CRYPTOSPHERE

Guide de migration post-quantique

Préparer votre infrastructure critique pour l'ère quantique

Version 2026.1 — Mars 2026

cryptops.fr

Sommaire

1. Pourquoi migrer maintenant ?

La menace « Harvest Now, Decrypt Later »

Des adversaires étatiques et privés collectent dès aujourd'hui des données chiffrées en transit, en vue de les déchiffrer ultérieurement lorsque des ordinateurs quantiques suffisamment puissants seront disponibles. Les organisations manipulant des données à long cycle de vie — défense, santé, finance, propriété intellectuelle — sont les premières exposées.

Calendrier ANSSI : hybridation obligatoire horizon 2030

L'ANSSI recommande l'adoption d'une approche hybride (classique + post-quantique) comme mesure transitoire immédiate, et préconise la migration complète des systèmes classifiés avant 2030. Les visas de sécurité CSPN et CC intégreront les exigences PQC dans leurs critères d'évaluation.

NIS2 et DORA imposent la résilience cryptographique

La directive NIS2 (applicable depuis octobre 2024) exige des entités essentielles qu'elles évaluent les risques liés aux technologies émergentes, incluant explicitement la menace quantique. Le règlement DORA, spécifique au secteur financier, impose des tests de résilience intégrant les scénarios de compromission cryptographique.

Horizon 2030-2035 : ordinateurs quantiques cryptographiquement pertinents

Les estimations convergent vers 2030-2035 pour l'apparition d'un ordinateur quantique capable de casser RSA-2048 et ECC via l'algorithme de Shor. Les algorithmes RSA, ECC et Diffie-Hellman, qui protègent la quasi-totalité des communications numériques, seront alors obsolètes.

> **La formule de Mosca :** Si la durée de confidentialité requise de vos données (x) plus le temps nécessaire pour migrer (y) dépasse le délai avant l'arrivée d'un ordinateur quantique (z), alors il faut agir maintenant.

2. Les algorithmes post-quantiques

Le NIST a finalisé en août 2024 trois standards de cryptographie post-quantique, recommandés par l'ANSSI pour les systèmes d'information français :

Standard	Usage	Base mathématique	Remarque
ML-KEM-1024 (FIPS 203)	Encapsulation de clés (remplace DH/ECDH)	Réseaux euclidiens (Module-LWE)	Niveaux 512/768/1024. Performances compétitives.
ML-DSA-87 (FIPS 204)	Signatures numériques (remplace RSA/ECDSA)	Réseaux euclidiens (Module-LWE)	Tailles de signatures plus grandes, vitesse excellente.
SLH-DSA (FIPS 205)	Signatures de secours	Fonctions de hachage (arbres de Merkle)	Indépendant des réseaux. Assurance supplémentaire.
AES-256-GCM	Chiffrement symétrique	—	Inchangé, déjà résistant aux attaques quantiques.

Approche hybride : classique + post-quantique

L'approche hybride combine un algorithme classique (ECDH, ECDSA) avec un algorithme post-quantique (ML-KEM, ML-DSA) pendant la transition. Si l'un des deux algorithmes s'avère vulnérable, la sécurité reste assurée par l'autre. Cette stratégie est unanimement recommandée par l'ANSSI, le BSI et la NSA.

En pratique, le mode hybride concatène deux opérations indépendantes : pour l'échange de clés, on réalise simultanément un ECDH classique et un ML-KEM, puis on dérive la clé de session à partir des deux secrets partagés. Le surcoût en bande passante est modéré (environ 1 Ko par handshake TLS).

3. Évaluer votre maturité PQC

Utilisez cette grille d'auto-évaluation pour situer votre organisation et identifier les actions prioritaires :

Niveau	Description	Actions recommandées	Délai cible
0	**Non considéré** Aucune prise en compte du risque quantique. Pas de sensibilisation.	Sensibiliser la direction. Lancer un état des lieux cryptographique. Former les équipes sécurité.	Immédiat
1	**Sensibilisé** Risque identifié. Inventaire cryptographique en cours.	Compléter l'inventaire. Cartographier les flux chiffrés. Évaluer l'exposition HNDL.	3-6 mois
2	**Planifié** Stratégie de migration définie. POC planifié.	Qualifier les solutions hybrides. Exécuter le POC. Budgéter la migration.	6-12 mois
3	**En cours** Déploiement hybride sur les flux critiques.	Étendre la couverture. Automatiser les tests. Préparer la certification.	12-24 mois
4	**Accompli** Migration complète. Certification ANSSI obtenue.	Maintien en condition. Veille algorithmes. Préparer l'abandon du classique.	24-36 mois

> **Où en êtes-vous ?** La majorité des organisations françaises se situent entre les niveaux 0 et 1. L'objectif ANSSI est d'atteindre le niveau 3 avant 2030 pour les OIV et entités essentielles NIS2.

