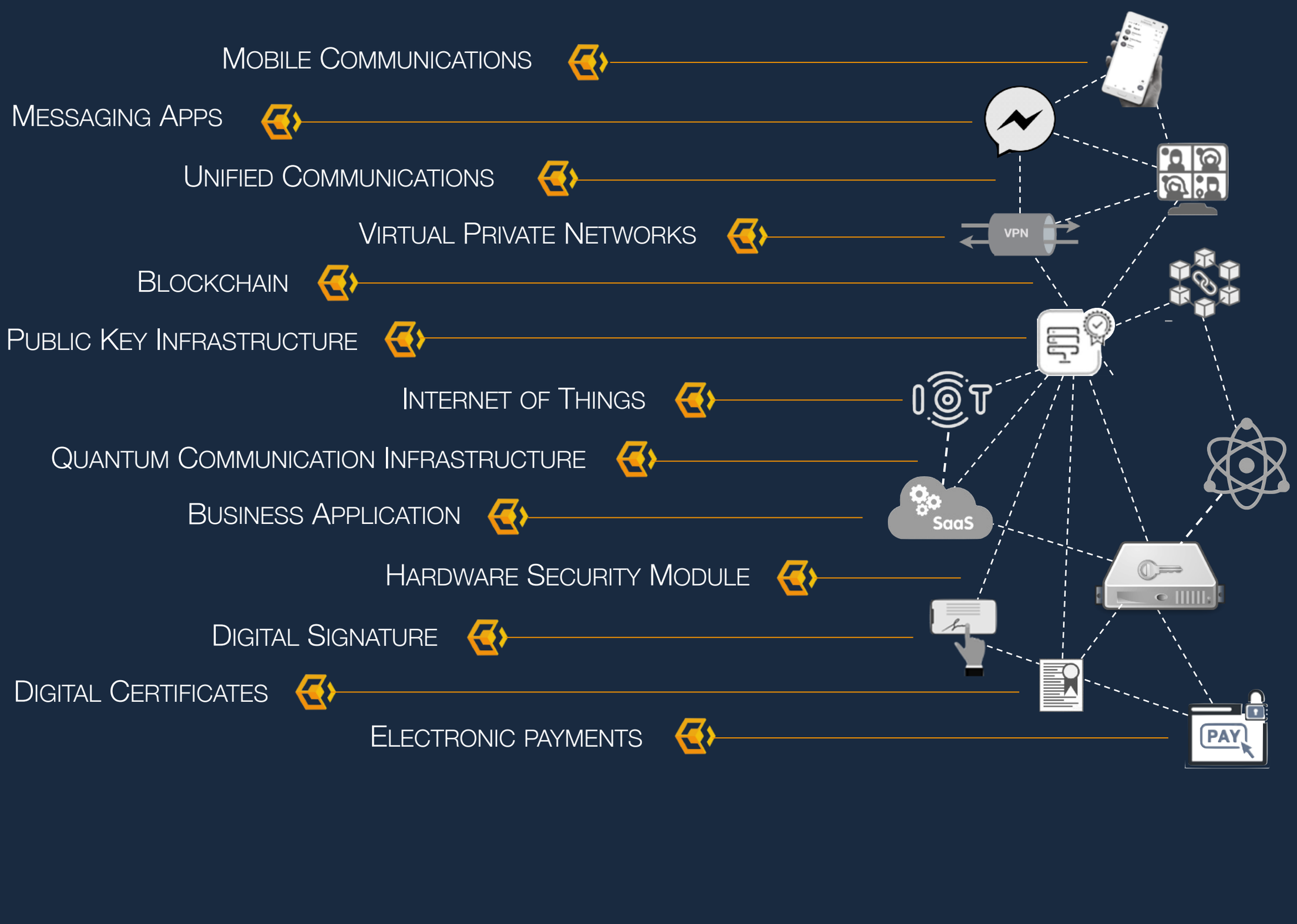
CRYPTONEXT SECURITY

Ultimate Post Quantum Security

We design a comprehensive, hi-performance and agile
quantum safe cryptography software suite
to secure critical datas, applications and systems for the long-term



