



Post-Quantum Remediation

Effective . Simple . Sustainable

The new generation of
Quantum Resistant Cryptography

CryptoNext Security Corporate Presentation Quantum Safe Remediation Solutions



May, 2023

TABLE OF CONTENTS

1

ABOUT CRYPTONEXT SECURITY

2

QUANTUM THREAT AND QUANTUM RESISTANT CRYPTOGRAPHY

3

CRYPTONEXT QUANTUM SAFE REMEDIATION SUITE

4

CUSTOMER SOLUTIONS & USE CASES

Post-Quantum Remediation

Effective . Simple . Sustainable




A SUCCESSFUL STARTUP FOCUSED ON POST QUANTUM CRYPTOGRAPHY (PQC) REMEDIATION SOLUTIONS

GARTNER STUDY OCT 2021 - CRYPTO NEXT SECURITY IDENTIFIED AMONG THE TOP5 VENDORS ON POST QUANTUM CRYPTOGRAPHY


Spinoff of INRIA, CNRS, and Sorbonne University, founded in 2019, after 20 years of academic research, **CryptoNext Security** develops « 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)










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



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



Many startup awards



READY INNOVATIVE TECHNOLOGY WITH PROVEN DEPLOYMENTS THROUGH COMMERCIAL PILOTS



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



TABLE OF CONTENTS

1

ABOUT CRYPTONEXT SECURITY

2

QUANTUM THREAT AND QUANTUM RESISTANT CRYPTOGRAPHY

3

CRYPTONEXT QUANTUM SAFE REMEDIATION SUITE

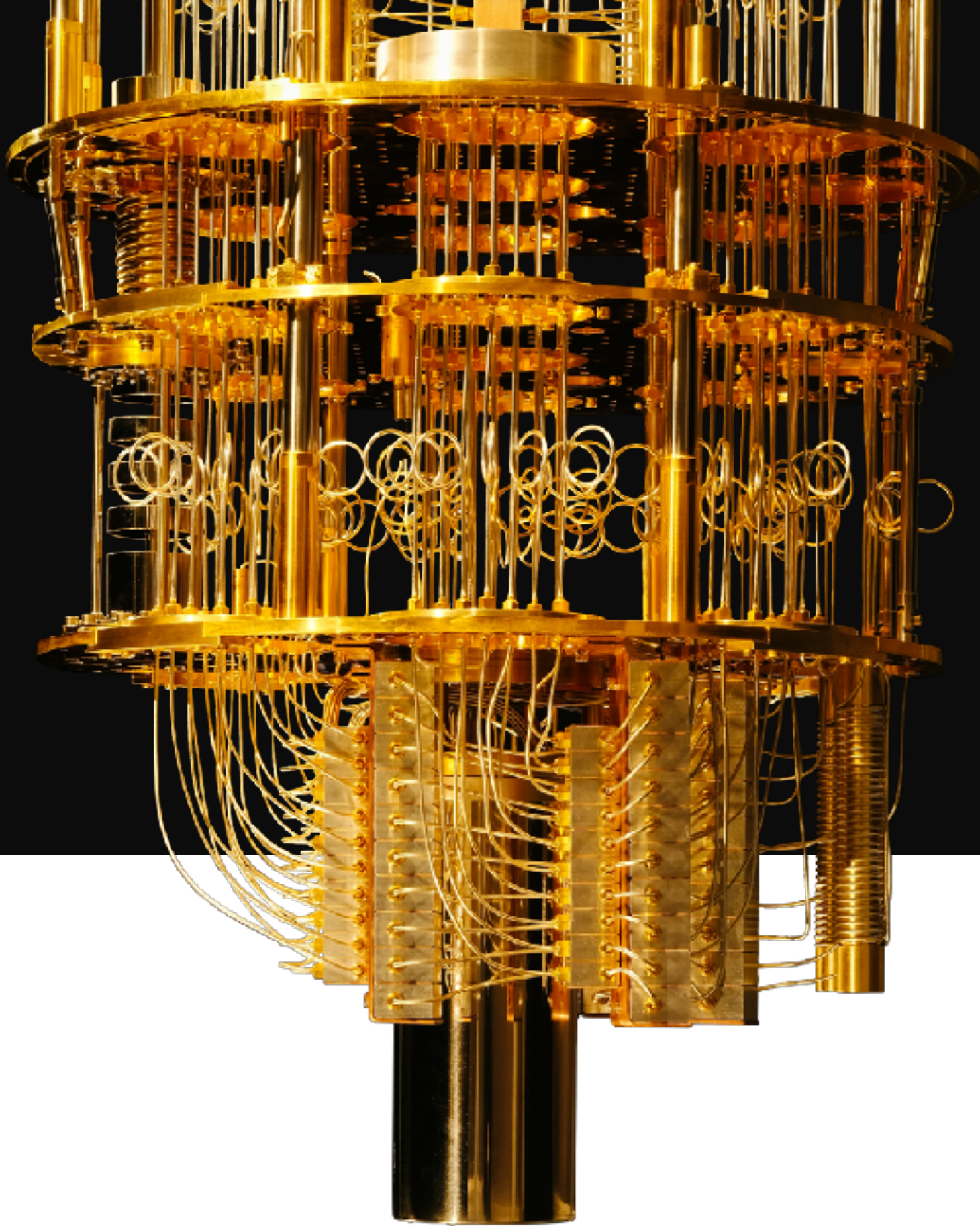
4

CUSTOMER SOLUTIONS & USE CASES

Post-Quantum Remediation



Effective . Simple . Sustainable





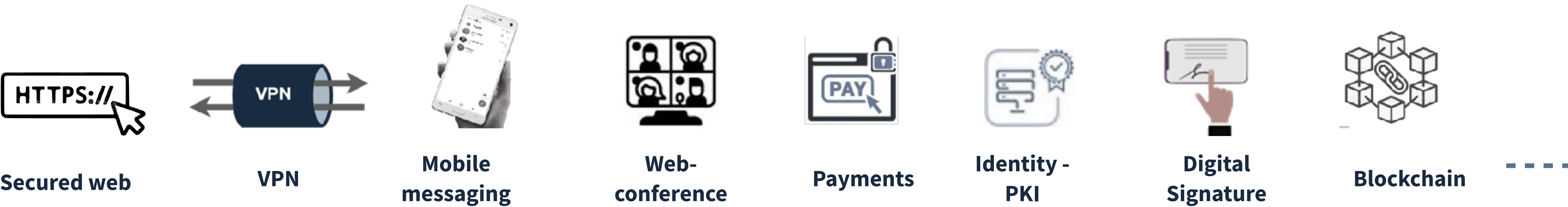
THE QUANTUM THREAT

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.



