;
- Validation systématique en pré-production (tests fonctionnels, de performance et d'interopérabilité) avant toute mise en production ;
- Plan de retour arrière formalisé pour chaque vague, activable en cas d'incident.

L'agilité cryptographique est menée en programme parallèle, et non comme prérequis bloquant, avec pour objectif de permettre le futur remplacement d'un algorithme sans refonte majeure.

1.7 BUDGET INITIAL ET ALLOCATION DES RESSOURCES

Le tableau suivant présente **une estimation à titre indicatif**, calibrée sur le profil d'une organisation de taille intermédiaire (environ 10 000 collaborateurs, un datacenter principal). Elle est destinée à servir de modèle de structuration, non de référence chiffrée.

Catégorie de coût	Pourcentage du coût global	Détail technique / rôle
Ressources humaines	~60%	Cryptographes/Architectes Sécurité (Externes) : expertise PQC, design du registre. Chefs de Projet IT/Sécurité (Internes) : Coordination. Analystes/Ingénieurs Systèmes : Déploiement des outils de scan et collecte des données
Outils et licences	~25%	Logiciels de gestion IGC/Certificats (CM) : Licences pour la découverte automatique et l'inventaire permanent. Outils SAST : Analyse du code pour les appels cryptographiques. Scanners Réseau : Identification des endpoints SSL/TLS.

Frais opérationnels	~15%	Infrastructure de test (pour le pilote), documentation de conformité, formations spécialisées des équipes internes sur la méthodologie PQC.
Total estimé du projet d'inventaire		(varie selon le niveau de shadow it et la complexité des systèmes legacy)

1.7.1 Ordres de grandeur issus de la littérature internationale

Les estimations ci-dessous sont issues de sources académiques et institutionnelles reconnues. Elles doivent être interprétées avec précaution : les contextes (organisationnel, géographique, sectoriel) varient significativement, et **aucun chiffre universel ne peut se substituer à une estimation propre à chaque organisation.**

BCG projette les coûts de transition PQC entre 2,5 % et 5 % du budget IT annuel, sur la base des premiers retours d'expérience et des enseignements tirés de la transition Y2K. Pour une organisation disposant d'un budget IT annuel d'un milliard de dollars, cela représente environ 25 millions de dollars en cas de démarrage anticipé et potentiellement le double, soit 50 millions, en cas de retard jusqu'en 2035 [8].

Selon le Trusted Computing Group, les organisations tendent à prioriser les systèmes d'IAM (Identity and Access Management) comme premier périmètre de protection, avec des budgets PQC représentant entre 6% et 10% des dépenses totales cyber [9].

Le gouvernement américain a estimé le coût de la migration PQC pour l'ensemble des agences fédérales à 7,1 milliards de dollars [10], un chiffre issu des premiers inventaires soumis par les agences concernées dans le cadre du Quantum Computing Preparedness Act [7]. Ce montant illustre l'ampleur de l'effort pour des organisations disposant de SI complexes et étendus.

Au-delà des coûts technologiques directs (matériel, licences, intégration), les organisations doivent anticiper le développement des compétences, la gestion des interruptions de service, le fonctionnement en parallèle pendant les phases de **transition, et les coûts de maintenance des environnements hybrides.**

1.7.2 Le coût de l'inaction

Si le coût de la migration peut sembler significatif, il doit être mis en regard du coût potentiel de l'inaction. Citi Institute estime **qu'une seule cyberattaque quantique sur une grande banque américaine pourrait générer entre 2 000 et 3 300 milliards de dollars de pertes économiques indirectes** (soit 10 à 17 % du PIB américain) à la suite d'une interruption d'une seule journée d'accès au réseau Fedwire [11]. Citi Institute qualifie la menace quantique d'événement à faible probabilité mais à sévérité extrême, comparable aux rares crises financières aux conséquences systémiques, et souligne que la comparaison avec Y2K sous-estime largement l'exposition réelle.

Par ailleurs, retarder la transition ne fait que prolonger l'exposition au risque : cela peut doubler le coût de la migration elle-même. BCG avertit explicitement que démarrer en 2030 sera déjà trop tard pour bénéficier d'une transition maîtrisée.