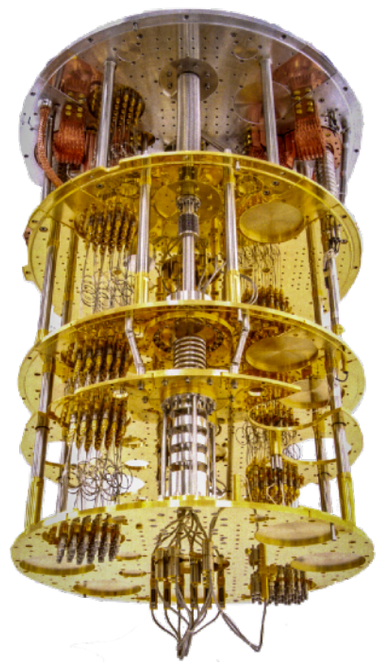
CRYPTONEXT SECURITY

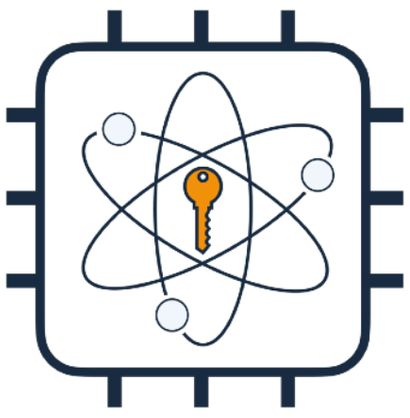
TAKE CONTROL OF YOUR POST QUANTUM SECURITY REVOLUTION

THE QUANTUM THREAT

Quantum computer will be able to break in few minutes public key crypto-systems (RSA, Elliptic curves).

The impact of this threat is systemic for the security of IT infrastructure as public key cryptography is everywhere.





Lattice based, Code based, Hash based, Multivariate based…

POST QUANTUM CRYPTOGRAPHY (PQC)

New harder quantum-safe mathematical problems have to be find to build a new quantum resistant cryptography or Post Quantum Cryptography.

A standardisation process is in course for the selection of algorithms (ex: NIST in US) and for defining new hybrid protocols (ex: IETF for X.509)

INITIALIZE TRANSITION « AS SOON AS POSSIBLE »

« The risk is now too high and can no longer be ignored » (NIST).

The following elements have to be considered:

- Timing of transition to new cryptography before the « Q-Day »
- Product life cycle ; for example for Industrial IoT, or automotive
- « Harvest now, and decrypt later » for sensitive long term data. For long term data with a value after 2030, ANSSI advises to initialize the transition « as soon as possible » with hybrid mechanisms.

