Plan d'Action Post-Quantum Cryptography : Guide RSSI 2026

> Plan d'action post-quantum cryptography en 5 phases pour migrer votre SI vers le PQC. Inventaire, priorisation, pilotes et déploiement pour RSSI et DSI…

Ce guide propose un plan d'action en 5 phases pour migrer votre système d'information vers la cryptographie post-quantique (PQC). Avec les standards NIST finalisés (FIPS 203/204/205) et les attaques HNDL déjà actives, la migration doit commencer maintenant. Le budget type varie de 200 000 à 680 000 € sur 3 ans pour une ETI, avec un horizon réglementaire de 2030 pour les systèmes critiques selon les directives ANSSI et ENISA.

La cryptographie post-quantique n'est plus une question théorique : avec la standardisation NIST finalisée en 2024 (FIPS 203, 204, 205) et les directives ANSSI, les RSSI doivent engager dès maintenant leur plan de migration. L'urgence est double — la menace des ordinateurs quantiques sur les algorithmes actuels (RSA, ECC) et les attaques *Harvest Now Decrypt Later* déjà actives. Ce guide propose un plan d'action structuré en 5 phases pour migrer vers la cryptographie post-quantique sans rupture d'activité, avec des jalons concrets, des priorités de traitement et un cadre budgétaire adapté aux ETI et grandes entreprises.

À RETENIR

À retenir

Les 3 standards NIST PQC sont finalisés (FIPS 203/204/205) — la migration peut et doit commencer

Les attaques HNDL sont actives dès maintenant — toute donnée sensible à longue durée de vie est à risque

L'approche hybride (classique + PQC) est recommandée par l'ANSSI pendant la transition

Commencez par l'inventaire cryptographique (CBOM) avant tout déploiement

Budget type : 200 000 à 680 000 € sur 3 ans pour une ETI

PROTECTION DES DONNÉES

Plan d'Action Post-Quantum Cryptography : Guide RSSI 2026

Pourquoi agir maintenant : l'urgence de la migration PQC

L'informatique quantique progresse à un rythme accéléré. En 2023, IBM a déployé un processeur à 1000+ qubits (Condor). En 2024, Google a démontré la correction d'erreurs quantiques à grande échelle avec Willow. Les experts estiment que la menace cryptographique à grande échelle pourrait se matérialiser entre 2030 et 2035.

Mais l'ennemi immédiat n'est pas un ordinateur quantique opérationnel — c'est l'attaque **Harvest Now Decrypt Later (HNDL)**. Des acteurs malveillants (étatiques notamment) collectent dès aujourd'hui des flux chiffrés pour les déchiffrer quand les ordinateurs quantiques seront suffisamment puissants. Toute donnée chiffrée avec des algorithmes actuels et dont la confidentialité doit être maintenue au-delà de 5-10 ans est déjà compromise.

Les signaux réglementaires sont clairs :

NSA (USA) : migration obligatoire vers PQC pour les systèmes classifiés avant 2030

ANSSI : publication du guide de migration post-quantique avec recommandations prioritaires

ENISA : rapport 2024 sur la préparation européenne à la menace quantique

BSI (Allemagne) : directive de migration pour les infrastructures critiques avant 2030

Les standards NIST PQC finalisés en 2024

Le NIST a officiellement standardisé 3 algorithmes en août 2024 :

Phase	Durée	Objectifs clés	Livrable
Phase 1 — Inventaire	Mois 1-3	CBOM complet, cartographie risques HNDL	Registre des actifs crypto
Phase 2 — Priorisation	Mois 3-6	Classification par durée de sensibilité, budget PQC	Roadmap priorisée
Phase 3 — Pilote	Mois 6-12	Hybridation TLS, tests ML-KEM sur systèmes non critiques	Rapport de pilote
Phase 4 — Migration progressive	Mois 12-30	Déploiement PKI hybride, migration systèmes critiques	Systèmes critiques migrés
Phase 5 — Consolidation	Mois 30-36	Suppression algorithmes obsolètes, conformité réglementaire	Audit final, certification

