CRYPTONEXT SECURITY

Post-Quantum Remediation

Effective . Simple . Sustainable

The new generation of
Quantum Resistant Cryptography

PROGRAMME DE TRANSFERT AU CAMPUS CYBER

Sécurité Numérique à l'Ère Quantique : Opportunités et Défis

Migration post-quantique: Outils, bonnes pratiques et cas d'usages

Campus Cyber - June 25th, 2024
Jean-Charles Faugère, Founder & Chief Technical Officer

Table of contents

1 CryptoNext Security: Société, histoire & filiation

2 Menaces, technologie, standards & solutions

3 Planification stratégique & Applications clients

4 Enjeux: Innovation, souveraineté & partenariats

Post-Quantum Remediation

Effective . Simple . Sustainable

CRYPTONEXT SECURITY

Pioneering Post Quantum Cryptography (PQC) cybersecurity transition

Spinoff of INRIA, CNRS, and SU, founded in 2019, after 20 years of academic research, **CryptoNext Security provides « Post Quantum cryptography » or « quantum resistant cryptography » software solutions** in order to help private and public organizations to manage smoothly the « quantum threat »

Scientific excellence and awards

Selection in **final round of US competition** for new standards (15 / 90 internat. teams)

NIST National Institute of Standards and Technology U.S. Department of Commerce

3rd prize in Chinese competition
(Only international team reward)

中国密码学会 Chinese Association for Cryptologic Research.CACR

Selection by the NCCoE with 18 international leading vendors for **Migration to PQC** project

NCCoE National Cybersecurity Center of Excellence

Many startup awards

i-Lab · Banking Cybersecurity Innovation Awards · Plug and Play Enterprise Tech · Prix de l'Innovation LA 22 · Paris Air Forum 2020 · Future 40 by Station F · Accélérateur Hexatrust · ---

Ready innovative technology with proven deployments

CryptoNext - Quantum Safe Remediation Suite
Multi-layer migration solution for data, applications, infrastructure with:

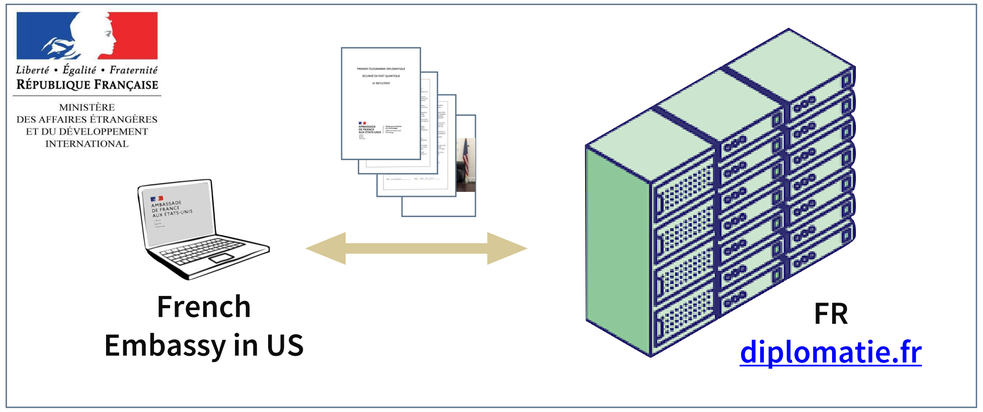
- core technology PQ Cryptographic Library
- upper layers with integration tools and application plugins with hybrid or pure PQ protocols of communication (TLS, IPSec, X.509…)

Clients

Ministère des Armées · Thales · NATO OTAN · Deutsche Bundesbank Eurosystem · Leading US Energy Corp. · Major Certificate provider · Banque de France Eurosystème · MBDA Missile Systems · Leading Bank EU · EDF · Société Générale · ---

In Dec 2022, President Macron announced the first diplomatic telegram secured in Post Quantum !

… Done with CryptoNext Security technology !



Diplomatic telegram sent during the State visit of President Macron in Washington DC in December 2022

Press release of French Ministry of Foreign Affairs quoting CryptoNext Security technology

Tweet of President Macron

TABLE OF CONTENTS

1 CRYPTONEXT SECURITY: SOCIÉTÉ, HISTOIRE & FILIATION

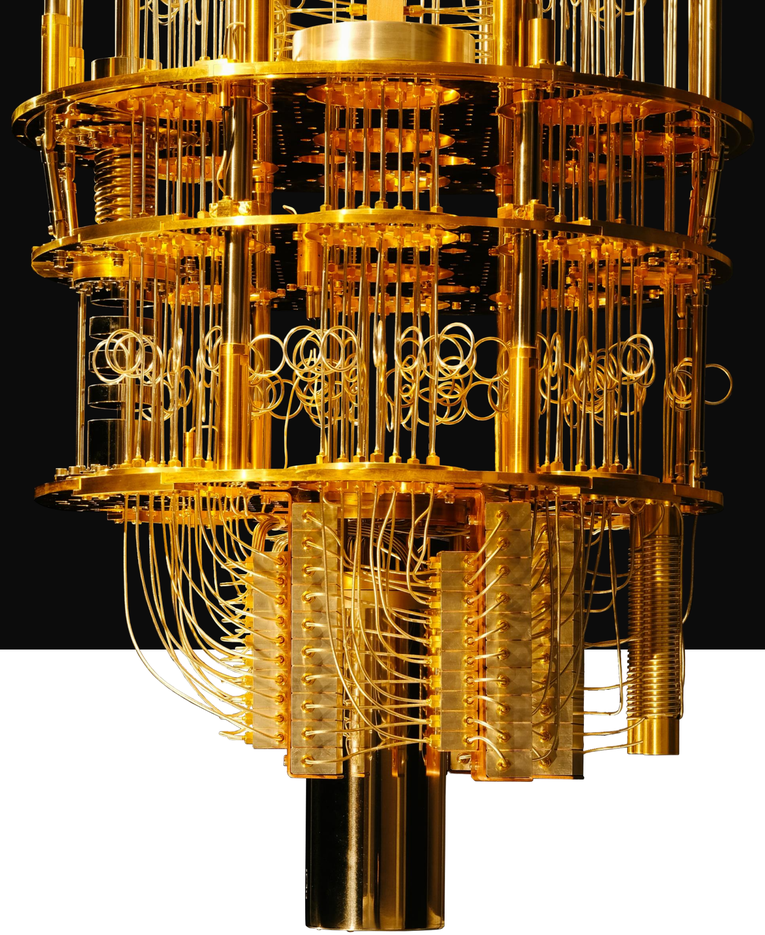
2 MENACES, TECHNOLOGIE, STANDARDS & SOLUTIONS