1.7.3 Conseils pour estimer son propre budget PQC

L'estimation du budget de migration doit tenir compte des facteurs suivants, dont l'importance relative varie selon chaque organisation :

Facteurs d'ampleur :

- Volume et complexité de l'inventaire cryptographique (nombre de systèmes, présence de shadow IT, legacy) ;
- Proportion de systèmes nécessitant une mise à niveau matérielle (HSM, équipements réseau, terminaux contraints) ;
- Dépendances fournisseurs et délais d'obtention de solutions conformes.

Facteurs de coûts souvent sous-estimés :

- Fonctionnement en mode hybride pendant la période de transition (double infrastructure temporaire) ;
- Migration de l'infrastructure hybride à une infrastructure PQC selon le degré de crypto-agilité des systèmes ;
- Formation et montée en compétence des équipes (cryptographes, architectes, administrateurs systèmes) ;
- Tests de régression, de performance et d'interopérabilité avant chaque mise en production ;
- Gestion du changement et communication interne.

Approche recommandée :

- Construire une estimation par phase et par périmètre, révisée annuellement ;
- Intégrer la migration PQC dans les cycles naturels de renouvellement des contrats et des infrastructures, afin de mutualiser les coûts ;
- Distinguer les coûts récurrents (maintien de l'agilité, surveillance, mises à jour) des coûts non récurrents liés à la migration initiale.

< 2. DÉMARRAGE AU DÉPLOIEMENT (2026-2027)>

La phase de démarrage du déploiement marque la transition entre la phase de préparation et l'entrée dans la mise en œuvre opérationnelle (à grande échelle) de la PQC. L'objectif principal de cette phase est de **valider les hypothèses formulées lors de la préparation/ évaluation, de structurer les process de déploiement et de poser les bases d'une migration.**

2.1 DÉPLOIEMENT PILOTE

Le déploiement pilote constitue la première brique d'une mise en production des mécanismes post-quantiques. Cela vise à valider, dans des conditions proches de la production, la faisabilité technique, la stabilité des services et de l'impact du déploiement des mécanismes post-quantiques.

Les mécanismes cryptographiques choisis lors de ces pilotes doivent combiner des schémas traditionnels et post-quantiques. Cette hybridation permet de réduire/limiter les risques liés à l'adoption de nouvelles technologies pas assez matures. L'exploitation du pilote permet de mettre en évidence les adaptations nécessaires des outils/systèmes/ infrastructures existants afin de supporter durablement la PQC. Ces adaptations doivent être documentées, avec un niveau de détail incluant les indicateurs techniques et organisationnels d'une telle migration. Ces indicateurs techniques traduiront la réaction du SI à l'augmentation des tailles de clés, des certificats, des messages échangés, à la variation dans la consommation de RAM, stack, consommation d'énergie (notamment dans le cas des terminaux contraints), etc. Ces indicateurs peuvent être par exemple la latence, la consommation de ressources système/réseaux.

Ces pilotes seront donc utilisés pour déterminer la faisabilité, permettre l'alignement des fournisseurs, les priorités pour la migration, les coûts, et les risques inhérents à l'adoption de la PQC. Globalement, **ces pilotes vont aussi servir à aider les organisations à préparer un meilleur plan de migration.**

2.2 DÉMARRAGE DE LA MISE EN PLACE DE L'AGILITÉ CRYPTOGRAPHIQUE

La mise en place de l'agilité cryptographique (ou la crypto-agilité) constitue un élément central pour assurer la pérennité du programme de la migration post-quantique mais aussi une meilleure gouvernance cryptographique. Dans un contexte où les standards et leurs différentes implémentations évoluent rapidement, et sans réel niveau de maturité, **les organisations doivent être en mesure d'adapter leurs choix cryptographiques sans refonte majeure de l'infrastructure** (code, hardware etc.). La crypto-agilité est donc un concept clé pour cette adaptation.