⚡ Retour terrain

Lors d'un accompagnement RGPD pour une PME de 120 personnes dans le secteur des ressources humaines, j'ai découvert que leurs bases de données de candidatures contenaient des données datant de 2011 — bien au-delà des durées de conservation légales. La purge des données expirées a représenté 78 % du volume initial. La mise en place d'une politique de rétention automatisée (archivage à 2 ans, suppression à 3 ans pour les candidats non retenus) a finalement été le changement le plus impactant de la mission.

FIPS 203 — ML-KEM (anciennement CRYSTALS-Kyber) : mécanisme d'encapsulation de clés, remplace ECDH pour l'échange de clés et le chiffrement hybride

FIPS 204 — ML-DSA (anciennement CRYSTALS-Dilithium) : signature numérique basée sur les réseaux euclidiens, remplace ECDSA et RSA-PSS

FIPS 205 — SLH-DSA (anciennement SPHINCS+) : signature basée sur les fonctions de hachage, alternative conservatrice à ML-DSA

Un 4e standard est en cours de finalisation : FALCON (FN-DSA), également basé sur les réseaux euclidiens, adapté aux environnements contraints.

L'ANSSI recommande d'adopter une approche **hybride** pendant la transition : combiner un algorithme classique (ECDH P-256) avec un algorithme PQC (ML-KEM) pour garantir la sécurité même si l'un des deux est compromis.

Phase 1 : Inventaire cryptographique (mois 1-3)

La migration PQC commence par un inventaire exhaustif de tous les usages cryptographiques dans l'organisation. Sans cet inventaire, la migration est impossible à planifier.

Périmètre de l'inventaire

Algorithmes d'échange de clés : RSA, ECDH, DH

Algorithmes de signature : RSA-PSS, ECDSA, DSA

Protocoles utilisant ces algorithmes : TLS 1.3, SSH, IPSec, S/MIME, PGP, JWT

Certificats X.509 : PKI interne et externe, autorités de certification

Données chiffrées au repos : bases de données, archives, HSM

Bibliothèques cryptographiques utilisées : OpenSSL, BouncyCastle, NSS, SunJCE

Matériels cryptographiques : HSM, TPM, cartes à puce, tokens FIDO2

Outils pour l'inventaire

CBOM (Cryptography Bill of Materials) : inventaire structuré des dépendances cryptographiques, au format CycloneDX

Cryptosense Analyzer : analyse dynamique des usages cryptographiques en Java/.NET

IBM Guardium Data Encryption : inventaire des données chiffrées

Scans TLS : SSLyze, testssl.sh pour auditer les endpoints

Analyse statique du code : SonarQube, Semgrep avec règles crypto

Durée estimée : 4 à 12 semaines selon la taille de l'organisation et la complexité du SI.

Phase 2 : Analyse de risques et priorisation (mois 3-5)

Tous les systèmes ne présentent pas le même niveau de risque face à la menace quantique. La priorisation doit se baser sur deux axes : la sensibilité des données et la durée de vie requise de leur confidentialité.

Matrice de priorisation RSSI

Priorité critique (migrer avant 2027) : données dont la confidentialité doit être maintenue > 10 ans — dossiers médicaux, secrets d'État, propriété intellectuelle stratégique, flux financiers souverains

Priorité haute (migrer avant 2028) : communications chiffrées longue durée, VPN inter-sites, certificats racine PKI

Priorité moyenne (migrer avant 2030) : TLS pour sites web, API internes, authentification FIDO2

Priorité basse : données éphémères, sessions courtes sans valeur long terme

Critères de criticité supplémentaires

Secteur réglementé (défense, santé, finance) : contraintes de migration plus strictes

Interconnexions partenaires et supply chain : nécessite coordination

Systèmes legacy : délais de migration potentiellement longs

Hardware cryptographique (HSM) : cycle de renouvellement matériel à anticiper

Phase 3 : Architecture hybride et pilotes (mois 5-10)

Avant de migrer l'ensemble du SI, il est essentiel de valider l'approche technique sur des systèmes pilotes représentatifs.