4. Les 5 étapes de la migration

1. Inventaire cryptographique

Identifier tous les flux chiffrés, protocoles, algorithmes et certificats de l'organisation. Cataloguer chaque actif avec son algorithme, sa taille de clé, sa durée de vie résiduelle et sa criticité métier. Couvrir également les partenaires et sous-traitants — les chaînes d'approvisionnement numériques héritent des vulnérabilités cryptographiques de chaque maillon.

2. Analyse de risque quantique

Classifier les données par durée de confidentialité requise vs horizon quantique. Appliquer la formule de Mosca pour prioriser. Les données dont la confidentialité doit être préservée au-delà de 2030 sont en risque immédiat si elles transitent aujourd'hui sur des canaux protégés uniquement par de la cryptographie classique. Présenter les résultats à la direction sous forme de matrice de risques.

3. Preuve de concept

Déployer un tunnel PQC hybride sur un flux non critique. Mesurer l'impact sur la latence, le débit et la consommation mémoire. Tester l'interopérabilité entre les différentes implémentations (liboqs, BoringSSL, wolfSSL, FPGA). Vérifier que les équipements intermédiaires (pare-feu, proxys, IDS) acceptent les paquets plus volumineux.

4. Déploiement progressif

Flux critiques d'abord (datacenters, sites de production, liaisons partenaires), puis extension. Mode hybride pendant la transition pour maintenir la connectivité avec les sites non encore migrés. Migrer la hiérarchie PKI de haut en bas : racine de confiance, autorités intermédiaires, puis certificats terminaux.

5. Certification et conformité

CSPN / EAL4+ pour les environnements OIV. Documenter la stratégie de migration PQC dans la PSSI. Maintenir un registre des actifs cryptographiques mis à jour trimestriellement. Assurer la traçabilité des décisions et actions de migration pour les audits de conformité NIS2 et DORA.

5. L'approche Cryptosphere

Cryptosphere conçoit et fabrique des chiffreurs réseau post-quantiques souverains, entièrement développés en France, pour les infrastructures critiques européennes.

Chiffreurs FPGA ligne-rate

Nos chiffreurs implémentent les algorithmes post-quantiques directement sur FPGA, offrant des performances déterministes de 1 Gbps à plusieurs Tbps. L'implémentation matérielle garantit une résistance aux attaques par canaux auxiliaires et une latence constante, indépendante de la charge. La reconfigurabilité du FPGA permet de mettre à jour les algorithmes sans remplacement matériel.

Déploiement transparent

Les chiffreurs s'intègrent de manière transparente dans l'infrastructure existante via IPsec. Aucune modification applicative n'est nécessaire. Le mode hybride (classique + PQC) est activé par défaut pendant la période de transition.

Trois modes d'exploitation

- **Souveraineté totale :** clés générées et stockées sur site, aucune dépendance extérieure.
- **Autonome :** gestion déléguée via la plateforme GARANCE (PKI + orchestration + supervision).
- **Managé :** service clé en main, opéré par Cryptosphere depuis la France.

GARANCE : PKI + orchestration + supervision

La plateforme GARANCE centralise la gestion des clés, l'orchestration des chiffreurs et la supervision en temps réel. Tableau de bord unifié, alertes automatisées, rotation des clés planifiable, journalisation complète pour la conformité.

Certification et souveraineté

Certification ANSSI CSPN visée, trajectoire EAL4+. Code source 100% Rust, licence EUPL-1.2. Conception, développement et fabrication entièrement en France.