Sur le plan technique, l'agilité cryptographique implique l'utilisation d'abstractions cryptographiques (fonctions crypto génériques avec algorithme, taille de clé, en paramètres) au sein des applications et de l'infrastructure. Les algorithmes ne doivent pas être codés/intégrés en dur dans le code ou les configurations, mais intégrés via des mécanismes modulaires/configurables. Cette approche est faite afin de faciliter les mises à jour futures de composants cryptographiques, de rebondir rapidement en cas d'obsolescence des algorithmes/librairies, et aussi de changer, dans le cas de la PQC, d'algorithme si les standards actuels s'avèrent vulnérables (par exemple aux attaques par canaux auxiliaires ou d'autre type d'attaques).

Toutefois, il est important de souligner que **la mise en place de la crypto-agilité représente un chantier technique et organisationnel important.** Une approche trop ambitieuse dès les premières phases du programme de transition, peut ralentir, voir devenir un obstacle au déploiement des mécanismes post-quantiques. Donc la crypto-agilité ne doit pas être définie comme un prérequis absolu à la migration PQC, mais un objectif progressif à atteindre en parallèle de la transition PQC. Le but est donc de définir un seuil minimal de crypto-agilité à construire pour permettre la migration post-quantique sans avoir à remplacer toute l'infrastructure utilisée jusqu'à présent et sans retarder la migration PQC. Il faut donc faire une évaluation afin de quantifier les efforts à fournir pour la crypto-agilité (durée, complexité, impacts sur l'infrastructure/architecture, coûts) sans pour autant nuire à la migration PQC de l'infrastructure. Dans le cadre de la création des nouveaux systèmes, la crypto-agilité doit être intégrée « by design », alors que pour des systèmes existants il faudra veiller à ce que la crypto-agilité ne retarde pas la migration PQC (en prenant en compte les ressources humaines et financières mises à disposition).

La crypto-agilité est une notion à prendre en compte tout au long de la migration PQC et devrait être intégrée dans la gouvernance cybersécurité. Il s'agit donc d'un projet à part entière, doté d'une feuille de route dédiée, à mener conjointement à la transition vers le PQC en fonction des ressources disponibles.

2.3 LANCEMENT DE LA MISE À JOUR DES COMPOSANTS CRITIQUES

Une fois les pilotes achevés, il faudra commencer à migrer un ensemble sélectionné de systèmes critiques (à haut risque) déjà identifiés dans l'analyse de risque pour la migration PQC.

On utilise l'expérience de la migration de ces composants critiques pour documenter les coûts, les défis opérationnels rencontrés et les dépendances vis-à-vis des solutions/fournisseurs. Il faudra intégrer ces informations dans la feuille de route globale de l'organisation pour la migration à grande échelle.

< 3. MIGRATION DES SYSTÈMES CRITIQUES (2028-2030)>

Cette phase se concentre sur les périmètres présentant les niveaux de risques les plus élevés (exposition, fonctions essentielles, criticité). **L'objectif principal de cette phase est de réduire de manière significative l'exposition aux menaces quantiques sur ces périmètres.** Cette période marque aussi le renforcement des exigences de sécurité concernant les nouveaux projets, les acquisitions à partir de 2027.

3.1 MIGRATION HYBRIDE/PQC TERMINÉE POUR LES SYSTÈMES À RISQUE ÉLEVÉ

La migration des systèmes à risque élevé constitue la priorité pour cette phase. Ces systèmes, par leur criticité, de la sensibilité des données traitées, ou de leur exposition aux menaces (protocoles exposés à internet "menace SNDL"), nécessitent une priorisation pour la migration. Des exemples pour ces systèmes à risque élevé :

- la PKI (Infrastructure à clé publique) à laquelle il faudra soit ajouter des certificats hybrides, soit deux chaînes de certificats (l'une en cryptographie traditionnelle, l'autre en PQC) ;
- les signatures numériques ;
- les protocoles exposés sur internet etc.

L'ajout de mécanismes cryptographiques hybrides à ces systèmes permet d'assurer un niveau de sécurité élevé face aux ordinateurs quantiques tout en limitant, durant la période pré-quantique, les risques liés à l'introduction d'algorithmes encore en phase de standardisation ou n'ayant pas encore atteint une pleine maturité. L'hybridation est recommandée par l'ANSSI en particulier pour les produits de sécurité destinés à offrir une protection durable des informations à l'horizon 2030 et au-delà ou qui seront potentiellement utilisés après 2030 sans possibilité de mise à jour.