A TIME BOMB ON CYBERSECURITY

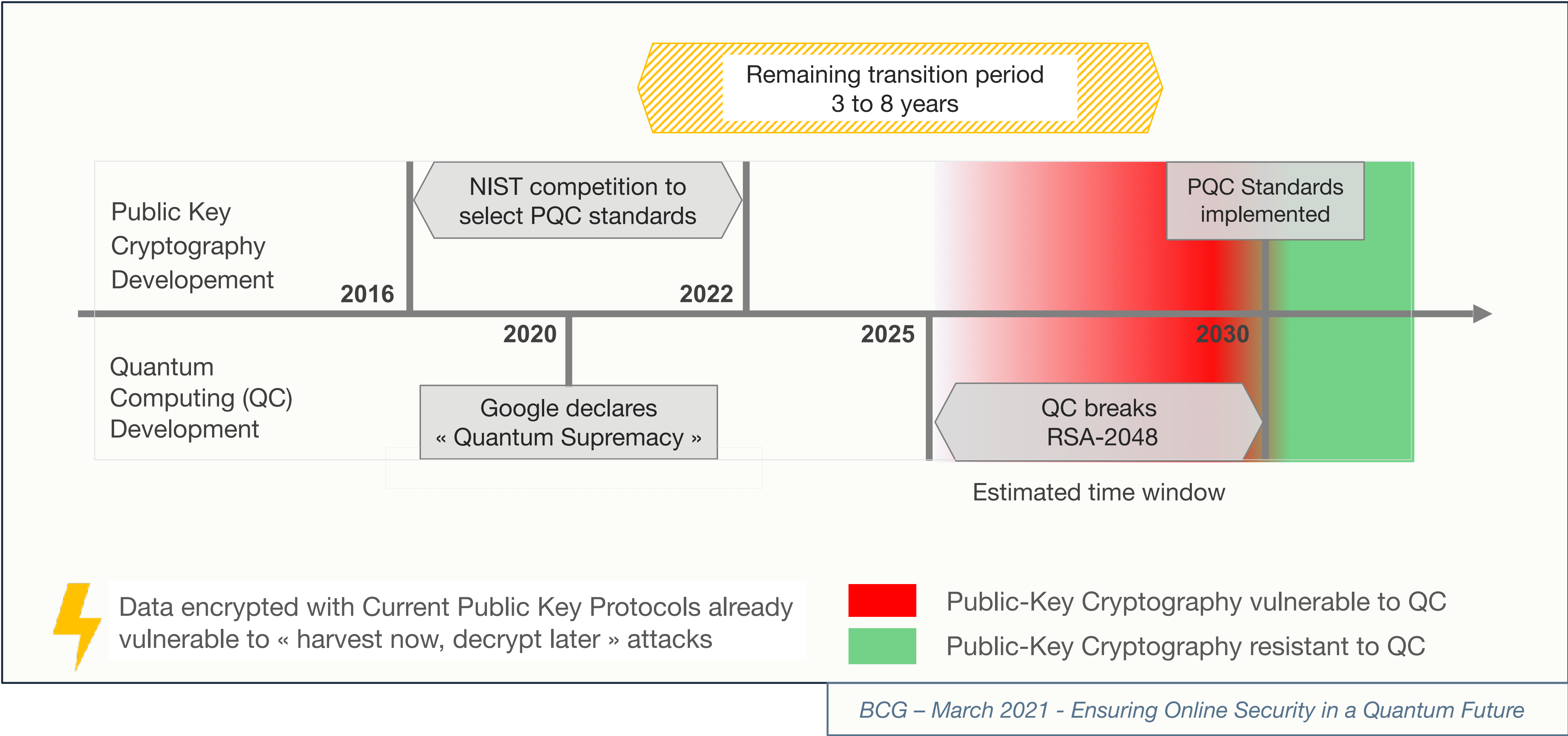
HARVEST NOW, DECRYPT LATER

It is possible for public or private organization to catch and store our communications, in order to decrypt them when an enough powerful computer will be available. Today, the risk is already there, and potentially, **all long term secret data are already impacted by such practise.**