3 PLANIFICATION STRATÉGIQUE & APPLICATIONS CLIENTS

4 ENJEUX: INNOVATION, SOUVERAINETÉ & PARTENARIATS

Post-Quantum Remediation
Effective . Simple . Sustainable

CRYPTONEXT SECURITY



THE QUANTUM THREAT

Quantum computer will be able to break within few seconds **public key cryptosystems.**

- RSA - ECC - Classic computer : hundreds to thousands years
- RSA - ECC - Quantum computer : **few seconds**

A SYSTEMIC IMPACT ON CYBERSECURITY

Public key cryptography is everywhere ; the **security of Internet is in question**. All private and public organizations are concerned and will have to migrate their IT infrastructure to **Quantum Resistant IT infrastructure** in the next years.

Secured web

VPN

Mobile messaging

Web-conference

Payments

Identity - PKI

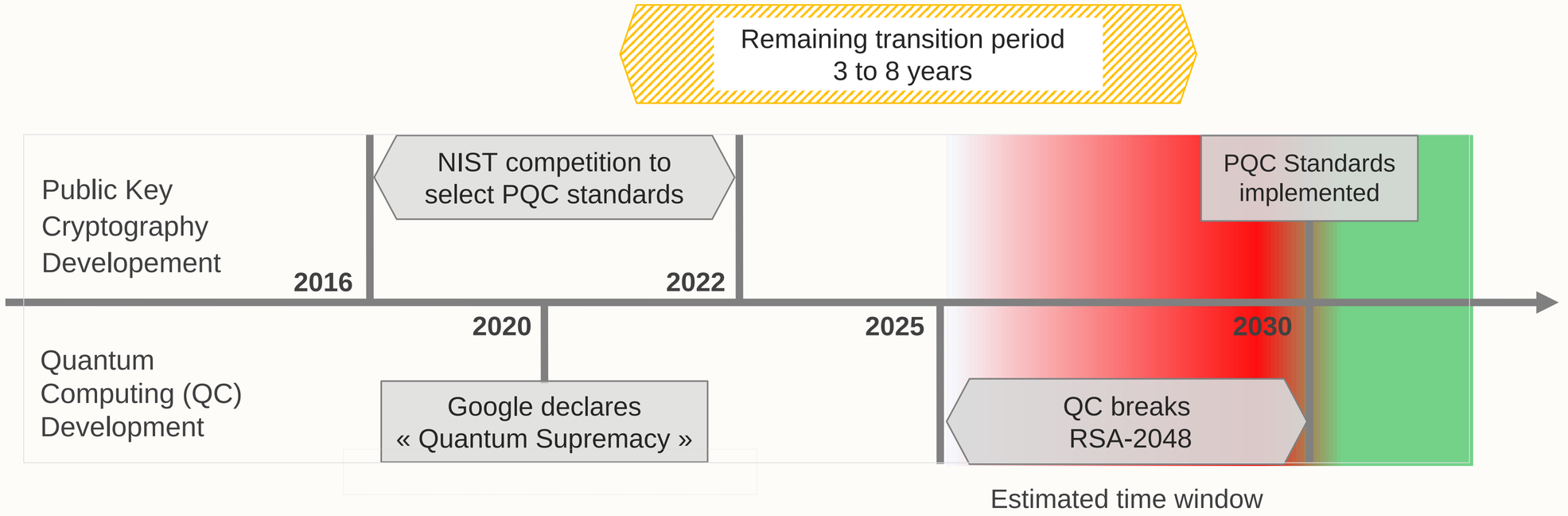
Digital Signature

Blockchain

A TIME BOMB ON CYBERSECURITY

HARVEST NOW, DECRYPT LATER

TIME TO CONDUCT TRANSITION PLAN BEFORE Q-DAY IS GETTING SHORTER



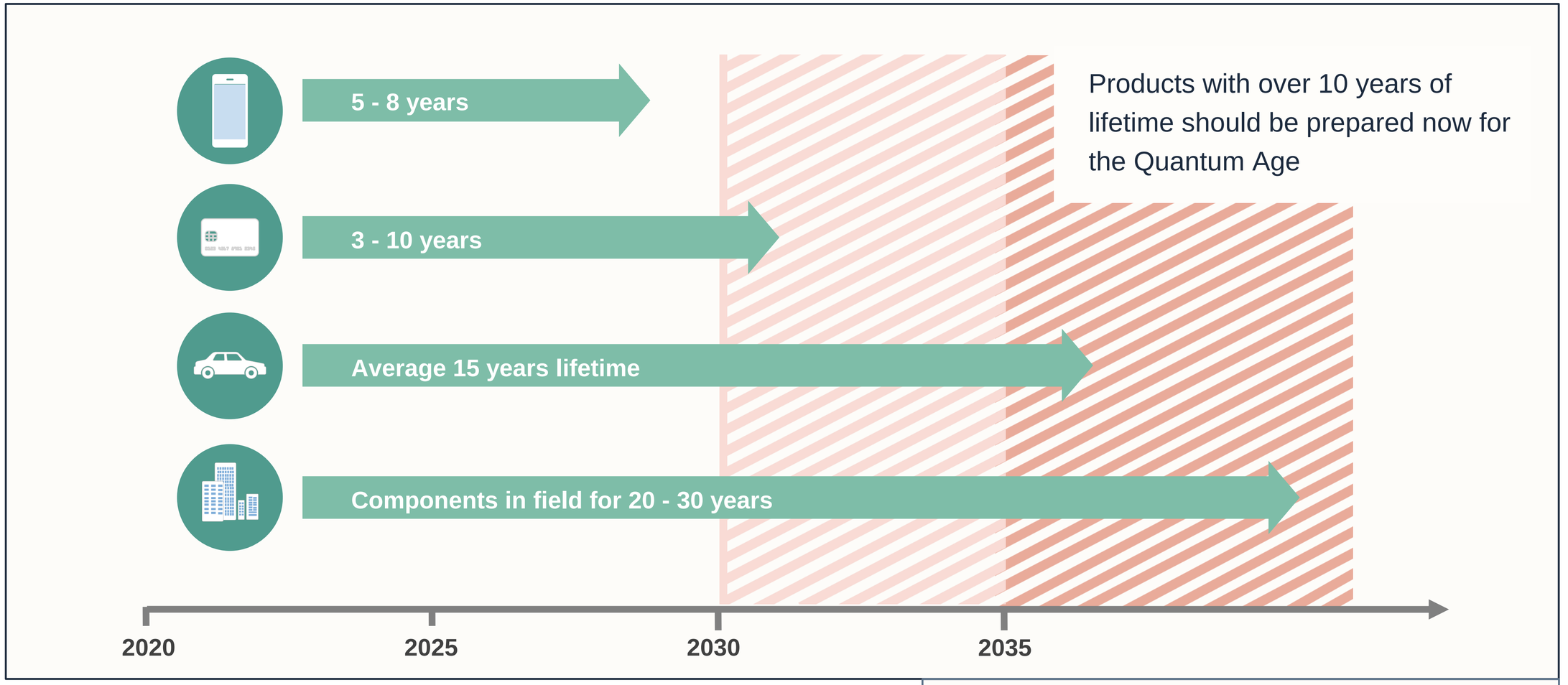
Data encrypted with Current Public Key Protocols already vulnerable to « harvest now, decrypt later » attacks