3.2 CONFORMITÉ PQC DES NOUVEAUX PRODUITS ACHETÉS

A partir de 2027, les solutions ne disposant pas de mécanismes compatibles avec la PQC (mécanismes hybrides ou exclusivement en PQC) ne sont plus éligibles aux processus de qualification de sécurité de l'ANSSI [5] ; ce qui impose une adaptation de sélection des fournisseurs afin de garantir que les nouveaux produits, solutions et services intégrés dans le SI soient résistantes aux technologies quantiques. Cette contrainte limite l'intégration de dépendances cryptographiques legacy dans le SI.

< 4. GÉNÉRALISATION & FINALISATION (2030-2035) >

Cette phase correspond à l'achèvement du programme de migration vers la PQC. Elle vise à **finaliser la migration des systèmes à risque moyen et faible, et à stabiliser les déploiements à grande échelle, puis de préparer progressivement la transition vers des solutions exclusivement post-quantiques (**sans utilisation de l'hybridation).

4.1.MIGRATION PQC/HYBRIDATION TERMINÉE POUR LES SYSTÈMES À RISQUE MOYEN

La migration des systèmes à risque moyen constitue une priorité de la phase de généralisation. Conformément à la proposition de feuille de route EU [1], l'objectif est d'atteindre un niveau de transition aussi complet que possible pour ces cas d'usage d'ici 2035. Cette échéance s'inscrit dans une convergence des feuilles de routes (celle des Etats-Unis ainsi que la proposition européenne) qui fixent l'horizon 2035 comme cible pour la réduction maximale du risque quantique et la fin progressive de l'usage cryptographique traditionnel (legacy à partir de 2030). Les renouvellements logiciel et matériel du SI (e.g. rachat de licences, renouvellement des contrats auprès de prestataires etc), les mises à jour des produits (e.g. via un mécanisme de mise à jour) et les nouveaux déploiements doivent être systématiquement résistants aux technologies quantiques.

4.2 MIGRATION ACHEVÉE POUR LES SYSTÈMES À RISQUE FAIBLE

En parallèle, la transition des systèmes à risque faible vise à couvrir le plus grand périmètre possible avant l'échéance de 2035. Bien que leur criticité soit plus limitée, ces systèmes représentent un grand volume des infrastructures existantes. Cette transition contribue à réduire la dépendance aux mécanismes cryptographiques traditionnels (qui seront considérés obsolètes à partir de 2030) et d'avoir un parc intégrant les algorithmes PQC.

4.3 PASSAGE AUX ALGORITHMES PQC SEULS

Conformément à la phase 3 de la transition vers la PQC de l'ANSSI [12], cette étape consiste à évaluer la possibilité de passer des modèles d'hybridation vers des modèles reposant exclusivement sur des algorithmes PQC lorsque leur niveau de maturité sera jugé équivalent à celui des algorithmes traditionnels (de type RSA, ECDSA, ECDH). L'objectif n'est donc pas une généralisation immédiate de l'abandon de l'hybridation, mais l'identification des cas d'usage pour lesquels on peut se permettre d'avoir exclusivement de la PQC. Pour les actifs qui ne peuvent pas être migrés vers la PQC, les organisations doivent adopter une gestion de risques combinant des mesures intermédiaires résistantes aux ordinateurs quantiques avec des plans de transformation à long terme. Si possible, prévoir une dégradation progressive menant à la mise hors service de ces actifs selon l'analyse de risques effectuée. Il sera également possible de faire de l'hybridation en combinant exclusivement des algorithmes PQC. Cela permet d'assurer une résistance aux attaques quantiques tout en maintenant une sécurité globale dans le cas où l'un des deux algorithmes serait cassé. Il s'agit d'une approche déjà évoquée dans certains articles académiques, mais à l'heure de l'écriture de ce document, ceci n'est qu'une possibilité.

