EVIDEN

Post-quantum Cryptography - FAQ

Post-quantum Cryptography - FAQ

Questions	Réponses	Date màj
General Context		
Quel est l'impact potentiel des ordinateurs quantiques sur la cybersécurité actuelle ?	Notre expertise principale porte sur la cryptographie, qui est un sous-ensemble de la cybersécurité. D'un point de vue cryptographique, les menaces diffèrent selon le type de cryptographie utilisé : • Symétrique (par exemple AES) : L'algorithme de Grover réduira la sécurité par un facteur de deux. Nous devrons utiliser des clés deux fois plus grandes pour obtenir le même niveau de sécurité qu'aujourd'hui. • Asymétrique (RSA/ECC/DH) : L'algorithme de Shor permet de résoudre "rapidement" les problèmes mathématiques sur lesquels repose la sécurité de la cryptographie asymétrique déployée (RSA, ECDSA, Diffie-Hellmann, etc.). Afin d'atténuer cette menace, il existe d'autres cryptosystèmes asymétriques qui ne sont pas menacés par l'ordinateur quantique : la cryptographie post-quantique (PQC).	22 juil. 2025
Comment notre infrastructure de confiance IDnomic PKI est-elle affectée par l'avènement des algorithmes post-quantiques ?	Les infrastructures PKI utilisent des signatures numériques pour certifier les clés publiques dans un large éventail d'applications. Les signatures et les clés publiques utilisées dans les ICP actuelles font partie de la cryptographie asymétrique menacée par l'ordinateur quantique. Les ICP devront donc utiliser des algorithmes résistants au quantum (cryptographie post-quantique).	22 juil. 2025

Quelles sont les recommandations de l'ANSSI en matière de PQC ?	L'ANSSI a publié différents articles sur la cryptographie post-quantique (PQC). L'ANSSI a partagé des recommandations, notamment • Une liste d'algorithmes cryptographiques asymétriques sécurisés contre l'ordinateur quantique (pour le KEM et la signature). • La transition vers les algorithmes asymétriques post-quantiques doit être une approche hybride : utilisation de la cryptographie traditionnelle avec la cryptographie post-quantique (pas pour les USA, le mode hybride n'est pas obligatoire). Nous devons anticiper et nous préparer dès maintenant ANSSI views on the Post-Quantum Cryptography transition Follow-position-paper-post-quantum-cryptography and PQC transition in France ANSSI views	22 juil. 2025
Quelles mesures pouvons-nous prendre dès maintenant pour préparer la transition vers la PQC ?	Nous recommandons de lire notre PQC Migration Guide. En bref, nous pouvons vous recommander, dans un premier temps, de dresser un inventaire des cryptomonnaies afin d'identifier les risques et les défis associés à l'ère post-quantique.	22 juil. 2025
Quel est le calendrier estimé pour l'adoption généralisée de la cryptographie post-quantique ?	Les premiers algorithmes ont été normalisés et la transition est en cours. Pour l'administration américaine, la transition doit se faire avant 2035. En Europe, un premier document appelé Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography a été publié en juin 2025 par le groupe de travail du CG NIS sur le sujet PQC et destiné aux États membres.	22 mai 2025

Comment Eviden Digital ID assurera-t-il une transition en douceur vers PQC ?	Les équipes de R&D sont déjà à l'œuvre : • à des intégrations dans des produits à des fins de test • au développement de PoC prenant en compte différents cas d'utilisation, • en suivant les normalisations et les recommandations de l'ANSSI, BSI, NIST, ENISA et apporter un soutien aux clients existants • en discussion avec les fournisseurs de HSM	22 juil. 2025
Quelles sont les meilleures pratiques en matière de cybersécurité pendant cette période de transition ?	Suivre les recommandations des agences gouvernementales et s'appuyer sur les organismes internationaux de normalisation (comme le NIST, l'IETF et l'ETSI).	22 juil. 2025
PQC et Produits Digital ID		