6. Spectre de déploiement

La gamme Cryptosphere couvre l'ensemble des besoins de chiffrement post-quantique, du site distant au backbone opérateur :

Segment	Modèle	Débit	Cas d'usage
Edge	PQC-WAN Agent	1 — 100 Gbps	Sites distants, agences, liaisons partenaires
Datacenter	PQC-800 / 1600 / 2400	800 Gbps — 2,4 Tbps	Cœur de réseau, interconnexions DC
Backbone	PQC-3200 / 6400	3,2 Tbps — multi-Tbps	Backbone opérateur, hyperscaler
Standalone	PQC-800S / 1600S	800 Gbps — 1,6 Tbps	Sites isolés, environnements air-gap
Cloud	PQC SecNumCloud	Selon besoin	Service managé, cloud souverain

Tous les modèles supportent le mode hybride (classique + post-quantique), le chiffrement IPsec ligne-rate et la gestion centralisée via GARANCE. La crypto-agilité intégrée permet de mettre à jour les algorithmes par reconfiguration du FPGA, sans intervention matérielle.

7. Conformité réglementaire

Le cadre réglementaire européen impose des exigences croissantes en matière de résilience cryptographique. Le tableau ci-dessous résume les principales obligations et la couverture Cryptosphere :

Réglementation	Exigence	Couverture Cryptosphere
LPM / OIV	Sécurisation des SI d'importance vitale. Chiffrement des flux sensibles.	Chiffreurs certifiables CSPN/EAL4+. Souveraineté totale des clés.
NIS2	Évaluation des risques technologies émergentes. Résilience des entités essentielles.	Chiffrement hybride PQC. Registre crypto automatisé.
DORA	Résilience opérationnelle numérique du secteur financier. Tests de résilience crypto.	Tests automatisés. Rotation de clés planifiable. Journalisation complète.
II 901	Protection des SI traitant d'informations classifiées.	Chiffrement ligne-rate. Gestion souveraine des clés.
SecNumCloud	Qualification des services cloud souverains.	Modèle PQC SecNumCloud. Hébergement France.
ANSSI PQC 2030	Migration PQC complète avant 2030 pour les systèmes classifiés.	Accompagnement de bout en bout. Crypto-agilité native.

8. Calendrier de migration recommandé

2025-2026 **Phase 1 — Préparation**

Inventaire cryptographique. Sensibilisation de la direction. Formation des équipes. Évaluation des risques quantiques. Sélection des solutions. Budget.

2026-2027 **Phase 2 — POC et qualification**

Preuve de concept sur flux non critique. Tests d'interopérabilité. Qualification des solutions matérielles et logicielles. Validation de l'architecture cible.

2027-2028 **Phase 3 — Déploiement hybride**

Déploiement du mode hybride sur les flux critiques. Migration PKI. Extension progressive. Certification CSPN.

2028-2030 **Phase 4 — Migration complète**

Extension à tous les périmètres. Abandon progressif des algorithmes classiques seuls. Conformité ANSSI PQC 2030. Maintien en condition opérationnelle.

> **Recommandation :** Commencez dès maintenant par l'inventaire cryptographique (Phase 1). C'est une action à faible risque, à fort impact, qui conditionne toute la suite de la migration.

9. Prochaines étapes

Vous souhaitez évaluer votre maturité PQC et planifier votre migration ? Voici comment avancer :

Demander un audit de maturité PQC

Notre équipe réalise un diagnostic gratuit de votre infrastructure cryptographique. En une demi-journée, nous identifions vos flux à risque, évaluons votre niveau de maturité et proposons une feuille de route de migration adaptée à votre contexte.

Planifier une preuve de concept

Déployez un chiffreur PQC sur un flux de test pour mesurer les performances et valider l'intégration avec votre infrastructure existante. La POC est réalisable en deux semaines.

Nous contacter

- Formulaire sécurisé : **cryptops.fr/contact**
- Email : **contact@cryptops.fr**

> Notre formulaire de contact est chiffré de bout en bout (RSA-4096 + AES-256-GCM). Votre message est chiffré dans votre navigateur avant tout envoi. Aucun intermédiaire n'a accès au contenu.

10. À propos de Cryptosphere

Cryptosphere est un fabricant français de chiffreurs réseau post-quantiques pour les infrastructures critiques européennes. Fondée avec la conviction que la souveraineté cryptographique est un enjeu stratégique, l'entreprise conçoit, développe et fabrique l'ensemble de ses solutions en France.

Nos chiffreurs FPGA implémentent les algorithmes post-quantiques standardisés par le NIST (ML-KEM, ML-DSA) avec des performances ligne-rate, de 1 Gbps à plusieurs Tbps. La crypto-agilité native permet de mettre à jour les algorithmes par reconfiguration, sans intervention matérielle.

Siège social	19 rue du Colisée, 75008 Paris
Laboratoire R&D	Rouen, France
Site web	cryptops.fr
Contact	contact@cryptops.fr