Approche hybride recommandée par l'ANSSI

L'hybridation consiste à utiliser simultanément un algorithme classique et un algorithme PQC. En TLS 1.3, cela se traduit par :

X25519MLKEM768 : combinaison ECDH X25519 + ML-KEM-768 pour l'échange de clés

Signature hybride : ECDSA P-256 + ML-DSA-44

Cette approche garantit que même si l'algorithme PQC est compromis (improbable mais possible dans un standard émergent), la sécurité classique reste intacte — et vice versa face aux ordinateurs quantiques.

Pilotes recommandés

VPN site-à-site inter-datacenters : protocole IKEv2/IPSec hybride

API internes critiques : TLS 1.3 avec suites hybrides

PKI interne : migration des certificats intermédiaires vers ML-DSA

Authentification forte : test des tokens FIDO2 avec PQC (standard en développement)

Phase 4 : Déploiement progressif (mois 10-24)

La migration en production doit être progressive, par vagues de systèmes classés par priorité.

Checklist de déploiement par système

Mise à jour des bibliothèques cryptographiques (OpenSSL 3.3+ avec OQS provider)

Renouvellement des certificats X.509 (durée de validité ≤ 2 ans recommandé)

Mise à jour de la configuration TLS : suites hybrides en priorité, suites classiques en fallback

Test d'interopérabilité avec les partenaires et fournisseurs

Mise à jour des politiques de sécurité et de la documentation

Formation des équipes (développeurs, ops, helpdesk)

Risques de déploiement

Les algorithmes PQC sont plus gourmands en ressources que leurs équivalents classiques :

ML-KEM-768 : clé publique de 1184 octets vs 64 octets pour ECDH P-256

ML-DSA-44 : signature de 2420 octets vs 64 octets pour ECDSA P-256

Impact sur les performances TLS : +1 à 3 ms de latence en pointe selon les benchmarks

Systèmes embarqués et IoT : contraintes mémoire importantes, utiliser ML-KEM-512 ou Kyber-512

Phase 5 : Gouvernance et suivi long terme (mois 18-36)

La migration PQC n'est pas un projet ponctuel — c'est un programme de transformation cryptographique qui s'inscrit dans la durée.

Gouvernance PQC recommandée

Création d'un **CBOM maintenu** : registre vivant de tous les usages cryptographiques, mis à jour à chaque déploiement

Processus de **crypto-agility** : capacité à changer d'algorithme en production en moins de 30 jours si un algorithme est compromis

Veille réglementaire : suivi des évolutions ANSSI, NIST, ENISA

Tests de régression crypto : intégrer la vérification des algorithmes dans les pipelines CI/CD

Budget type pour une ETI (500-2000 employés)

Phase 1 (inventaire) : 30 000-80 000 € (prestataire + outils)

Phase 2-3 (analyse + pilotes) : 50 000-150 000 €

Phase 4 (déploiement) : 100 000-400 000 € selon la complexité du SI

Phase 5 (gouvernance, formation) : 20 000-50 000 €/an

Budget total estimé : 200 000 à 680 000 € sur 3 ans

Cas d'usage sectoriels

Secteur financier

Les établissements bancaires sont en première ligne : les transactions interbancaires (SWIFT, TARGET2), les données KYC et les archives de conformité bénéficient d'une durée de conservation légale de 5 à 10 ans, les exposant directement aux attaques HNDL. La directive DORA (en vigueur depuis janvier 2025) impose une gestion des risques ICT incluant la cryptographie. Les banques systémiques doivent anticiper les exigences BCE/EBA qui s'aligneront sur les recommandations PQC d'ici 2026-2027.