Public-Key Cryptography vulnerable to QC

Public-Key Cryptography resistant to QC

BCG – March 2021 - Ensuring Online Security in a Quantum Future

THE PRODUCT LIFE CYCLE MUST BE TAKEN INTO ACCOUNT TO ANTICIPATE Q-DAY



Infineon – July 2021 - PQCrypto conference - Seoul

STANDARDISATION AND REGULATION ACTIVITIES AS A KEY DYNAMIC DRIVER

NIST National Institute of Standards and Technology U.S. Department of Commerce

A LONG AND ON-GOING PROCESS OF NEW QUANTUM RESISTANT CRYPTOGRAPHIC COMPETITION

XMSS IETF RFC 8391 (2018)

LMS IETF RFC 8554 (2019)

→ Stateful Hash-Based Signature Schemes
NIST SP 800-208, 2020

→ Revision
NIST SP 800-208, 2024

NIST round 1
(2016 – 2018)
(86 submissions)

→ NIST round 2
(2019 – 2020)

→ NIST round 3
(2020 – 2022)
(15 submissions)

→ Selection July 2022
Key Exchange: **Kyber**
Signature: **Dilithium**, Falcon, Sphincs+

→ PQC standards drafts
ML-KEM,ML-DSA,ML-SLH
2023

→ **PQC standards**
August.,2024

NIST round 3 (2020 – 2022) (15 submissions) → NIST round 4 - from 2022
(Key Exchange - 4 submissions)

→ Final Selection
Fall 2024

ACCELERATION IN US

NIST new call - from 2023
(Signature alternative schemes
(≈ 40 submissions)

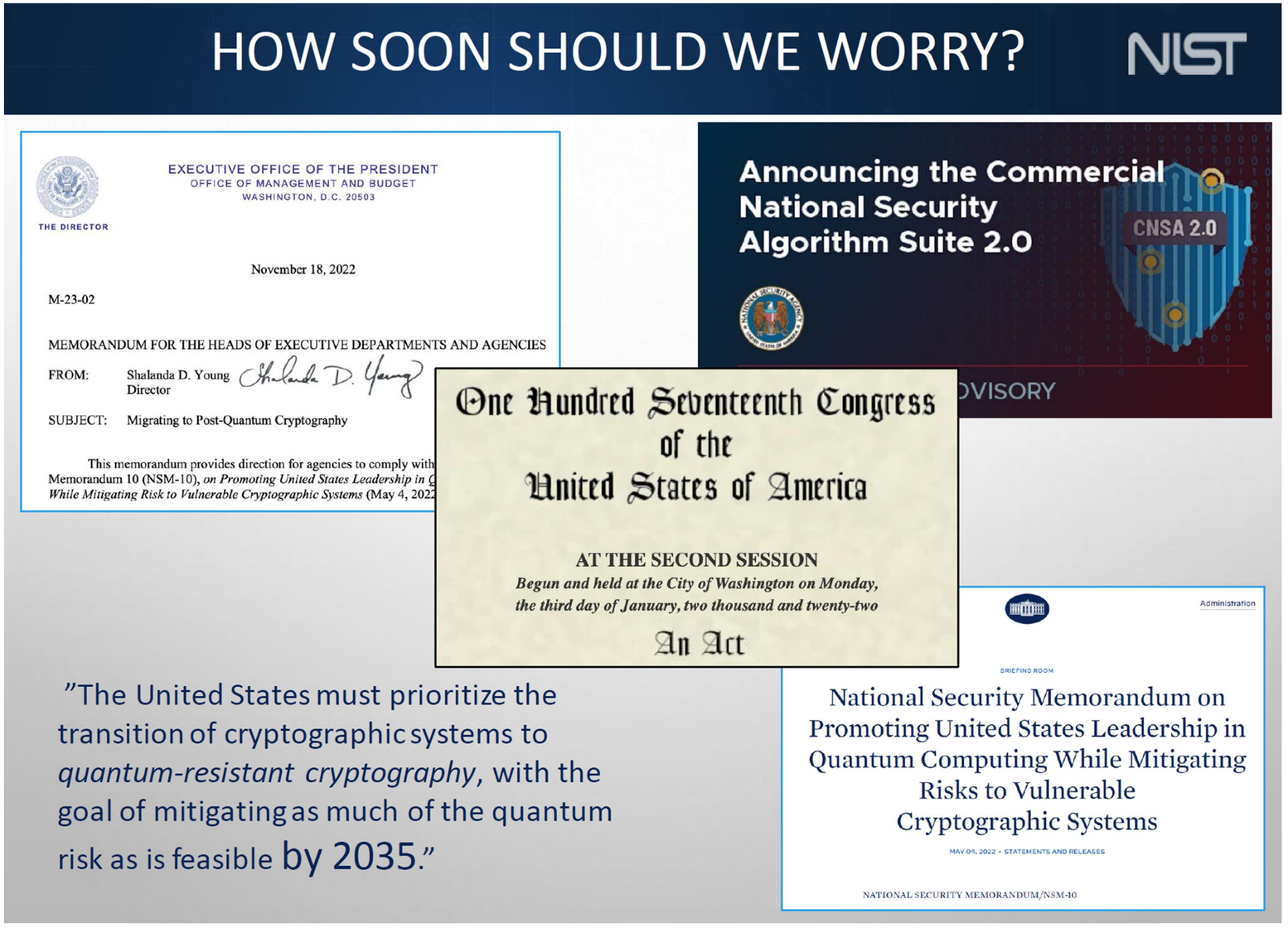
→ Round 2
End 2024

- **FIPS 203 :** Module-Lattice-Based Key Encapsulation Mechanism: 3 algorithms ML-KEM-512, ML-KEM-768, and ML-KEM-1024 (based on Kyber)
- **FIPS 204 :** Module-Lattice-Based Digital Signature : 3 algorithms ML-DSA-44, ML-DSA-65, and ML-DSA-87 (based on Dilithium).
- **FIPS 205 :** Stateless Hash-Based Digital Signature : 12 algorithms (3 security levels, 2 underlying hash options SHA-2/SHAKE-256).
- **FN-DSA (Falcon):** under development.

