Post-quantum Cryptography - FAQ

Post-quantum Cryptography - FAQ

Questions	Responses	Update date
General Context		
What is the potential impact of quantum computers on today's cybersecurity?	Our core expertise focuses on cryptography, which is a subset of cybersecurity. From a cryptographic point of view, the threats are different depending on the kind of cryptography used: • Symmetric (e.g. AES): Grover's algorithm will reduce security by a factor of two. We'll have to use keys twice as big to have the same level of security as today. • Asymmetric (RSA/ECC/DH): Shor's algorithm provides a "fast" way of solving the mathematical problems on which the security of deployed asymmetric crypto (RSA, ECDSA, Diffie-Hellmann, etc.) is based. In order to mitigate this threat, there are other asymmetric cryptosystems that are not threatened by the quantum computer: the post-quantum cryptography (PQC).	22 juil. 2025
How is our IDnomic PKI trust infrastructure affected by the advent of post-quantum algorithms?	PKI infrastructures use digital signatures to certify public keys for a broad range of applications. The signatures and public keys used in today's PKIs are part of the asymmetric cryptography threatened by the quantum computer. PKIs will therefore have to use quantum-resistant algorithms (post-quantum cryptography).	22 juil. 2025

What are ANSSI's recommendations on PQC?	ANSSI has published different articles on the Post-Quantum Cryptography (PQC). ANSSI shared recommendations including: • A list of asymmetric cryptographic algorithms secured against quantum computer (for KEM and signature) • The transition to post-quantum asymmetric algorithms must be a hybrid approach: use of traditional cryptography with post-quantum one (not for USA, hybrid mode is not mandatory) • We must anticipate and prepare now ANSSI views on the Post-Quantum Cryptography transition Follow-position-paper-post-quantum-cryptography and PQC transition in France ANSSI views	22 juil. 2025
What steps can we take now to prepare for the transition to PQC?	We recommend reading the PQC Migration Guide. In brief, we can recommend you as a first step to initiate a crypto inventory to identify the risks and challenges associated to the post-quantum era.	22 juil. 2025
What is the estimated timeline for the widespread adoption of post-quantum cryptography?	The first algorithms have been standardized and the transition is underway. For US administration the transition must be done before 2035. In Europe, a first document called Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography was published last June 2025 by the NIS CG work stream on PQC and aimed to Member States.	22 mai 2025

How will Eviden Digital ID ensure a smooth transition to PQC?	R&D teams are already working: • integrations into products for tests purposes • on development of PoC considering different use cases, • following standardizations and recommendations from ANSSI, BSI, NIST, ENISA, … • and making support for existing clients • in discussion with HSM providers	22 juil. 2025
What are the best practices for cybersecurity during this transition?	Follow the recommendations of government agencies and rely on international standards bodies (like NIST, IETF and ETSI).	22 juil. 2025
PQC Digital ID Products		

post quantum algorithms ML-DSA,SLH-DSA, ML-KEM, as well as Hashed-Based Signature Standards (XMSS, LMS) MUST be supported.	PQC integration is part of our product roadmap. As we are integrating the Bouncy Castle library, the IDnomic PKI product benefits from embedded algorithms provided by this library, PQC algorithms are part of it. For the time being, we are focusing on ML-DSA (previously named Dilithium) and ML-KEM (previously named Kyber) algorithms. Other algorithms could be integrated later after study and validation. These algorithms are already standardized since August 2024: • FIPS 203 (ML-KEM), Module-Lattice-Based Key-Encapsulation Mechanism Standard • FIPS 204 (ML-DSA), Module-Lattice-Based Digital Signature Standard The hashed-based Signature Standards XMSS and LMS were standardized in 2019: • FIPS 205 (SLH-DSA), Stateless Hash-Based Digital Signature Standard HQC was selected for standardization on March 11, 2025 and is not yet published (standard expected in 2027).	22 juil. 2025
Which post quantum safe cryptography algorithms are supported by IDnomic PKI besides the one listed?	Today, IDnomic PKI supports ML-DSA for tests purposes only. More algorithms will be supported afterwards.	22 juil. 2025

PQC certificates SHOULD be backwards compatible.	Our objective is to focus on hybrid solutions containing both traditional and PQC algorithms. All approaches for PQC hybrid certificates don't guarantee for backward compatibility with existing systems. The most experimented ones require today that existing systems are first upgraded to support these hybrid certificates. Full PQC certificates (containing only PQC algorithms) will not be backward compatible with existing certificates. Moreover, early issued PQC certificates (hybrid or not) can only be used for PoCs and will need to be replaced once the standards (if not yet) will be published and considered as sufficient secure.	22 juil. 2025
Is your PKI solution able to generate quantum safe certificates in an early testing phase ?	Our IDnomic PKI solution is able to generate PQC only certificates for test purposes. With the new features, it is possible to: 1. Generate PQC only certificates for tests including CA hierarchy 2. Perform integration test: use these test certificates into a test environment. This could involve configuring servers, applications, and network devices to use the new certificates, if they are able to support the PQC certificate format. 3. Conduct performance testing: evaluate the impact of PQC on the performance of your systems. PQC algorithms will have different computational requirements to traditional algorithms. Most PQC algorithms are using larger key and certificates sizes compared to traditional algorithms. The next step in the roadmap is the support of hybrid certificates focusing first on catalyst format.	22 juil. 2025

Is Eviden Digital ID PKI compatible with all HSM units on the market concerning PQC?	Today, IDnomic PKI is compatible with Trustway HSM Proteccio. We are in discussion with other providers (Thales, Entrust and Utimaco, etc.) about PQC integration.	22 juil. 2025
Could OT PKI support PQC?	No, OT PKI will not support PQC algorithms.	22 juil. 2025
When can IDnomic PKI be used for PQC?	The first version of IDnomic PKI supporting the PQC only certificates will be 2.9. This version will include PQC features that can only be used for test purposes and are not recommended for production use. Our demo platform already includes an environment for PQC tests with IDnomic PKI and Trustway HSM Proteccio.	22 juil. 2025
What needs does PKI in PQC mode meet?	IDnomic PKI with PQC will initially support signature use cases. Today, we tested PQC certificates for web server authentication and VPN.	22 juil. 2025