Press Release

CryptoNext Security, First Company in the European Union to Receive NIST CAVP Certification for All Three Standardized Quantum-Safe Algorithms.

- **First in the EU**: CryptoNext Security is the first company in the European Union to achieve NIST CAVP certification for **all three** standardized algorithms.
- **Quantum-Safe Technology**: This certification validates the implementations of post-quantum algorithms in CryptoNext Security's Quantum-Safe Library.
- **Path to FIPS 140 Certification**: This is a crucial step towards obtaining the FIPS 140 certification, essential for ensuring the security of devices incorporating CryptoNext Security's technology.

Paris, France – March 10, 2025 – CryptoNext Security, a pioneering leader in cryptographic solutions, is proud to announce that it has become the first company in the European Union to receive the prestigious Cryptographic Algorithms Validation Program (CAVP) certification from the National Institute of Standards and Technology (NIST) for all three standardized algorithms: ML-KEM / FIPS 203, ML-DSA / FIPS 204, and SLH-DSA / FIPS 205. The official certificate (A6638) can be found on the NIST website.

The CAVP certification is a rigorous program that validates the functional compliance of cryptographic algorithms to NIST standards. This achievement underscores CryptoNext Security's commitment to delivering cutting-edge, secure cryptographic solutions that meet the highest international standards.

This certification is a crucial step towards obtaining the esteemed FIPS 140 (CMVP - Cryptographic Module Validation Program) certification, which is essential for ensuring the security of devices incorporating CryptoNext Security's technology. The tests were conducted under the supervision of SERMA Security & Safety, a renowned security evaluation laboratory.

"*Receiving the CAVP certification for all three standardized algorithms is a testament to our dedication to excellence and innovation in cryptographic security*," said Jean-Charles Faugère, Founder and CTO of CryptoNext Security. "*This milestone not only validates our Quantum-Safe Library but also paves the way for broader adoption of our technology in secure and critical applications and embedded systems.*"

CryptoNext Security's Quantum-Safe Library is designed to protect against the emerging threats posed by quantum computing, ensuring that data remains secure well into the future. This certification reinforces the company's position as a leader in post-quantum cryptographic solutions.

About CryptoNext Security

CryptoNext Security is a software company specializing in post-quantum cryptography (PQC) and crypto-agility management solutions. Founded in 2019, the company builds on more than 20 years of academic research in the field of post-quantum cryptography.

CryptoNext Security empowers organizations to seamlessly transition their products, systems, and IT/OT infrastructures from cryptography discovery toward crypto-agile cybersecurity, ensuring long-term resilience against quantum threats. Its solutions also help anticipate and mitigate cryptographic risks over time.

CryptoNext Security's offerings are segmented into three areas to support organizations in their transition to quantum-resilient cybersecurity: evaluation to measure the impact of PQC on applications and infrastructures while gaining expertise, inventory of cryptographic assets to set migration priorities and implement agile crypto management, and embedded solutions to integrate PQC into applications and systems.

CryptoNext Security serves renowned clients in finance, defense, industry, and institutional sectors, where long-term security is crucial.

For more information about CryptoNext Security and its groundbreaking cryptographic solutions, please visit https://www.cryptonext-security.com.

Media Contact:

Nicolas Drouault – Head of Marketing and Communications
nicolas.drouault@cryptonext-security.com

End of Press Release