STANDARDISATION AND REGULATION ACTIVITIES AS A KEY DYNAMIC DRIVER OF THE MARKET

HOW SOON SHOULD WE WORRY?

ACCELERATION IN US



Are we there yet ? *Dustin Moody, 2024, 5th PQC standardization conference*

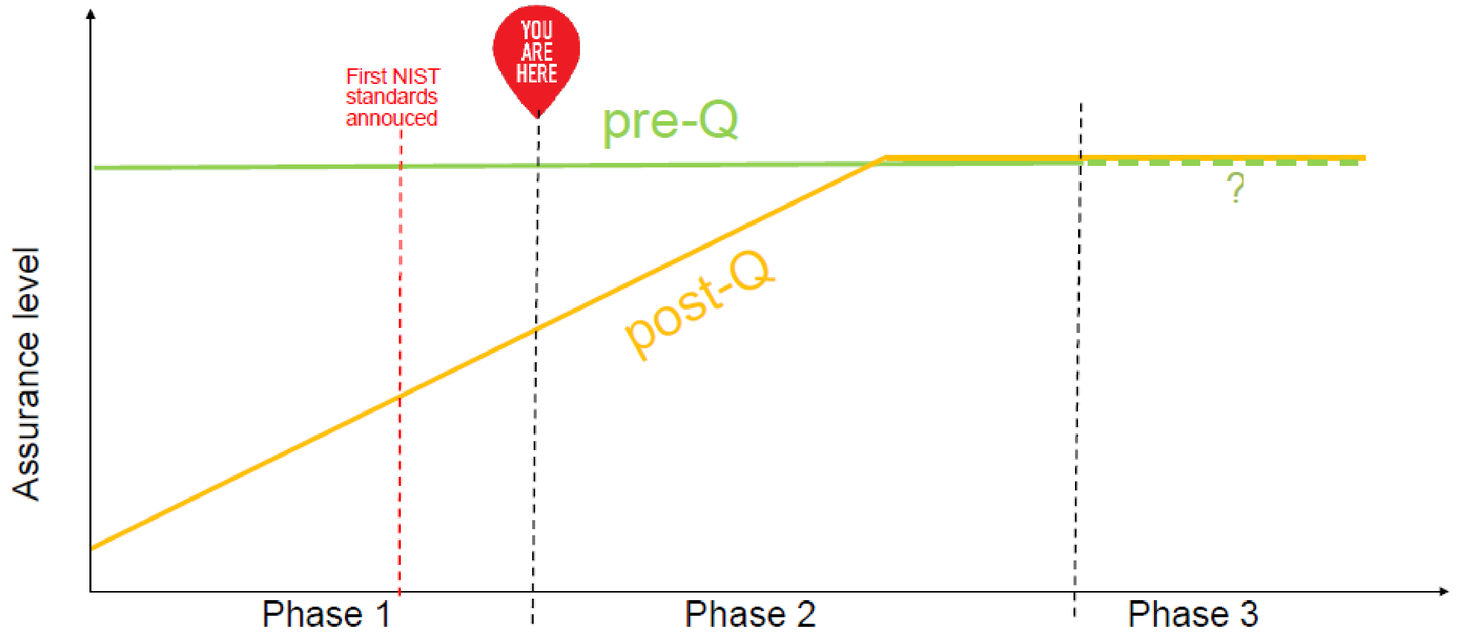
STANDARDISATION AND REGULATION: A KEY DRIVER FOR LARGE SCALE MIGRATION

FRANCE'S ANSSI STIMULATES AN ACTIVE TRANSITION « AS SOON AS POSSIBLE »

"For security products aimed at offering a long-lasting protection (after 2030) of information: ANSSI encourages to start transitioning with hybrid mechanisms as soon as possible."

- *ANSSI (National French Agency for Security of Information Systems), Dec 2021*
- *ANSSI views on the Post-Quantum Cryptography transition, Dec. 2023*

Dec. 2023
ANSSI also decided **to speed-up the original agenda**. First French security visas for products implementing **hybrid post-quantum cryptography** are expected to be delivered around **2024- 2025**.



Hybrid PQC as a defense-in-depth add-on.

Hybrid PQC as post-quantum mitigation.

TBD depending on the context and PQC assurance level

HYBRID CRYPTOGRAPHY (ANSSI view)

ANSSI Agence nationale de la sécurité des systèmes d'information

A *hybrid* mechanism (key establishment or signature) **combines** the computations of a **recognized pre-quantum public key** algorithm **and** an **additional algorithm** conjectured post-quantum secure.

- This makes the mechanism benefit both from the **strong assurance** on the resistance of the first algorithm against classical attackers **and** from the conjectured resistance of the second algorithm against quantum attackers.
- Certain hybrid protocols are in standardization processes like for TLS 1.3 or for IKEv2.

STANDARDISATION AND REGULATION ACTIVITIES AS A KEY DYNAMIC DRIVER OF THE MARKET

CRYPTONEXT'S PARTICIPATION TO STANDARDISATION BODIES & COLLABORATIVE INITIATIVES

NIST COMPETITION FOR THE DEFINITION OF NEW STANDARD PQC ALGORITHMS

Participation of Jean-Charles Faugère and CryptoNext Security

- NIST Round 3 (Alternative Signature GEMMS)
- NIST New call for alternative signature schemes

NCCOE - COLLABORATIVE GROUP ON THE MIGRATION TO PQC

Participation to the initiative of NCCoE (US NIST organisation) to share the Best Practise for the migration to PQC and to stimulate inter-operability of the solutions.

