PRESS RELEASE

# CryptoNext Security announce immediate support of algorithms selected by NIST for its post-quantum cryptography solutions

- NIST has announced its first selection of standard algorithms for quantum computer-resistant cryptography. The ANSSI and BSI agencies have indicated their support for it.
- Enterprises can now consider going live with their post-quantum protection for their IT/OT data, systems and applications.
- CryptoNext Security solutions already implement the selected standards as well as a full range of integration and migration tools to enable customers to master this strategic transition.

**Paris, September 21st, 2022** – CryptoNext Security SAS (CryptoNext), European post-quantum cryptography (PQC) pioneer and leader vendor welcomes with enthusiasm the announcement by the National Institute for Standards & Technology (NIST), opening a new phase in the effective setup of cybersecurity protections against threats coming with quantum computers.

Advent of Quantum Computer opens great opportunities through huge computing capabilities to tackle inaccessible problem solving until now. It also comes with a new major threat for our cybersecurity through its capacity to « break » the public-key cryptosystems that secure today's internet and IT infrastructures.

Suh quantum threat and its remediation is the rising emergency for today, considering :

- Already existing « Harvest now/Decrypt later » attacks where state or private organizations have started to collect massive amount of datas in order to decrypt them later as soons as a powerful enough quantum computer will be available (impact on long-life sensitive data)
- Migration of technical infrastructures and applications towards quantum resistance full operational capacity typically are counted in years.
- Products life cycle from design to end of operations most frequently exceeds 15-20 years as observed in the Industrial IoT space.

It is in this context that, on July 5, 2022, at the end of a process initiated in 2016 for the selection of new public key cryptography standards intended to resist the quantum computer, the NIST unveiled its first selection.

Four algorithms are selected at this stage including one for the key exchange (Key Exchange Mechanism - KEM) namely Crystals-Kyber, as well as for the digital signature (Digital Signature - DS), Crystals-Dilithium in first choice, accompanied by 2 other alternatives: Falcon (for shorter signatures) and Sphincs+ (based on different mathematical problems to have diversity).

Beyond this first selection, the NIST announces the continuation of this process in the form of 2 initiatives:

- The passage of several KEM algorithms not selected at this stage in thorough examination (Round 4).
- The opening in June 2023 of a new call for submissions to offer short signatures and a rapid verification mechanism.

The main European national agencies have in the process, abounded in the same direction by providing additional details:

- • In July 2022, ANSSI in France confirmed its support for the selected algorithms and recalled its scientific opinion (position paper) of January 22 on the recommendation of hybridization (except Sphincs + for which hybridization is not necessary ) and its position for an unclosed list of algorithms: it renews its support for the examination of new algos, in particular FRODOKEM for high security apps.
- The BSI in Germany had already communicated in May 2022 its support for this standardization process with a similar recommendation to take FRODOKEM into account. In July, it stressed the urgency : « *migration to post-quantum cryptography, the standardization of which is already well advanced in the NIST process, a clear priority from BSI's point of view* ».

For its part, the NSA, in its press release on the new CNSA2.0 cybersecurity directives published on September 7, 2022, also recommends the use of Crystals-Kyber for KEM, Crystals-Dilithium and Xtended Merkle Signature Scheme (XMSS). It underlined the urgency: « Software and firmware signing : Begin transitioning immediately »

Florent Grosmaitre, President & CEO of CryptoNext Security points out that : « *NIST's decision and support from national security agencies is a game-changer. These are now production projects that should be carried out without delay for everything containing sensitive data as well as updating all the corresponding hardware and software infrastructures*.»

As a European pioneer, CryptoNext Security has participated in this competition since its creation, particularly following the filing of the GEMSS algorithm for short signatures, the recommended typology for the new DS call for submissions.

Thanks to its involvement in this process and with standardization bodies, CryptoNext Security anticipated the selection very early on, by:

1. Integrating all the finalist algorithms of the 3rd round of the competition into its library.
2. Developing a high-level library, natively crypto-agile and ready for hybridization as well as the suite of software tools constituting its PQ integration platform.
3. Introducing Kyber and Dilithium as default algorithms in its library.
4. Already integrating the FRODOKEM algorithm.

Jean-Charles Faugère, Co-Founder & CTO of CryptoNext Security highlights : « *We welcome the decision of NIST and the position of ANSSI, BSI, NLNCSA, etc… which we had anticipated and encourage companies to concretely implement in production the post-quantum security of their infrastructures, data and the most sensitive applications without delay. We also welcome the BSI/ANSSI/NLNCSA position on FRODOKEM based on an unstructured mathematical problem and offering a reduced attack surface at the cost of a performance impact. We recommend focusing for the time being only on the 4 selected algorithms + FRODOKEM in Europe, recent events having shown the deficiency of certain algorithm proposals not selected*.»

CryptoNext Security has developed its offer to take into account this new complexity induced by the transition from a situation based on a single standard (RSA then ECC) for signing and for key

exchange, to a situation including distinct algorithms for each of the functions, and a variety of algorithms in each case. Such variety is made necessary given their low maturity, the evolution of protocols and their standardization to which CryptoNext Security actively contributes, as well as the variety of use cases.

To this end, CryptoNext Security has natively integrated, both at the level of its library of cryptographic algorithms and its tools for integrating cryptographic protocols, the notions of crypto-agility and hybridization recommended by the agencies.

« *All of these algorithms and the associated implementations have already been the subject of multiple operational customer deployments* » says Florent Grosmaitre, adding that « *The "CryptoNext Quantum Safe Suite" multi-level software platform (library, protocol and migration tools, application plugins) is already ready for these new international and European standards, deployed at large users, service providers, equipment manufacturers and publishers for the end-to-end security of multiple use cases. It provides a guarantee of expertise, mastery and timing of deployment at controlled costs in this context where time is now running out with clarified standards.*»

## About CryptoNext Security

CryptoNext Security, based in Paris, was created in 2019 following more than 20 years of academic research. CryptoNext Security is a software vendor specializing in quantum computer resistant cryptography (PQC: post-quantum cryptography). CryptoNext offers its software suite of quantum-resistant tools and applications "Quantum Safe Software Suite", including its world reference library Quantum Safe Library (C-QSL) with the entire selection of NIST algorithms, to user enterprises and integrators, to help them in their migration to the era of post-quantum cybersecurity.
CryptoNext Security was cited among the 5 reference leaders of the report on post-quantum cryptography by Gartner in October 2021 and distinguished in 2022, Innovation Prize from "les Assises de la Sécurité". For more information, visit www.cryptonext-security.com

## Contacts

For CryptoNext Security : Christian d'Orival, Chief Revenue Officer. Email: christian.d-orival@cryptonext-security.com