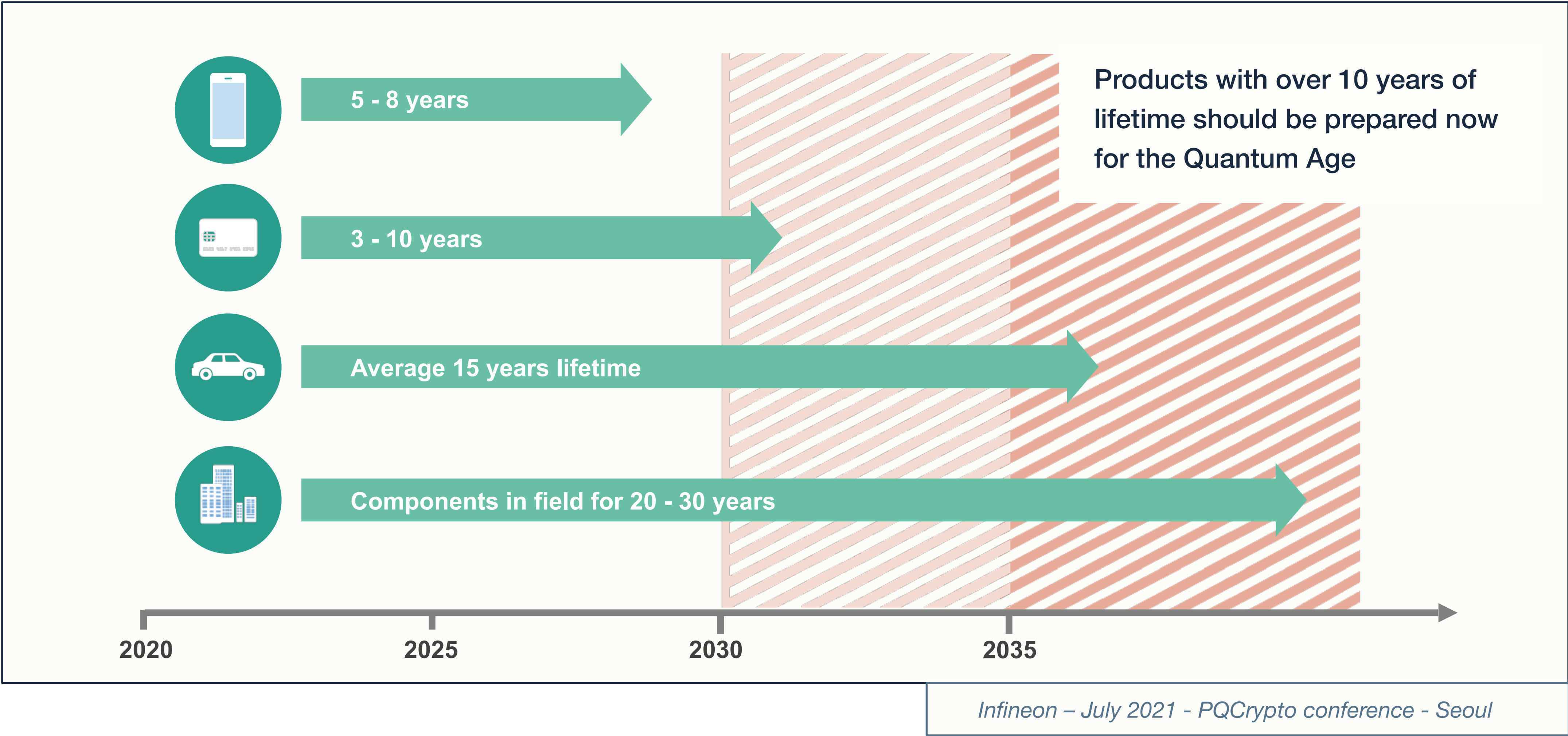
TIME TO CONDUCT TRANSITION PLAN BEFORE Q-DAY IS GETTING SHORTER

According to the forecasted date for Q-Day (date when Quantum Computer will break RSA-2048 keys) in BCG study of march 2021, time window to drive the transition to quantum resistant infrastructure is between 3 to 8 years.



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

The lifetime of the products and the ability to upgrade cryptography after deployment have to be considered to anticipate Q-Day