- Selection by NCCoE with 20 international leaders on the topic (AWS, Microsoft, IBM, Cisco, Isara…)
- Active participation to migration & inter-operability workstream (sub-groups TLS, HSM…) and leading X.509 working group.

IETF FOR THE DEFINITION OF NEW STANDARD PQC PROTOCOLS

The definition of new protocols and cryptographic standards (such IPSec, TLS, X.509, PKCS#11…) - hybrid or pure PQ - is a key challenge aside the PQ algorithm definition.

- Technical watch in order to implement the last RFC, including the drafts in course of definition.
- Proposal of new RFC (S/MIME in collaboration with Entrust) and participation to the working groups (LAMPS, IPSec…)
- Participation to dedicated groups for validating inter-operability (X.509 hackathon).

POST-QUANTUM CRYPTOGRAPHY COALITION (SEP. 2023)

- Various working groups

X.509 PQC Formats

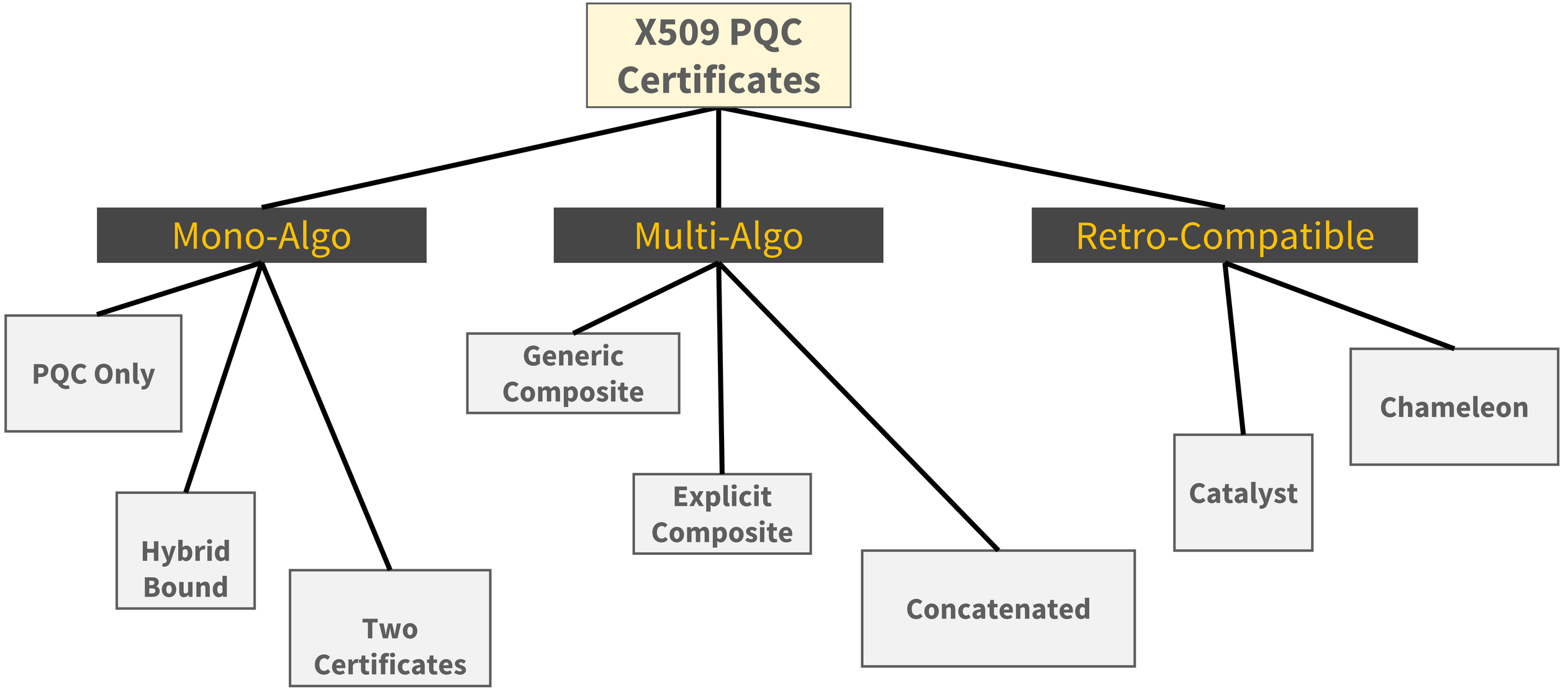


TABLE OF CONTENTS

1 CRYPTONEXT SECURITY: SOCIÉTÉ, HISTOIRE & FILIATION

2 MENACES, TECHNOLOGIE, STANDARDS & SOLUTIONS

3 PLANIFICATION STRATÉGIQUE & APPLICATIONS CLIENTS

4 ENJEUX: INNOVATION, SOUVERAINETÉ & PARTENARIATS

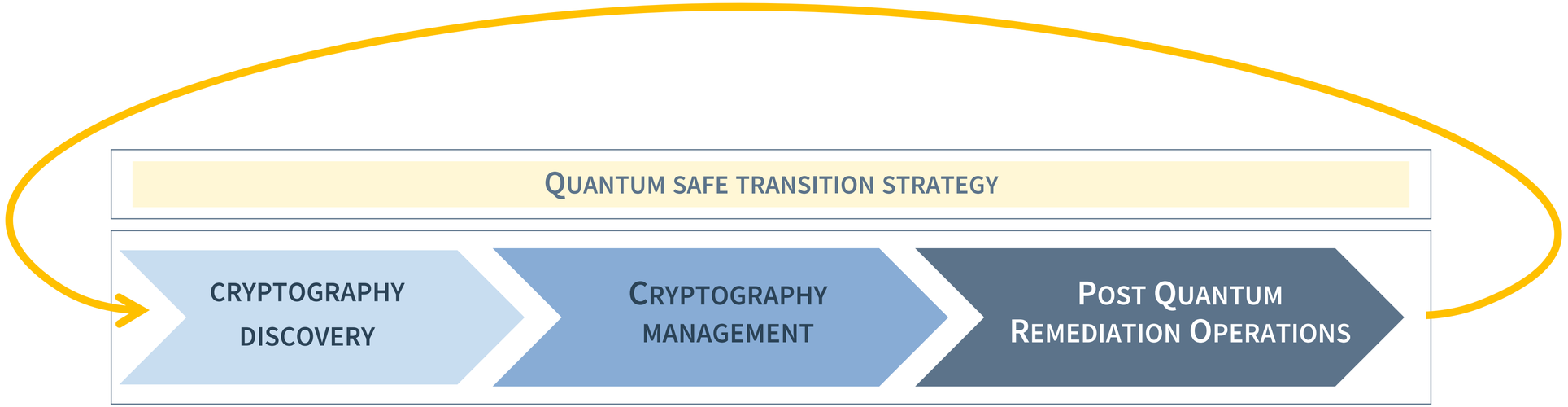
Post-Quantum Remediation
Effective . Simple . Sustainable

