AYI NEDJIMI Consultants

Cryptographie Post-Quantique : Guide Migra

29 April 2026 • Mis à jour le 29 April 2026 • 48 min de lecture

Guide complet cryptographie post-quantique : ML-KEM (Kyber), ML-DSA (agility, certificats hybrides, inventaire CBOM, risque Q-Day.

La cryptographie post-quantique represente le defi securitaire le plus critique de l infrastructures numeriques mondiales. Avec l'emergence des ordinateurs quantiqu temps polynomial, les fondations memes de la securite informatique moderne — F menacees d'obsolescence. Le National Institute of Standards and Technology (NIS post-quantiques, inaugurant une ere de transition qui concernera chaque organisa manipulant des primitives cryptographiques. Ce guide exhaustif parcourt l'ensemb ML-KEM, ML-DSA, SLH-DSA et FN-DSA aux strategies de migration, en passant p l'inventaire cryptographique (CBOM), l'impact sur TLS, PKI, VPN et SSH, et le risqu securite, les RSSI et les ingenieurs DevSecOps, comprendre ces enjeux n'est plus immediate. La migration post-quantique ne s'improvise pas : elle se planifie, se tes annees, et le compte a rebours a deja commence.

À RETENIR

A retenir : Le NIST a publie les standards FIPS 203, 204 et 205 en aout 2024. inventaire cryptographique des maintenant. Le risque "Harvest Now, Decrypt pas future.

Pourquoi la cryptographie classique est-elle menacee par l'informatique quanti

Pour comprendre la menace quantique, il faut remonter aux fondements mathema actuelle. RSA repose sur la difficulte de factoriser de grands nombres semi-premi courbes elliptiques (ECDH, ECDSA) reposent sur le probleme du logarithme discre computationnellement difficiles pour les ordinateurs classiques : factoriser un nom avec les meilleurs algorithmes classiques connus.

En 1994, Peter Shor a publie un algorithme quantique capable de factoriser des er temps polynomial. Concretement, un ordinateur quantique suffisamment puissant RSA-2048 en quelques heures. L'algorithme de Grover, publie en 1996, offre une a un espace non structure, ce qui reduit effectivement la securite des algorithmes s une securite equivalente a 128 bits, ce qui reste acceptable, mais AES-128 tomber

La distinction entre ces deux menaces est fondamentale pour la strategie de migra ChaCha20) et les fonctions de hachage (SHA-256, SHA-3) survivent a l'ere quanti cles. La cryptographie asymetrique, en revanche, doit etre entierement remplacee problemes mathematiques differents, resistants aux attaques quantiques connues

L'etat actuel des ordinateurs quantiques

En 2025, les ordinateurs quantiques les plus avances disposent de quelques millie encore significatifs. IBM a deploye des processeurs depassant les 1 000 qubits, G