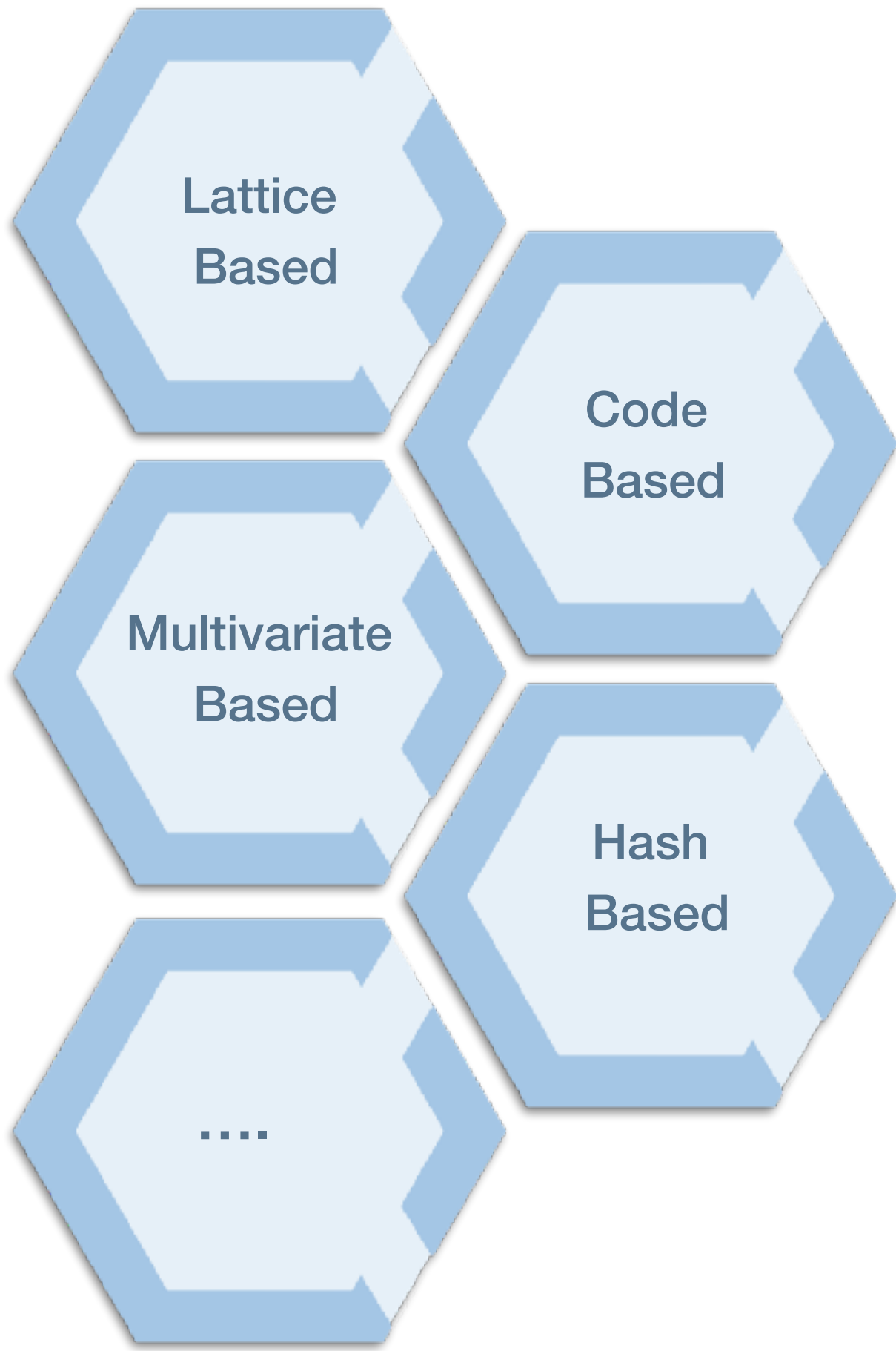


Current public-key cryptographic standards (RSA - ECC) are based on mathematical problems difficult to solve for classical computers but easy to solve for a quantum computer.

➔ New harder quantum-safe mathematical problems have to be find to build a new **quantum resistant cryptography or post quantum cryptography (PQC)**

Example : Multivariate crypto hard problem solving a system of non-linear equations

$$\begin{aligned} p^{(1)}(x_1, \dots, x_n) &= \sum_{i=1}^n \sum_{j=i}^n p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^n p_i^{(1)} \cdot x_i + p_0^{(1)} \\ p^{(2)}(x_1, \dots, x_n) &= \sum_{i=1}^n \sum_{j=i}^n p_{ij}^{(2)} \cdot x_i x_j + \sum_{i=1}^n p_i^{(2)} \cdot x_i + p_0^{(2)} \\ &\vdots \\ p^{(m)}(x_1, \dots, x_n) &= \sum_{i=1}^n \sum_{j=i}^n p_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^n p_i^{(m)} \cdot x_i + p_0^{(m)} \end{aligned}$$



➔ Core and historical **know-how of CryptoNext**

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

NEW STANDARD ALGORITHMS ARE IN DEFINITION IN US, WITH A STRONG STIMULATION FROM THE AUTHORITIES



“Quantum risk is now simply too high and can no longer be ignored”
US NIST, 2016.