< ANNEXE 1 : LISTE DÉTAILLÉE DES TÂCHES >

Dans cette section, nous présentons quelques exemples de tâches techniques à effectuer:

Tâches technique	Description
Définition du périmètre	Identifier les systèmes, réseaux et applications in-scope (interfaces publiques, VPN, systèmes internes, dispositifs IoT) et établir les exclusions.
Sélection des outils	Choisir et déployer les outils de découverte : scanners de ports (e.g., nmap), outils de découverte de certificats (e.g., zgrab, crt.sh), solutions d'analyse statique du code (sast) et solutions de gestion de clés/certificats (pki/kms). si des outils de découverte existaient déjà, les mettre à jour pour compléter l'inventaire.
Configuration des accès	Obtenir les accréditations et permissions nécessaires pour les scans non-intrusifs et l'accès aux dépôts de code source et aux configurations serveurs.
Création du schéma de données	Définir les attributs critiques à collecter pour chaque actif (algorithme, taille de clés, protocole et sa version, localisation, application associée, criticité métier, propriétaire).
Scan réseau et ponts d'accès	Identifier et analyser les services réseau exposant une cryptographie : ports SSL/TLS (443, 8443, etc.), sessions SSH, VPN, et tout service utilisant un canal chiffré.
Inventaire des certificats	Extraction systématique des métadonnées de tous les certificats (X.509) dans les HSM, les serveurs d'applications, les key stores et les trust stores.
Analyse du code et des binaires	Utiliser des outils SAST pour parcourir les dépôts de code afin de détecter les bibliothèques cryptographiques utilisées (e.g., OpenSSL, Bouncy Castle, librairies internes) et les appels d'API cryptographiques spécifiques.
Inspection des configurations	Analyser les fichiers de configuration des serveurs web (Apache, Nginx, IIS), des bases de données et des OS pour documenter les suites de chiffrement et les protocoles autorisés (TLS 1.2/1.3, etc.).
Identification des actifs froids	Découverte des clés et certificats utilisés pour l'archivage de données, la signature de code ou les accès offline.
Classification algorithmique	Catégorisation de chaque actif par type d'algorithme (RSA, ECC, SHA, AES, etc.) et par taille de clé (e.g., RSA-2048, ECC P-256).
Cartographie des dépendances	Créer des liens clairs entre les certificats, les clés, les applications qui les consomment et les bibliothèques sous-jacentes. Cibler les dépendances indirectes (transitives).
Identification des vulnérabilités PQC	Isoler spécifiquement tous les actifs utilisant de la cryptographie à clé publique non résistante au quantique (RSA, ECC, Diffie-Hellman), qui nécessiteront une migration PQC.

Tâches technique	Description
Attribution des métadonnées	Enrichir les entrées avec la criticité métier (impact en cas de panne) et la fenêtre de maintenance (facilité/difficulté de mise à jour).
Normalisation des données	Nettoyer et harmoniser les données hétérogènes des différents outils de découverte pour garantir leur uniformité.
Création du registre crypto-graphique	Importer toutes les données vérifiées dans un registre centralisé (souvent une base de données ou une CMDB dédiée).
Génération du rapport d'inventaire	Produire le document final incluant : la liste exhaustive des actifs, la cartographie des dépendances, la quantification des actifs vulné-rables PQC et une proposition de priorisation pour la remédiation.
Validation par les propriétaires	Revue finale du registre avec les équipes IT et les propriétaires d'applications pour valider l'exactitude des informations et préparer les plans de remédiation (hybridation et migration PQC).

< ANNEXE 2 : FEUILLES DE ROUTE HORS UE >

Dans cette section, nous présenterons des feuilles de route pour la migrations originaires en dehors des frontières de l'Union européenne.

