CryptoNext — Post Quantum Cryptography Remediation

CRYPTONEXT SECURITY

Vertical
Cybersecurity

Founders
Florent Grosmaitre (CEO)
Jean-Charles Faugère (Co-founder & CTO)

AVP Investment
Series A / November 2023

https://www.cryptonext-security.com/

Company Description

Quantum computers are capable of breaking public-key cryptosystems in seconds. Next generation post-quantum cryptography is out there. Our mission is ultimate post-quantum remediation. Cryptonext provides optimal end-to-end post-quantum cybersecurity remediation tools and solutions for IT/OT infrastructures & applications to enable governments, enterprises & organizations to deliver long-term, trusted services of undisputed quality.

CryptoNext Security is a pioneer in post-quantum cryptography. Founded in 2019 as a start-up after 20 years+ of founders academic research at the Sorbonne University (SU), INRIA and CNRS in Paris

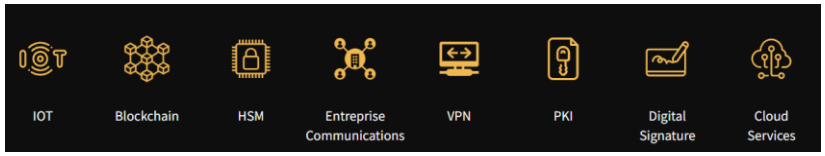
Differentiation

Comprehensive, hi-performance, agile software tool suite is designed to secure critical data, applications and systems long-term

Target Segment

Governments, Ente
Organizations

Use Cases & Selected Partners



BANQUE DE FRANCE EUROSYSTÈME · NATO OTAN · THALES · EDF · orange · IDQ

Market Solutions & Use Cases

Messaging Applications
Popular secured messaging apps used by consumers are now widely used in the Enterprise space. User transparent end to end Post-Quantum authentication and secured communications through an additional layer of quantum resistant cryptography along with Enterprise groups features are required.
See NATO Use Case

Virtual Private Network
Create a full chain of trusted communications: quantum safe VPN with quantum safe authentication.
See Banque de France Use Case

Digital Certificates Solutions
IT/OT teams use PKI for authentication and encryption, while digital certificates and signatures are vulnerable to quantum-enabled attacks. Use crypto-agility to upgrade critical assets and ensures interoperability with long term "quantum resistant" certificates, backward compatiblewith current formats.
See Major Certificate Provider Use Case

Digital Signature Solutions
Integrity of digitally signed contracts is not anymore guarantee, including the signature date. Solution is to add a quantum resistant time stamp.
See Leading European Bank Use Case

HSM Equipment & Solutions
Upgrade your HSM with a hybrid quantum resistant cryptographic Integration of CryptoNext software for a transparent use throughPKCS#11 API, whilekeeping HSM's certification.
See Thales Use Case

Internet Of Things & Embedded System
From defense to automotive or medical IoT, systems rely on the root public key for software/firmware future-proof code signingandover-the-air updates. We enable quantum-safe algorithms to run on resource-constrained devices.
See Defense Industry Use Case

Public Key Infrastructure
PKI is a fundamental infrastructure for many use cases that needs to be upgraded with PQC due to the quantum threat. It can be implemented with simple configuration with or without HSM.
See Top-Tier Commercial Bank Use Case

Mobile Communications
Enabling quantum resistant voice, message or video calls with secured smartphones brings user transparent end to end PQ authentication and securedcommunications through an additional layer of quantum resistant cryptography.
See French MOD Use Case

Quantum Computing Infrastructure
PQC brings authentication required to secure QCI QKD (Quantum Key Distribution) network backbones.
See Orange Paris QCI Use Case

Blockchain
Blockchains use RSA or Elliptic curves algorithms for public key cryptography. Work on code structure and PQC signature schemes upgrade and bring crypto-agility, something no blockchain should be without.