Secteur santé

Les dossiers médicaux (DMP) ont une durée de conservation de 20 ans minimum. L'exposition HNDL est maximale. La certification HDS impose des niveaux de chiffrement élevés que la migration PQC doit maintenir. Les équipements médicaux connectés posent un défi particulier : cycles de vie longs (10-15 ans), contraintes embarquées, certification réglementaire à renouveler.

Défense et secteur public

Les informations classifiées SECRET sont déjà soumises aux directives ANSSI d'utilisation d'algorithmes approuvés. La migration vers le PQC est une priorité gouvernementale avec des échéances strictes. Pour les OIV (Opérateurs d'Importance Vitale), les systèmes ICS/SCADA posent un challenge supplémentaire en raison de leurs contraintes temps-réel.

FAQ : Plan d'action post-quantum cryptography

Quand dois-je commencer la migration vers le PQC ?

Dès maintenant pour l'inventaire et l'analyse de risques. Le déploiement sur les systèmes critiques doit commencer en 2025-2026 au plus tard. Les données sensibles chiffrées aujourd'hui sont vulnérables aux attaques HNDL si leur confidentialité doit être maintenue au-delà de 2030.

Les algorithmes NIST PQC sont-ils suffisamment matures pour la production ?

Les 3 standards finalisés (FIPS 203, 204, 205) ont subi des années de cryptanalyse publique intense. ML-KEM et ML-DSA sont considérés comme prêts pour la production avec une approche hybride. Les implémentations dans les grandes bibliothèques (OpenSSL, BoringSSL, NSS) sont disponibles.

Faut-il migrer tous les systèmes en même temps ?

Non — une approche progressive et priorisée est recommandée. Commencez par les systèmes traitant des données à longue durée de vie, puis progressez vers les systèmes moins critiques. L'hybridation permet de maintenir la compatibilité avec les partenaires non encore migrés.

Quel impact sur les performances des applications ?

L'impact est mesurable mais généralement acceptable : +1 à 3 ms de latence TLS en pointe, augmentation de la taille des certificats (×10 à ×50 selon l'algorithme). Les systèmes à haute fréquence de transactions nécessitent des tests de charge spécifiques avant déploiement.

Lire aussi : cryptographic agility pour l'ère post-quantique, comprendre la menace Harvest Now Decrypt Later, implémenter CRYSTALS-Kyber et Dilithium et architecture Zero Trust + Post-Quantum.

Sources : NIST Post-Quantum Cryptography Project | ANSSI Migration Post-Quantique

Gestion de la transition pour les applications métier

La migration PQC ne concerne pas uniquement l'infrastructure — elle touche aussi profondément les applications métier qui embarquent de la cryptographie. Trois catégories d'applications nécessitent une attention particulière.

Applications de signature électronique

Les solutions de signature électronique (DocuSign, Yousign, Adobe Sign) reposent sur des certificats X.509 émis par des autorités de certification. La migration implique :

Anticipation du renouvellement des certificats qualifiés avant leur expiration naturelle

Coordination avec les prestataires de services de confiance (PSCo) accrédités eIDAS

Test de compatibilité des signatures PQC avec les lecteurs de documents côté destinataires

Mise à jour des politiques de signature avec les nouvelles empreintes algorithmiques

Note importante : les signatures existantes réalisées avec des algorithmes classiques restent valides et n'ont pas besoin d'être recréées. Seules les nouvelles signatures doivent utiliser les algorithmes PQC.

