EVIDEN

Post-quantum Cryptography - FAQ

Post-quantum Cryptography - FAQ

Questions	Responses	Update Date
General Context		
Welche potenziellen Auswirkungen haben Quantencomputer auf die heutige Cybersicherheit?	Unsere Kernkompetenz liegt im Bereich der Kryptografie, einem Teilgebiet der Cybersicherheit. Aus kryptografischer Sicht unterscheiden sich die Bedrohungen je nach Art der verwendeten Kryptografie: • Symmetrisch (z. B. AES): Der Grover-Algorithmus reduziert die Sicherheit um den Faktor zwei. Wir müssen doppelt so große Schlüssel verwenden, um das gleiche Sicherheitsniveau wie heute zu erreichen. • Asymmetrisch (RSA/ECC/DH): Der Shor-Algorithmus bietet eine „schnelle" Möglichkeit, die mathematischen Probleme zu lösen, auf denen die Sicherheit der eingesetzten asymmetrischen Kryptografie (RSA, ECDSA, Diffie-Hellmann usw.) basiert. Um diese Bedrohung zu mindern, gibt es andere asymmetrische Kryptosysteme, die nicht durch den Quantencomputer gefährdet sind: die Post-Quanten-Kryptografie (PQC).	22 juil. 2025
Wie wirkt das Aufkommen von Post-Quanten-Algorithmen auf die IDnomic PKI-Vertrauensinfrastruktur aus?	PKI-Infrastrukturen verwenden digitale Signaturen, um öffentliche Schlüssel für eine Vielzahl von Anwendungen zu zertifizieren. Die in heutigen PKIs verwendeten Signaturen und öffentlichen Schlüssel sind Teil der asymmetrischen Kryptografie, die durch Quantencomputer bedroht ist. PKIs müssen daher quantenresistente Algorithmen (Post-Quanten-Kryptografie) verwenden.	22 juil. 2025

Was sind die internationalen Empfehlungen zum Thema PQC?	Die ANSSI (Frankreich) hat verschiedene Artikel zur Post-Quanten-Kryptografie (PQC) veröffentlicht. Die ANSSI hat unter anderem folgende Empfehlungen herausgegeben: • Eine Liste asymmetrischer kryptografischer Algorithmen, die gegen Quantencomputer gesichert sind (für KEM und Signaturen) • Der Übergang zu post-quantenasymmetrischen Algorithmen muss hybride Vorgehensweise: Verwendung traditioneller Kryptografie zusammen mit post-quantenbasierter Kryptografie (gilt nicht für die USA, wo der hybride Modus nicht vorgeschrieben ist) Wir müssen jetzt vorausschauend handeln und uns vorbereiten ANSSI views on the Post-Quantum Cryptography transition Follow-position-paper-post-quantum-cryptography and PQC transition in France ANSSI views	22 juil. 2025
Welche Schritte können wir jetzt unternehmen, um uns auf den Übergang zu PQC vorzubereiten?	Wir empfehlen unseren PQC Migration Guide. Kurz gesagt, wir empfehlen Ihnen als ersten Schritt, eine Krypto-Bestandsaufnahme durchzuführen, um die Risiken und Herausforderungen im Zusammenhang mit der Post-Quanten-Ära zu identifizieren.	22 juil. 2025

Wie sieht der voraussichtliche Zeitplan für die flächendeckende Einführung der Post-Quanten-Kryptografie aus?	Die ersten Algorithmen wurden standardisiert, und der Übergang ist im Gange. Für die US-Regierung muss der Übergang bis 2035 abgeschlossen sein. In Europa wurde ein erstes Dokument zu PQC mit dem Titel Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography im Juni 2025 vom NIS CG-Arbeitsbereich veröffentlicht und an die Mitgliedstaaten gerichtet.	22 mai 2025
Wie wird Eviden Digital ID einen reibungslosen Übergang zu PQC gewährleisten?	Unsere Forschungs- und Entwicklungsteams arbeiten bereits daran: • Integrationen in Produkte zu Testzwecken • Entwicklung von PoC unter Berücksichtigung verschiedener Anwendungsfälle • Befolgung von Standardisierungen und Empfehlungen von ANSSI, BSI, NIST, ENISA usw. • Support für bestehende Kunden • Gespräche mit HSM-Anbietern	22 juil. 2025
Was sind die besten Vorgehensweisen für Cybersicherheit während dieser Umstellung?	Befolgen Sie die Empfehlungen von Regierungsbehörden und verlassen Sie sich auf internationale Normungsgremien (wie NIST, IETF und ETSI).	22 juil. 2025
PQC Digital ID Products		