Pays / Région	Entité	Date de publication	Titre de la roadmap	Echéances clés
Royaume-Unis	NCSC	2025	Timelines for migration to post-quantum cryptography [13]	2028 : Inventaire et planification ; 2031 : Migration prioritaire ; 2035 : Fin de migration globale.
Etats-Unis	NSA	2025	Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) [14]	2030 : Équipements réseaux et signatures logicielles ; 2033 : OS et Cloud ; 2035 : Transition totale.
Australie	ASD / ACSC	2025	Planning for post-quantum cryptography [15]	2026 : Plan raffiné ; 2030 : Fin de la cryptographie asymétrique traditionnelle.
Canada	Centre canadien pour la cyber	2025	Roadmap for the migration to PQC for the Gov. of Canada [16]	2026 : Plans départementaux ; 2031 : Systèmes prioritaires ; 2035 : Systèmes restants.
G7 (Finance)	G7 Cyber Expert Group	2026	Advancing a Coordinated Roadmap for PQC in the Financial Sector [17]	2030-2032 : Priorisation des systèmes critiques financiers ; 2035 : Cible globale.
Inde	National Quantum Mission	2026	Implementation of Quantum Safe Ecosystem in India [18]	2027-2029 : Infrastructures critiques (CII) ; 2033 : Entreprises régulières.

< ANNEXE 3 : GUIDES/ PRATIQUES DE MIGRATION ET CADRES DE PRÉPARATION >

France (ANSSI) :
- Avis de l'ANSSI sur la transition vers la cryptographie post-quantique. Document soulignant l'importance stratégique de l'hybridation. [12]
- Point de vue de l'ANSSI sur la crypto-agilité. Recommandations de l'ANSSI concernant la crypto-agilité [19]
- FaQ sur la cryptographie post-quantique. [5]

Pays-Bas (AIVD / TNO) : The PQC Migration Handbook. Manuel pratique pour l'inventaire des actifs et l'exécution technique. [3]

Singapore (CSA) : The Post-Quantum Cryptography Migration Starts Today. Rapport du groupe de travail DGX sur les étapes initiales de préparation gouvernementale. [20]

Belgique (Cyber Security Coalition) : Preparing for the Quantum Era: A Practical Guide to Post-Quantum Cryptography. Guide à destination des entreprises privées pour structurer leur stratégie. [21]

États-Unis (NIST) : Considerations for Achieving Crypto Agility: Strategies and Practices (CSWP 39). White paper destiné aux exécutifs, architectes et développeurs pour structurer une approche d'agilité cryptographique dans le cadre de la transition PQC. [22]

Union européenne (Europol) : Post Quantum Cryptography. Rapport d'analyse sur l'état de la cryptographie post-quantique et ses implications pour les institutions européennes. [23]

Cryptomathic (Série «A Banker's Guide to Quantum-Safe Cryptography») :
- Partie 1 : The Compliance Mandate for PQC Migration. Analyse des moteurs réglementaires (DORA, NIS2) pour le secteur bancaire. [lien]
- Partie 2 : Roadblocks and Strategic Solutions. Étude des obstacles à l'agilité cryptographique et des solutions de gestion centralisée. [lien]
- Partie 3 : Roadmap to PQC Migration for Financial Institutions. Cadre opérationnel pour structurer la transition dans les systèmes financiers. [lien]

< BIBLIOGRAPHIE>

[1] «A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (Part 1, Version 1.1),» 2025. [En ligne]. Available: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

[2] «Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography,» Federal Office for Information Security (BSI).

[3] AIVD CWI TNO, «The PQC Migration Handbook,» December 2024. [En ligne]. Available: https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf.

[4] Campus Cyber, «Matrice d'évaluation du niveau de maturité d'une organisation en matière de PQC,» 2024. [En ligne]. Available: https://wiki.campuscyber.fr/Matrice_d%27%C3%A9valuation_du_niveau_de_maturit%C3%A9_d%27une_organisation_en_mati%C3%A8re_de_PQC.

[5] ANSSI, «FAQ de l'ANSSI sur la PQC,» Octobre 2025. [En ligne]. Available: https://cyber.gouv.fr/enjeux-technologiques/cryptographie-post-quantique/faq-pqc/

[6] «Suomen kansallisen kryptotyöryhmän linjaukset kansallisiin PQC-salaustuotearviointeihin,» Octobre 2025. [En ligne]. Available: https://www.kyberturvallisuuskeskus.fi/fi/uutiset/suomen-kansallisen-kryptotyoryhman-linjaukset-kansallisiin-pqc-salaustuotearviointeihin-112026-alkaen

[7] United States, Congress, House., «H.R.7535 - Quantum Computing Cybersecurity Preparedness Act,» 2022. [En ligne]. Available: https://www.congress.gov/117/plaws/publ260/PLAW-117publ260.pdf.