Applications de messagerie chiffrée (S/MIME, PGP)

Les communications chiffrées par email posent un problème spécifique : un email chiffré en 2024 doit rester déchiffrable en 2035. Les entreprises utilisant S/MIME pour les communications sensibles (contrats, RH, financier) doivent :

Identifier tous les emails archivés chiffrés avec des algorithmes classiques

Évaluer la durée de conservation réglementaire des archives (5 ans pour la comptabilité, 30 ans pour certains contrats)

Déchiffrer et rechiffrer les archives critiques avec des algorithmes PQC avant la menace quantique

Mettre en place une politique de durée de vie des clés adaptée (rotation annuelle recommandée)

Applications de gestion des identités (IAM, PAM)

Les systèmes d'authentification forte sont également concernés :

FIDO2/WebAuthn : le standard est en cours d'évolution pour intégrer le PQC (FIDO Alliance PQC WG)

Certificats clients pour les accès VPN et PKI interne : à renouveler avec ML-DSA dès que les équipements le supportent

JWT (JSON Web Tokens) : les tokens signés avec RS256 ou ES256 doivent migrer vers ML-DSA

SAML et OAuth2 : vérifier le support PQC des IdP (Okta, Azure AD, Keycloak)

Coordination avec les fournisseurs et partenaires

La migration PQC ne peut pas se faire en silo. L'interopérabilité avec les partenaires est un enjeu majeur : si votre organisation migre mais que vos partenaires ne supportent pas encore les algorithmes PQC, des mécanismes de fallback classique seront nécessaires.

Approche de la migration coordonnée

Inventaire des interconnexions : cartographier toutes les connexions chiffrées avec des partenaires externes (APIs, VPN, EDI, messagerie)

Communication proactive : informer les partenaires clés de votre calendrier de migration et demander le leur

Clauses contractuelles : inclure des exigences PQC dans les renouvellements de contrats fournisseurs 2025-2026

Fallback hybride : maintenir un mode de compatibilité avec les algorithmes classiques le temps que tous les partenaires migrent

Les grandes plateformes cloud et les éditeurs de solutions de sécurité ont déjà intégré le PQC dans leurs roadmaps :

AWS : support ML-KEM disponible dans AWS Certificate Manager et CloudFront depuis 2024

Azure : Azure Key Vault avec support PQC en preview, Azure VPN Gateway sur la roadmap

Google Cloud : Chrome et Cloud Load Balancing supportent ML-KEM depuis 2024

Cloudflare : support ML-KEM en production pour tous les serveurs Cloudflare depuis 2023

Métriques et indicateurs de suivi de la migration PQC

Pour piloter efficacement la migration, il est essentiel de définir des indicateurs de performance (KPIs) mesurables.

KPIs de couverture

Taux de couverture du CBOM : % des systèmes ayant un inventaire crypto complet (cible : 100% des systèmes critiques en 6 mois)

Taux de systèmes migrés : % des endpoints TLS utilisant des suites hybrides PQC (cible : 50% en 2026, 100% en 2028)

Taux de certificats PQC : % des certificats X.509 émis avec ML-DSA (cible : 80% en 2027)

Couverture des partenaires évalués : % des partenaires critiques dont la roadmap PQC est connue

KPIs de qualité

Incidents liés à la migration : nombre d'incidents de production causés par les changements cryptographiques (objectif zéro)

Temps moyen de renouvellement de certificat : doit rester inférieur à 24h (automatisation requise)

Score de maturité PQC : score sur la checklist quantum readiness, suivi trimestriellement

Un tableau de bord RSSI dédié à la migration PQC, présenté trimestriellement au COMEX, permet de maintenir la visibilité et le soutien de la direction générale sur la durée du programme.

Les pièges à éviter dans la migration PQC

Erreur 1 : Attendre que tous les systèmes soient prêts

Certains équipements (IoT industriels, mainframes anciens) ne supporteront jamais le PQC nativement. Attendre la migration de 100% des systèmes bloque l'ensemble du projet. La stratégie correcte est d'isoler les systèmes non-migrables derrière des proxies cryptographiques et de progresser sur les systèmes migrables.