Post-Quanten-Algorithmen ML-DSA, SLH-DSA, ML-KEM sowie Hash-basierte Signaturstandards (XMSS, LMS) MÜSSEN unterstützt werden.	• Die Integration von PQC ist Teil unserer Produkt-Roadmap. Da wir die Bouncy Castle-Bibliothek integrieren, profitiert das IDnomic PKI-Produkt von den in dieser Bibliothek enthaltenen Algorithmen, zu denen auch PQC-Algorithmen gehören. Derzeit konzentrieren wir uns auf die Algorithmen ML-DSA (früher Dilithium) und ML-KEM (früher Kyber). Weitere Algorithmen könnten nach Prüfung und Validierung zu einem späteren Zeitpunkt integriert werden. Diese Algorithmen sind bereits seit August 2024 standardisiert: • FIPS 203 (ML-KEM), Module-Lattice-Based Key-Encapsulation Mechanism Standard • FIPS 204 (ML-DSA), Module-Lattice-Based Digital Signature Standard Die hashbasierten Signaturstandards XMSS und LMS wurden 2019 standardisiert: • FIPS 205 (SLH-DSA), Stateless Hash-Based Digital Signature Standard HQC wurde am 11. März 2025 für die Standardisierung ausgewählt und ist noch nicht veröffentlicht (Standard voraussichtlich 2027).	22 juil. 2025
Welche weiteren quantensicheren Kryptografiealgorithmen werden von IDnomic PKI neben dem aufgeführten unterstützt?	Derzeit unterstützt IDnomic PKI ML-DSA nur zu Testzwecken. Weitere Algorithmen werden später unterstützt werden.	22 juil. 2025

PQC-Zertifikate SOLLTEN abwärtskompatibel sein.	Unser Ziel ist es, uns auf Hybridlösungen zu konzentrieren, die sowohl traditionelle als auch PQC-Algorithmen enthalten. Alle Ansätze für PQC-Hybridzertifikate garantieren keine Abwärtskompatibilität mit bestehenden Systemen. Die am weitesten entwickelten Ansätze erfordern heute, dass bestehende Systeme zunächst aktualisiert werden, um diese Hybridzertifikate zu unterstützen. Vollständige PQC-Zertifikate (die nur PQC-Algorithmen enthalten) sind nicht abwärtskompatibel mit bestehenden Zertifikaten. Darüber hinaus können frühzeitig ausgestellte PQC-Zertifikate (hybrid oder nicht) nur für PoCs verwendet werden und müssen ersetzt werden, sobald die Standards (falls noch nicht geschehen) veröffentlicht und als ausreichend sicher angesehen werden.	22 juil. 2025

Ist Ihre PKI-Lösung in der Lage, quantensichere Zertifikate in einer frühen Testphase zu generieren?	Unsere IDnomic PKI-Lösung ist in der Lage, PQC-only-Zertifikate für Testzwecke zu generieren. Mit den neuen Funktionen ist Folgendes möglich: 1. Generieren von PQC-only-Zertifikaten für Tests einschließlich CA-Hierarchie 2. Durchführen von Integrationstests: Verwenden Sie diese Testzertifikate in einer Testumgebung. Dies kann die Konfiguration von Servern, Anwendungen und Netzwerkgeräten für die Verwendung der neuen Zertifikate umfassen, sofern diese das PQC-Zertifikatformat unterstützen. 3. Durchführung von Leistungstests: Bewertung der Auswirkungen von PQC auf die Leistung Ihrer Systeme. PQC-Algorithmen haben andere Rechenanforderungen als herkömmliche Algorithmen. Die meisten PQC-Algorithmen verwenden im Vergleich zu herkömmlichen Algorithmen größere Schlüssel- und Zertifikatsgrößen. Der nächste Schritt in der Roadmap ist die Unterstützung von Hybridzertifikaten, wobei der Schwerpunkt zunächst auf dem Catalyst-Format liegt.	22 juil. 2025
Ist Eviden Digital ID PKI hinsichtlich PQC mit allen auf dem Markt erhältlichen HSM-Einheiten kompatibel?	Heute ist IDnomic PKI mit Trustway HSM Proteccio kompatibel. Wir sind mit anderen Anbietern (Thales, Entrust und Utimaco usw.) im Gespräch über die PQC-Integration.	22 juil. 2025
Könnte OT-PKI PQC unterstützen?	Nein, OT PKI wird keine PQC-Algorithmen unterstützen.	22 juil. 2025

Wann kann IDnomic PKI für PQC verwendet werden?	Die erste Version von IDnomic PKI, die PQC-zertifikate unterstützt, wird 2.9 sein. Diese Version wird PQC-Funktionen enthalten, die nur zu Testzwecken verwendet werden können und nicht für den produktiven Einsatz empfohlen werden. Unsere Demo-Plattform enthält bereits eine Umgebung für PQC-Tests mit IDnomic PKI und Trustway HSM Proteccio.	22 juil. 2025
Welche Anforderungen erfüllt PKI im PQC-Modus?	IDnomic PKI mit PQC wird zunächst Anwendungsfälle für Signaturen unterstützen. Heute haben wir PQC-Zertifikate für die Webserver-Authentifizierung und VPN getestet.	22 juil. 2025