Press Release

CryptoNext Security's technology used in post-quantum email system experiment by the Banque de France and the Monetary Authority of Singapore.

- The two financial institutions conducted a joint experiment on quantum-resistant email communications.
- This experiment was made possible by using CryptoNext Security's hybrid post-quantum plug-in for Outlook.

Paris, November , 2024 - The Banque de France (BDF) and the Monetary Authority of Singapore (MAS) released a report yesterday detailing the success of a joint international post-quantum cryptography (PQC) experiment leveraging CryptoNext Security's technology. The objective of this initiative was to use quantum-resistant cryptographic algorithms for email signing and encryption, ensuring the future security of electronic communications while maintaining compatibility with current standards, technologies, and digital channels.

This experiment demonstrates not only the practical feasibility of these new security methods but also their effectiveness in widely used application environments.

The post-quantum cryptography was implemented in a hybrid manner, combining the strength of current algorithms with post-quantum algorithms, as recommended by several European security agencies (ANSSI, BSI, NLNCSA, Swedish Armed Forces).

The BDF and MAS report highlights the following key findings:

- *"Using Microsoft Outlook as the email client coupled with CryptoNext's PQC email plugin, BDF and MAS successfully exchanged digitally-signed and encrypted emails using PQC algorithms, namely CRYSTALS-Dilithium and CRYSTALS-Kyber.*
- *The longer key lengths of CRYSTALS-Dilithium and CRYSTALS-Kyber may not have a significant impact on low-transaction applications, such as email usage.*

- *There is potential to integrate this technology into payment networks. By integrating PQC algorithms into payment networks, financial institutions can future-proof their security measures against the looming threat of quantum computing, ensuring the long-term integrity and confidentiality of sensitive financial data."*

Jean Charles Faugère, founder and CTO of CryptoNext Security, stated: *"Using our technology and exptertise, CryptoNext Security is very proud to have contributed to the success of this experiment, advancing the long-term security of communications between two institutions whose mission is to guide the financial community in addressing these emerging threats."*

Download the full publication here.

About CryptoNext Security: *CryptoNext Security is a European software vendor based in Paris, an industry leader in quantum-proof cryptography (PQC) solutions. Our vision and the solutions we are developing are designed to manage the complete lifecycle of post-quantum migration, including the phases of discovery, remediation, and management. Founded in 2019 after 20+ years of academic research within the prestigious INRIA, CNRS and Sorbonne University, CryptoNext Security is identified by Gartner as part of its Top 5 in PQC and is, to date, the first European company selected by NIST's NCCoE group dedicated to the best PQC migration practices. We are developing an integrated, quantum-safe remediation suite allowing for the automation of PQC migration for IT/OT systems, infrastructures and applications. Our objective is to help businesses and HW/SW vendors face the quantum threat in an efficient, agile and sustainable way.*