Erreur 2 : Ignorer la supply chain logicielle

De nombreuses bibliothèques cryptographiques utilisées dans les applications métier sont embarquées via des dépendances transitives. Une analyse SBOM (Software Bill of Materials) est nécessaire pour identifier tous les usages crypto, y compris ceux cachés dans les dépendances tierces.

Erreur 3 : Négliger la formation des développeurs

La crypto-agility — la capacité à changer d'algorithme facilement — ne peut être implémentée que si les développeurs intègrent les bons patterns dès la conception. Un développeur qui hardcode un algorithme RSA dans son code plutôt que d'utiliser une abstraction crypto-agile crée une dette technique PQC immédiate.

Erreur 4 : Sous-estimer l'impact sur les performances

Les tests de performance doivent être conduits avant tout déploiement en production. Sur les systèmes à haute fréquence de transactions (trading, paiements), l'impact de +2 à 5 ms par handshake TLS peut être significatif. Des optimisations matérielles (accélération hardware PQC) ou architecturales (session resumption TLS) peuvent être nécessaires.

Retours d'expérience : premières migrations PQC en production (2024-2025)

Les premières migrations PQC en production livrent des enseignements précieux pour les organisations qui s'apprêtent à se lancer.

Cloudflare : migration globale de l'infrastructure TLS

Cloudflare a activé le support ML-KEM pour l'ensemble de son réseau CDN en 2023-2024, couvrant des millions de sites web. Résultat : 20% des connexions TLS depuis Chrome utilisent désormais une suite hybride PQC. L'impact sur les performances est inférieur à 1 ms dans 95% des cas grâce à l'optimisation matérielle. Leçon principale : commencer par les endpoints TLS côté serveur est la migration la moins risquée et la plus rapide à déployer.

Secteur bancaire américain : migration PKI interne

Plusieurs grandes banques américaines ont démarré la migration de leur PKI interne vers ML-DSA en 2024, à la demande du régulateur fédéral. Le principal défi identifié : l'augmentation de la taille des certificats ML-DSA (×10 vs ECDSA) a nécessité des ajustements dans les applications qui validaient la taille maximale des certificats. Leçon : tester exhaustivement tous les parseurs de certificats dans les applications métier avant déploiement.

Administration française : approche pilote ANSSI

L'ANSSI a lancé en 2024 un programme pilote avec plusieurs administrations pour tester la migration vers les protocoles PQC hybrides sur les VPN inter-ministériels. Les enseignements sont en cours de publication sous forme de guides pratiques disponibles sur le site de l'ANSSI. Les administrations participantes rapportent que la phase d'inventaire a nécessité 2 à 3 fois plus de temps qu'estimé initialement, en raison de la découverte de nombreux usages crypto non documentés.

Ces retours d'expérience convergent vers une recommandation commune : **sous-estimer l'inventaire et surestimer la vitesse de déploiement** sont les deux erreurs les plus fréquentes. Planifiez large sur la phase 1, puis accélérez sur les phases suivantes une fois que vous disposez d'une cartographie fiable.

La migration vers la cryptographie post-quantique est un marathon, pas un sprint. Les organisations qui commencent maintenant bénéficient d'un avantage compétitif : elles se donnent le temps de le faire correctement, avec des pilotes, des tests d'interopérabilité et une formation adéquate des équipes. Celles qui attendent risquent de devoir migrer en urgence, sous pression réglementaire, avec les coûts et les risques opérationnels que cela implique. Le moment optimal pour commencer était hier ; le deuxième meilleur moment est aujourd'hui.

Pour en savoir plus sur les standards et les outils disponibles, consultez les ressources de l'ANSSI (ssi.gouv.fr), le portail NIST PQC (csrc.nist.gov/projects/post-quantum-cryptography) et l'initiative Open Quantum Safe (openquantumsafe.org) qui fournit des implémentations open-source de référence pour les algorithmes NIST PQC, notamment la bibliothèque liboqs utilisée par OpenSSL et les principaux fournisseurs de solutions de sécurité.