Bundesamt für Sicherheit in der Informationstechnik

ANSSI

NIST National Institute of Standards and Technology

CRYPTONEXT QUANTUM SAFE SOLUTION

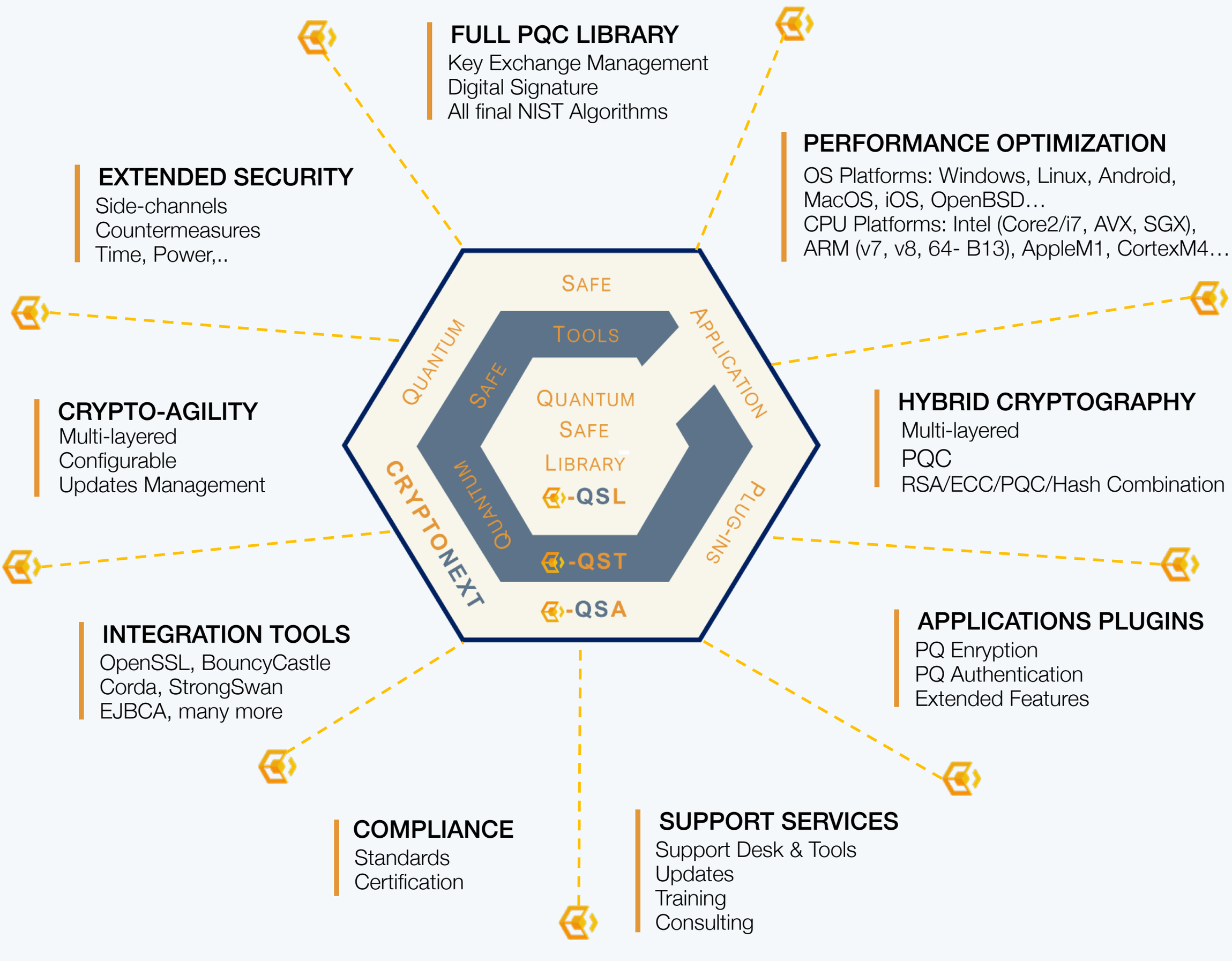
C-QS Solution enables customers build a smooth, controlled efficient migration path to the disruptive post-quantum era for the long-term at minimal costs.

C-QS Solution is a customizable integrated software suite, designed with end-to-end transition in mind, based on its core CryptoNext's Quantum Safe Library, a comprehensive set of Quantum Safe Tools & Applications and Maintenance & Support Services.

CryptoNext Quantum Safe Technology & Solution

CryptoNext Quantum Safe Software Suite C-QS Suite*

C-QS Intelligence relies on an end-to-end vision for ultimate PQ security, performance, and integrated view at all levels: algorithms, protocols, tools and applications with long-term agility and evolution in mind.



C-QS Framework is a customizable integration of products & services:
CryptoNext's Quantum Safe Library (C-QSL), Tools (C-QST), Applications (C-QSA) as well as Consulting & Support Services (C-MSS)

Unique technology For multiple applications

Post Quantum Cryptography security is a concern for almost all IT applications.
Amongst most well-known examples are:

Mobile communications & Messaging Apps

Brings user transparent end to end secured communications (voice, message, video calls) through an additional layer of quantum resistant cryptography.

Virtual Private Networks

Create a full chain of long term trusted communications with hybrid post quantum key exchange and hybrid post quantum authentication

Hardware Security Modules

Upgrade your HSM with CryptoNext's functional module, that brings a transparent hybrid quantum resistant cryptographic solution (with PKCS#11 API).

Public Key Infrastructures & Digital certificates

IT/OT teams use PKI for authentication, while digital certificates are vulnerable to quantum-enabled attacks. Use crypto-agility to upgrade critical assets and ensures interoperability with long term "quantum resistant" certificates, backward compatible with current formats

Internet of Things - IoT & Embedded systems

From automotive to medical IoT, systems rely on the root public key for software/firmware future-proof code signing and over-the-air updates. We enable quantum-safe algorithms to run on resource-constrained devices.

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.

Blockchain

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

Electronic Payments

All onsite and online payments will require infrastructures using Post-Quantum Cryptography to secure the transactions.

www.cryptonext-security.com

16 Boulevard Saint Germain
75005 Paris - France

contact@cryptonext-security.com

+33 1 84 60 84 29