➔ ON GOING PROCESS OF NEW QUANTUM RESISTANT CRYPTOGRAPHIC STANDARDS THROUGH NIST



ACCELERATION IN US



➔ WHITE HOUSE MEMORANDUM + NSA RECOMMENDATIONS + NEW BILL

- NSA published on Sept 2021 an **update of security standards for National Security Systems (NSS)**, including PQC.
- Federal agencies have to **check compliance of NSS with new standards, build consistent plan of transition, setup pilots in production** (White House memo of Nov 18 2022)

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

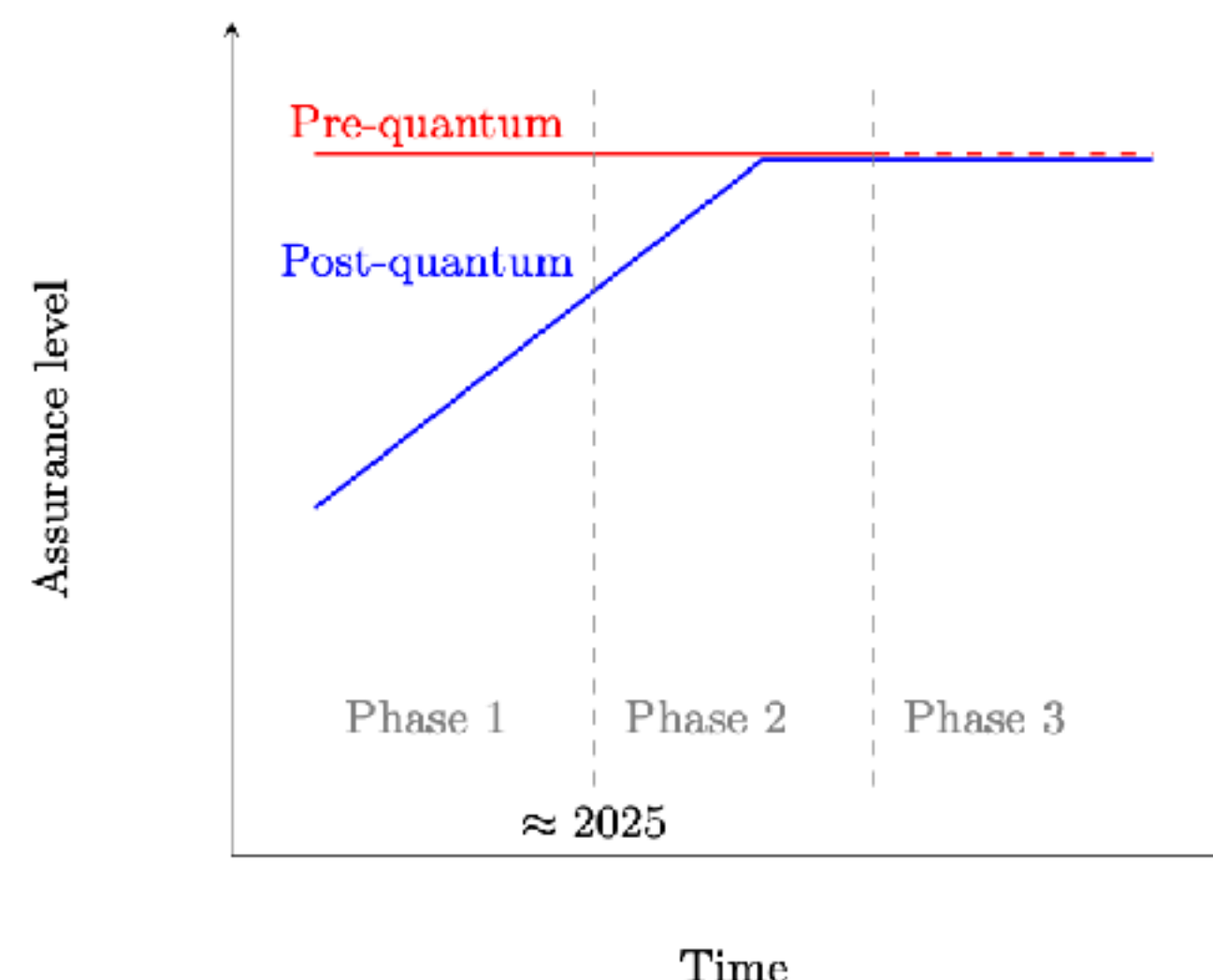
FRANCE'S ANSSI STIMULATES AN ACTIVE TRANSITION « AS SOON AS POSSIBLE »