CRYPTONEXT SECURITY

Post Quantum transition path

Post-Quantum Safe Remediation Maturity

All organizations will have to set up and pilot a post quantum transition plan



POST QUANTUM TRANSITION PATH

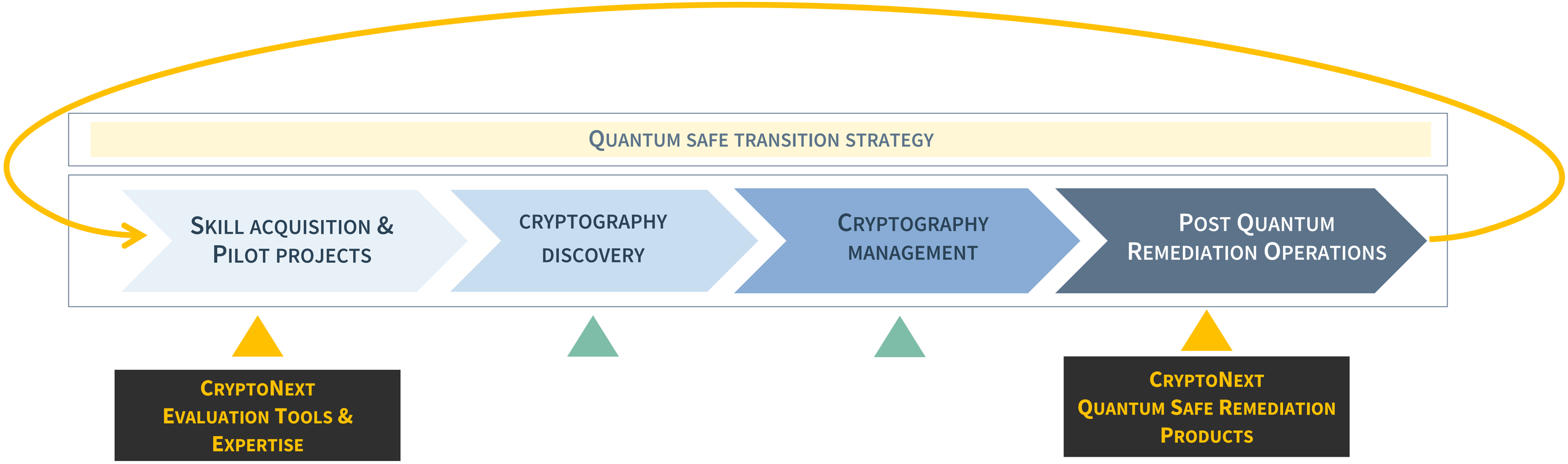
CRYPTONEXT QUANTUM SAFE REMEDIATION: VISION & PLANNING

- All organizations to set up and pilot on-board expertise and prepare for a post quantum transition plan

From Evaluation to Remediation

CryptoNext's End-to-End Global Approach & Tools

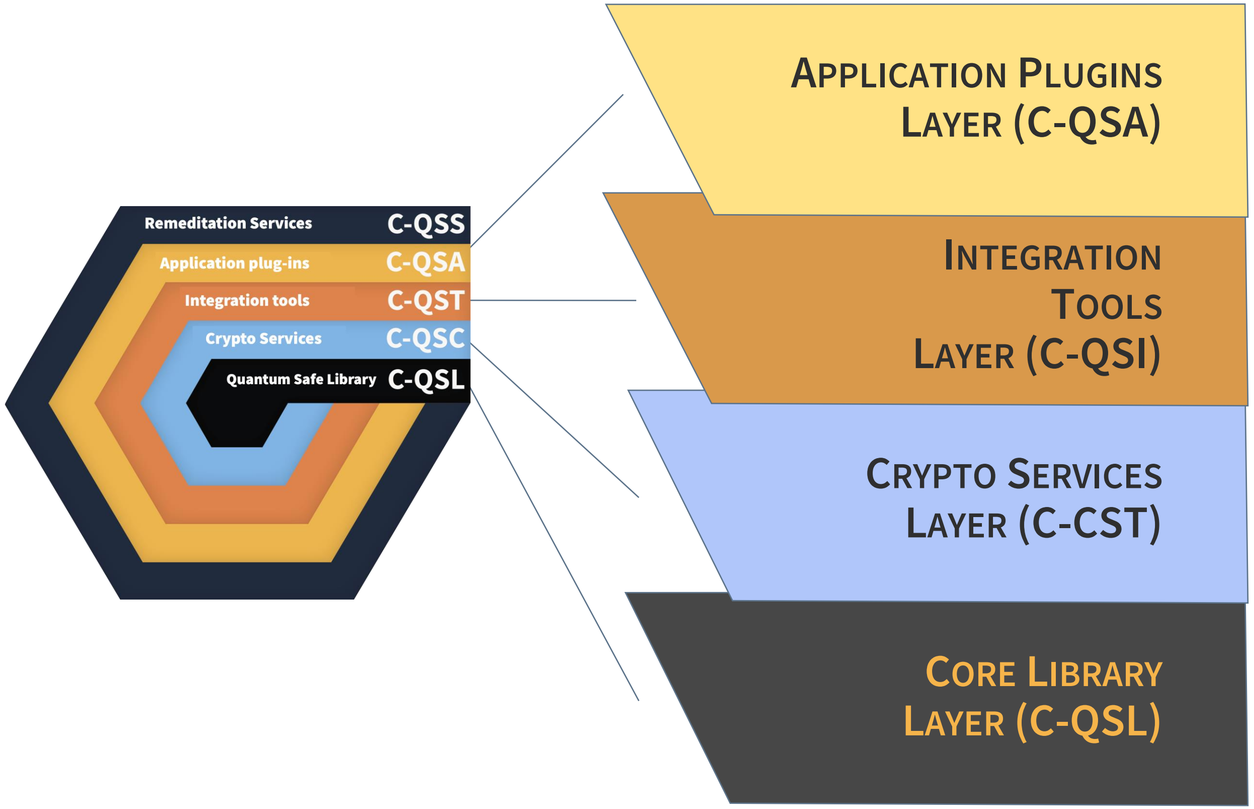
- All organizations will require tools & expertise to manage pilot projects, plan and manage post quantum transition & run operations



CryptoNext Security 's full offering brings remediation technology and know-how at the various stages of migration and operations

A Multi-Layer Bottom-Up Requirement

CryptoNext Quantum Safe Multi-Layer Remediation Suite



PQ Secured Communications, Network Infrastructure and Security Infrastructure Application plugins and connectors (PKI, HSM, Messaging App, Proxy…).