[8] Boston Consulting Group (BCG), «How Quantum Computing Will Upend Cybersecurity,» 2025. [En ligne]. Available: https://www.bcg.com/publications/2025/how-quantum-computing-will-upend-cybersecurity.

[9] Trusted Computing Group (TCG), «State of PQC Readiness 2025,» 2025.

[10] The White House, «REPORT ON POST-QUANTUM CRYPTOGRAPHY,» 2024. [En ligne]. Available: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf.

[11] Citi Institute, «Quantum Threat The Trillion-Dollar Security Race Is On,» 2026. [En ligne]. Available: https://www.citigroup.com/rcs/citigpa/storage/public/Citi_Institute_Quantum_Threat.pdf.

[12] ANSSI, «Avis de l'ANSSI sur la migration vers la cryptographie post-quantique,» Agence nationale de la sécurité des systèmes d'information, 2023

[13] «Timelines for migration to post-quantum cryptography,» 2025. [En ligne]. Available: https://www.ncsc.gov.uk/guidance/pqc-migration-timeline

< BIBLIOGRAPHIE>

[14] «Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) Algorithms,» National Security Agency (NSA), 2025.

[15] ASD, «Planning for post-quantum cryptography,» Septembre 2025. [En ligne]. Available: https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography.

[16] Gouvernement du Canada, «Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001),» Juin 2025. [En ligne]. Available: https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001

[17] «G7 Cyber Expert Group Statement on Advancing a Coordinated Roadmap for the Transition to PQC in the Financial Sector,» G7 Cyber Expert Group, 2026

[18] Department of science & technology, «Implementation of Quantum Safe Ecosystem in India,» février 2026. [En ligne]. Available: https://dst.gov.in/sites/default/files/Report_TaskForce_PQMigration_4Feb26%20%28v1%29.pdf.

[19] ANSSI, «ANSSI's views on crypto-agility - For developers and systems architects,» 2026. [En ligne]. Available: https://messervices.cyber.gouv.fr/documents-guides/ANSSI-views-on-crypto-agility.pdf.

[20] Groupe de travail DGX de CSA - Singapour, «The Post-Quantum Cryptography - version 1.0,» Septembre 2024. [En ligne]. Available: https://isomer-user-content.by.gov.sg/85/6877c87b-44d9-4fbe-98c6-53c2704b8446/DGX_2024_Cyber_Working_Group_Report.pdf.

[21] Belgium's cyber security coalition, «Preparing for the quantum era: a practical guide to Post-Quantum Cryptography,» Septembre 2025. [En ligne]. Available: https://cybersecuritycoalition.be/wp-content/uploads/CSC-WP-Post-Quantum-Crypto_300925_FINAL.pdf

[22] NIST, «Considerations for Achieving Crypto Agility: Strategies and Practices (CSWP 39),» Décembre 2025. [En ligne]. Available: https://csrc.nist.gov/pubs/cswp/39/considerations-for-achieving-cryptographic-agility/final

[23] QSFF , «Prioritising Post-Quantum Cryptography migration activities in financial services,» 2026. [En ligne]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/Post-quantum-cryptography-report.pdf

[24] Maveris Labs, Budgeting for a PQC Future, 2024.

< REMERCIEMENTS >

Le Campus Cyber adresse ses remerciements aux contributrices et contributeurs du Groupe de travail « Guide de migration vers la cryptographie post-quantique » :

- Air France KLM
- AXA
- Banque de France
- BNP Paribas
- CryptoNext Security
- Eviden
- Orange Cyberdefense
- Portyq
- QuRISK

CAMPUS CYBER

POUR EN SAVOIR PLUS : **WIKI.CAMPUSCYBER.FR**
ADRESSE MAIL DE CONTACT : **COMMUNAUTES@CAMPUSCYBER.FR**
5 - 7 RUE BELLINI 92800, PUTEAUX

CE PROJET A ÉTÉ FINANCÉ PAR LE GOUVERNEMENT
DANS LE CADRE DU PROGRAMME D'INVESTISSEMENTS D'AVENIR