Les algorithmes postquantiques ML-DSA, SLH-DSA, ML-KEM, ainsi que les normes de signature basées sur le hachage (XMSS, LMS) DOIVENT être pris en charge.	L'intégration de PQC fait partie de notre feuille de route. Comme nous intégrons la bibliothèque Bouncy Castle, le produit IDnomic PKI bénéficie des algorithmes intégrés fournis par cette bibliothèque, et les algorithmes PQC en font partie. Pour l'instant, nous nous concentrons sur les algorithmes ML-DSA (anciennement appelé Dilithium) et ML-KEM (anciennement appelé Kyber). D'autres algorithmes pourront être intégrés ultérieurement après étude et validation. Ces algorithmes sont déjà normalisés depuis août 2024 : • FIPS 203 (ML-KEM), Module-Lattice-Based Key-Encapsulation Mechanism Standard • FIPS 204 (ML-DSA), Module-Lattice-Based Digital Signature Standard Les normes de signature XMSS et LMS basées sur le hachage ont été normalisées en 2019 : • FIPS 205 (SLH-DSA), Stateless Hash-Based Digital Signature Standard Le HQC a été sélectionné pour la normalisation le 11 mars 2025 et n'est pas encore publié (norme attendue en 2027).	22 juil. 2025
Quels algorithmes de cryptographie post quantique sont pris en charge par IDnomic PKI en plus de ceux énumérés ?	Aujourd'hui, IDnomic PKI prend en charge ML-DSA à des fins de test uniquement. D'autres algorithmes seront pris en charge ultérieurement.	22 juil. 2025

Les certificats PQC DOIVENT être rétro compatibles.	Notre objectif est de nous concentrer sur des solutions hybrides contenant à la fois des algorithmes traditionnels et des algorithmes PQC. Toutes les approches pour les certificats hybrides PQC ne garantissent pas la compatibilité ascendante avec les systèmes existants. Les plus expérimentées exigent aujourd'hui que les systèmes existants soient d'abord mis à niveau pour prendre en charge ces certificats hybrides. Les certificats PQC complets (contenant uniquement des algorithmes PQC) ne seront pas rétrocompatibles avec les certificats existants. En outre, les premiers certificats PQC émis (hybrides ou non) ne peuvent être utilisés que pour les PoC et devront être remplacés une fois que les normes (si ce n'est pas encore le cas) seront publiées et considérées comme suffisamment sûres.	22 juil. 2025

Votre solution PKI est-elle capable de générer des certificats quantiques sûrs pour des tests en avant phase ?	Notre solution IDnomic PKI est capable de générer des certificats PQC uniquement à des fins de test. Avec les nouvelles fonctionnalités, il est possible de : 1. Générer des certificats PQC uniquement pour les tests, y compris la hiérarchie de l'autorité de certification. 2. Effectuer un test d'intégration : utiliser ces certificats de test dans un environnement de test. Il peut s'agir de configurer des serveurs, des applications et des dispositifs de réseau pour qu'ils utilisent les nouveaux certificats, s'ils sont en mesure de prendre en charge le format de certificat PQC. 3. Effectuer des tests de performance : évaluer l'impact de PQC sur la performance de vos systèmes. Les algorithmes de CQP auront des exigences de calcul différentes de celles des algorithmes traditionnels. La plupart des algorithmes PQC utilisent des clés et des certificats de plus grande taille que les algorithmes traditionnels. La prochaine étape de la feuille de route est la prise en charge des certificats hybrides, en se concentrant d'abord sur le format du catalyseur.	22 juil. 2025
La PKI d'Eviden Digital ID est-elle compatible avec toutes les unités HSM du marché en ce qui concerne PQC ?	Aujourd'hui, IDnomic PKI est compatible avec Trustway HSM Proteccio. Nous sommes en discussion avec d'autres fournisseurs (Thales, Entrust, Utimaco, etc) au sujet de l'intégration de PQC.	22 juil. 2025
Est-ce que OT-PKI pourrait-elle supporter la PQC ?	Non, OT-PKI ne supportera pas les algorithmes PQC.	22 juil. 2025

Quand la PKI d'IDnomic peut-elle être utilisée pour la PQC ?	La première version d'IDnomic PKI prenant en charge les certificats PQC uniquement sera la version 2.9. Cette version comprendra des fonctionnalités PQC qui ne peuvent être utilisées qu'à des fins de test et ne sont pas recommandées pour une utilisation en production. Notre plateforme de démonstration comprend déjà un environnement pour les tests PQC avec IDnomic PKI et Trustway HSM Proteccio.	22 juil. 2025
À quels besoins répond la PKI en mode PQC ?	IDnomic PKI avec PQC prendra initialement en charge les cas d'utilisation de la signature. Aujourd'hui, nous avons testé les certificats PQC pour l'authentification du serveur web et le VPN.	22 juil. 2025