Hybrid PQ Implementations for most common development tools (OpenSSL provider, Java provider…)

Hybrid or Pure Post-Quantum Communication Protocols, Crypto Objects and Programming Interfaces (TLS, IPSEC, X.509, PKCS#11…)

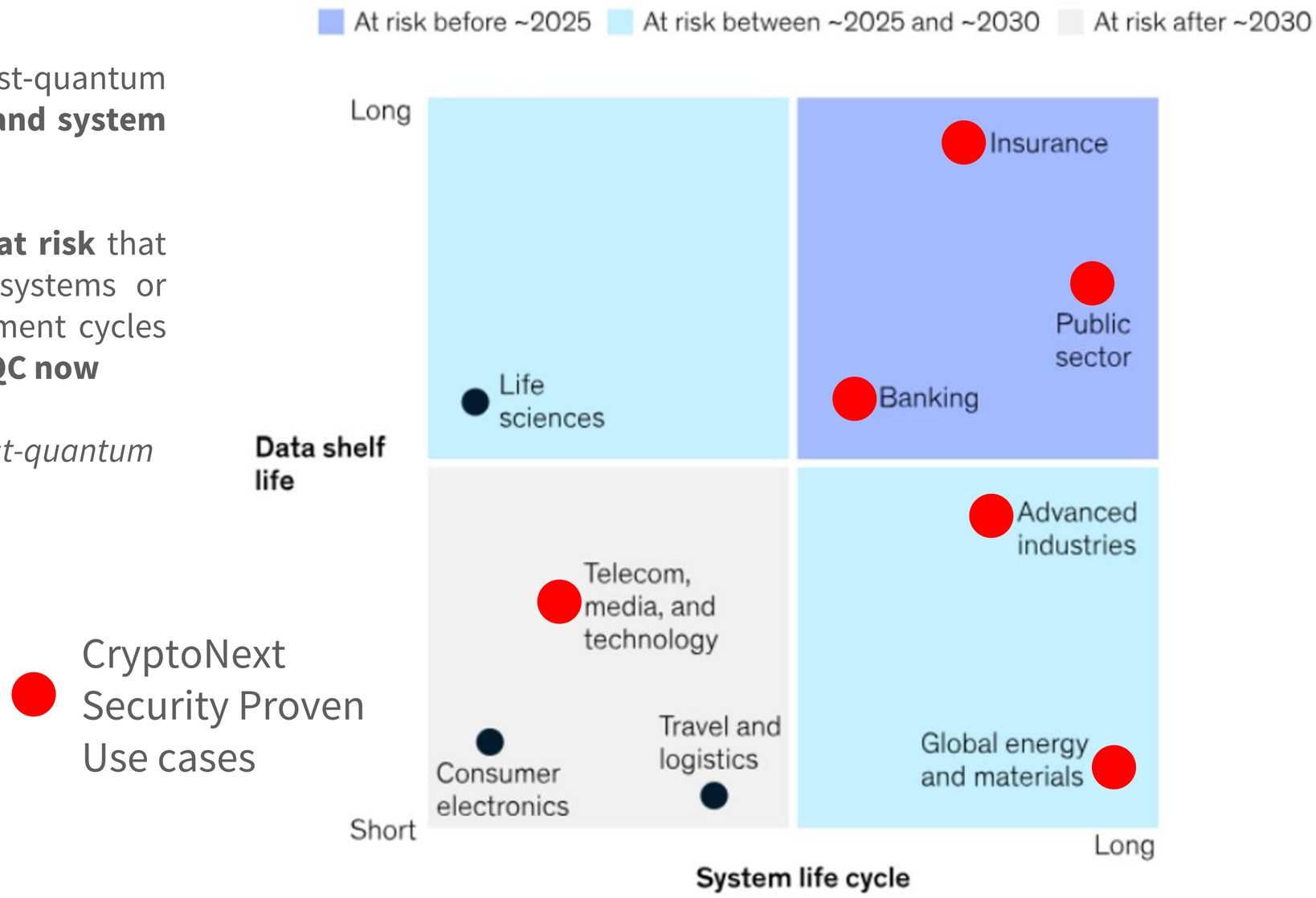
Library of PQ Algorithms (NIST & EU) with full set of language connectors, multiple OS/CPU Platforms and Side-Channels Attacks protection availability (Kyber, Dilithium, FrodoKEM…)

A complete offer and eco-system adapted for various targets of clients: from the OEM & systems integrators to the end customers

TIMELINE BY VERTICAL: RISK OF QYANTUM-POWERED ATTACK BY INDUSTRY

- Industries should prepare for post-quantum cryptography based on **data shelf life and system lifetime**
- **Organizations with substantial value at risk** that have data with long shelf lives and systems or products with potential life or development cycles **should formulate their responses to PQC now**

Mc Kinsey « When and how to prepare for post-quantum cryptography – May 4th, 2022



CryptoNext's Multiple Applications Proven Use Cases

Integrity of digitally signed contracts

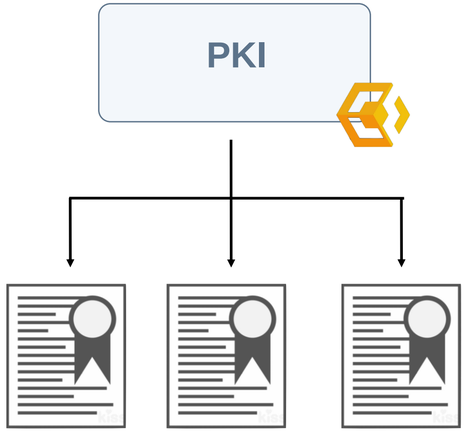
LEADING
EU BANK

Inter-banking communications

BANQUE DE FRANCE EUROSYSTÈME

DEUTSCHE BUNDESBANK EUROSYSTEM

Public Key Infrastructure (PKI)

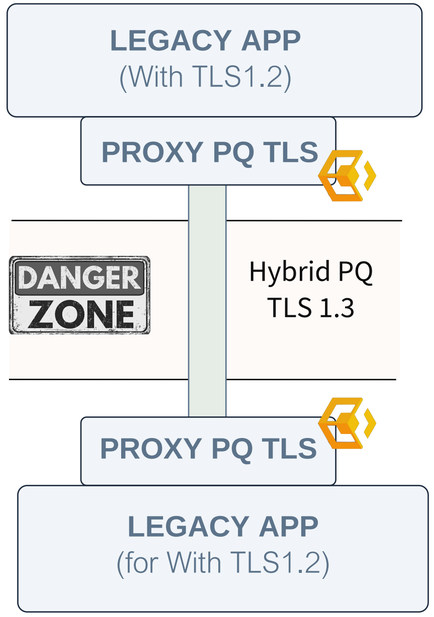


PQ X.509 various PQ format

LEADER
DEFENSE INDUSTRY

LEADING
EU BANK

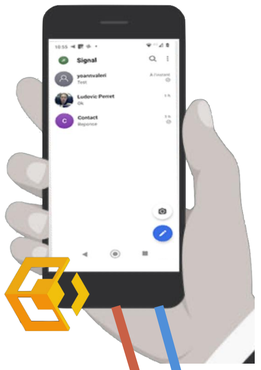
Business Software



FINANCIAL MARKET
INFRASTRUCTURE

CryptoNext Multiple Applications Proven Use Cases

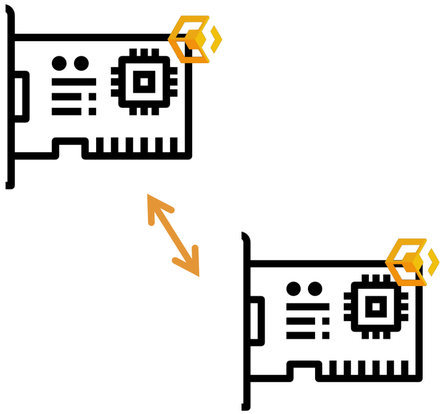
Mobile
Messaging and Com App



Quantum-safe crypto
(KYBER – KEM
DILITHIUM - DSA)

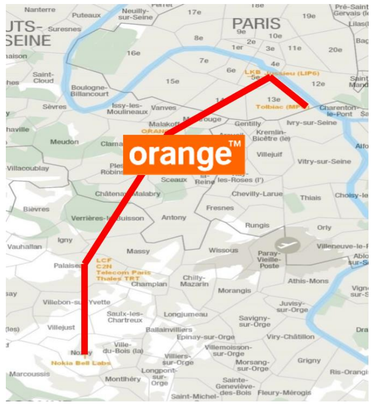
Classical crypto
(RSA - ECC)

Quantum Resistant
IoT & Embedded



mTLS 1.3 between cards
with Arm Cortex M4/R4/M7

PQC - QKD
Integration



Hybridization of PQC - QKD
ParisRegionQCI – FranceQCI - QSNP

NATO OTAN

US PLAYER ENERGY

LEADER IN
DEFENSE INDUSTRY

orange™ THALES AIRBUS

TABLE OF CONTENTS

1 CRYPTONEXT SECURITY: SOCIÉTÉ, HISTOIRE & FILIATION

2 MENACES, TECHNOLOGIE, STANDARDS & SOLUTIONS

3 PLANIFICATION STRATÉGIQUE & APPLICATIONS CLIENTS

4 ENJEUX: INNOVATION, SOUVERAINETÉ & PARTENARIATS

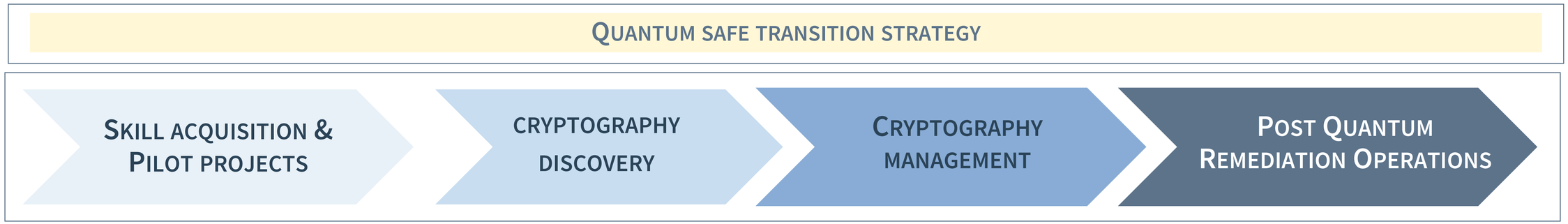
Post-Quantum Remediation
Effective . Simple . Sustainable

CRYPTONEXT SECURITY

POST QUANTUM TRANSITION CALL TO ACTION

All organizations have to set up and pilot a post quantum transition plan

WHERE ARE YOU?



Migration knowledge acquisition & planning

Lessons from our customers: Pragmatic & phased

- Acquiring knowledge about the threat, remediation technologies and management: A need for BdF in order to be able to later build a solid transition plan.
- A progressive and structured strategy for experimentation projects was decided, given the deep and vast complexity in addition of the rapid evolution of tools, standards & certifications:

BdF Internal PQC VPN

Expand to multiple Central Bank partners of the Network

Expand to full PQC enabled application

- Both banking applications (payment, regulatory deposits,…) & IT applications (Email,…)
- Internally & with commercial partners.

PARTENARIAT ACADÉMIQUE/STARTUP = SOUVERAINETÉ LONG-TERME

PQC Migration:
- We are at the beginning - > a large, scalable and agile project over the long term
- It starts now.

Continuous innovation that is sustainable in all areas:
- Technology
- Produce
- Business Model

Technology Partnerships
- Importance of academic relationships over time
- Importance of supporting research efforts

CryptoNext Security
- A major player in French technological sovereignty in security in the quantum era of tomorrow.

CRYPTONEXT SECURITY

Post-Quantum Remediation

Effective . Simple . Sustainable

The new generation of
Quantum Resistant Cryptography

contact@cryptonext-security.com
www.cryptonext-security.com
https://www.linkedin.com/company/cryptonext-security