“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 DEFINES 3 STAGES OF TRANSITION**



PHASE 1 : THE SOONER THE BETTER - INITIALIZE

- Hybrid post quantum cryptography*
- Post quantum cryptography not mandatory

PHASE 2 : LABEL PQ AND MANDATORY IN SOME CASES

- From 2025
- Hybrid post quantum mechanisms
- Certification Label Post Quantum
- Post quantum cryptography mandatory in some cases

PHASE 3 : OPTIONAL HYBRIDATION

- Date not clearly defined, and not before 2030
- Hybrid mechanisms not mandatory
- Pre quantum cryptography not mandatory

* Regarding the choice of PQC algorithms, advice to choose from the NIST finalists, in particular FRODO scheme, no commitment from ANSSI and BSI to follow the final NIST selection.

** In order to specify this overview, French government announced in December 2022 some guidelines (planning and methodology) for the end of Q1 2023.

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).

+ PARTICIPATION TO VARIOUS GROUPS ABOUT PQC, SUCH PQC GROUP OF CAMPUS CYBER IN FRANCE

TABLE OF CONTENTS

1

ABOUT CRYPTONEXT SECURITY

2

QUANTUM THREAT AND QUANTUM RESISTANT CRYPTOGRAPHY

3

CRYPTONEXT QUANTUM SAFE REMEDIATION SUITE

4

CUSTOMER SOLUTIONS & USE CASES

Post-Quantum Remediation

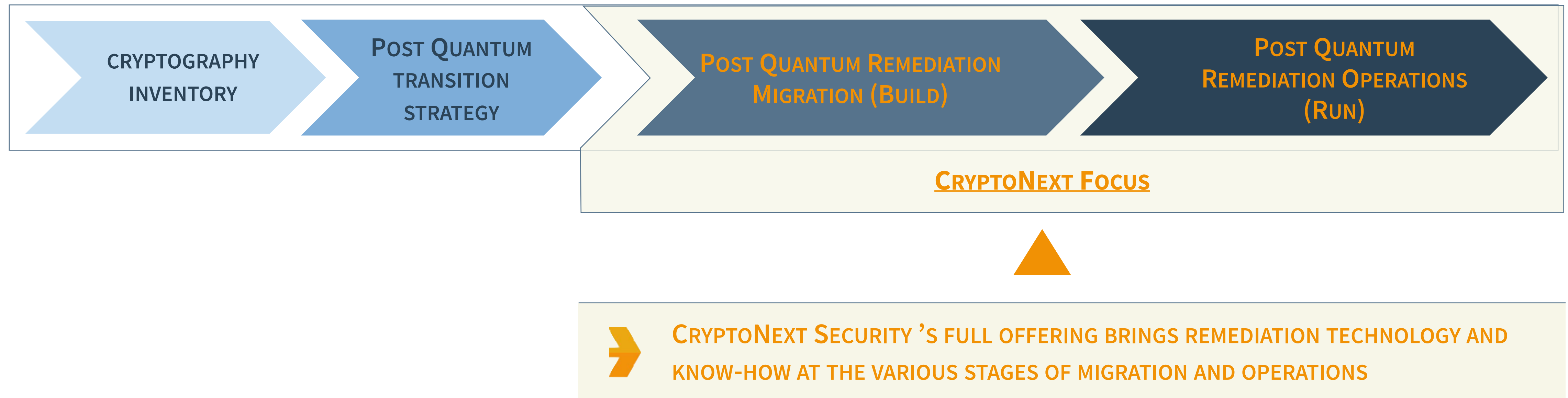
Effective . Simple . Sustainable



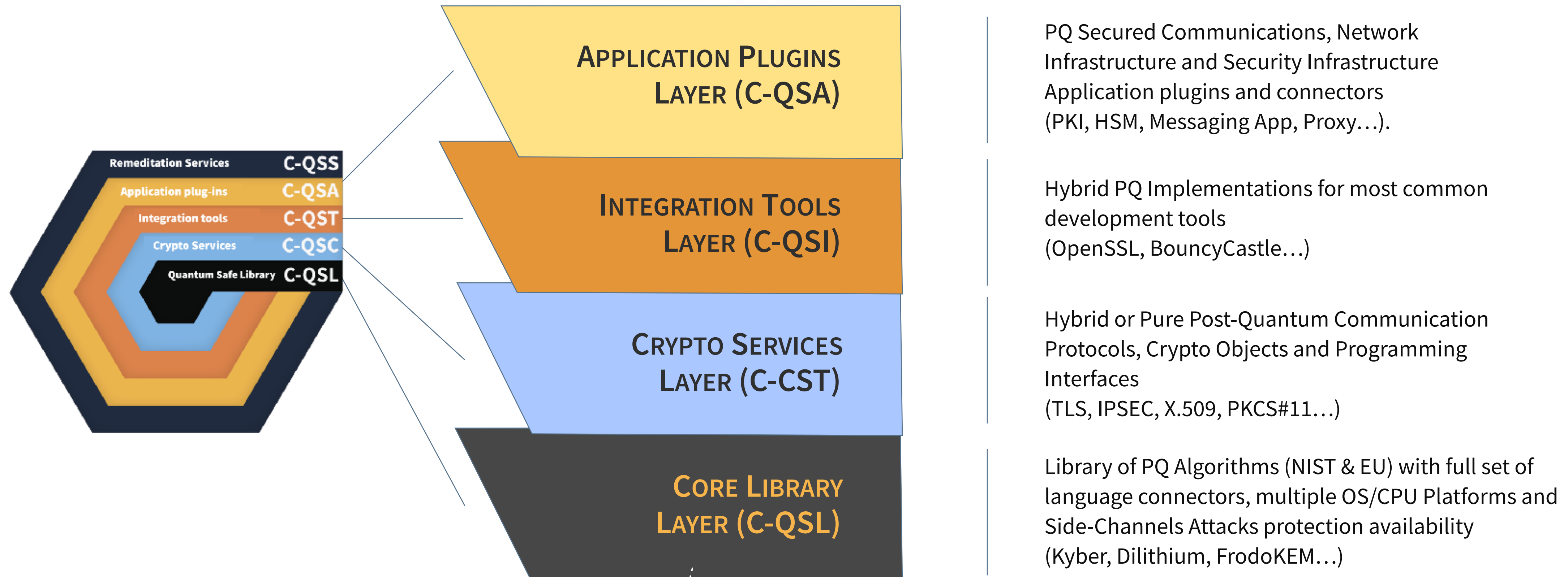
POST QUANTUM TRANSITION PATH

CRYPTONEXT QUANTUM SAFE REMEDIATION

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



CryptoNext Remediation Suite (C-QSR) is an effective, simple and sustainable integrated multi-layer migration solution for applications, data & infrastructure with ultimate PQ security and performance at all levels: algorithms, protocols, tools and applications, with long-term agility and evolution in mind.



A COMPLETE OFFER AND ECO-SYSTEM ADAPTED FOR VARIOUS TARGETS OF CLIENTS: FROM THE OEM & SYSTEMS INTEGRATORS TO THE END CUSTOMERS

SUCCESSFULLY DEPLOYED

TABLE OF CONTENTS

1

ABOUT CRYPTONEXT SECURITY

2

QUANTUM THREAT AND QUANTUM RESISTANT CRYPTOGRAPHY

3

CRYPTONEXT QUANTUM SAFE REMEDIATION SUITE

4

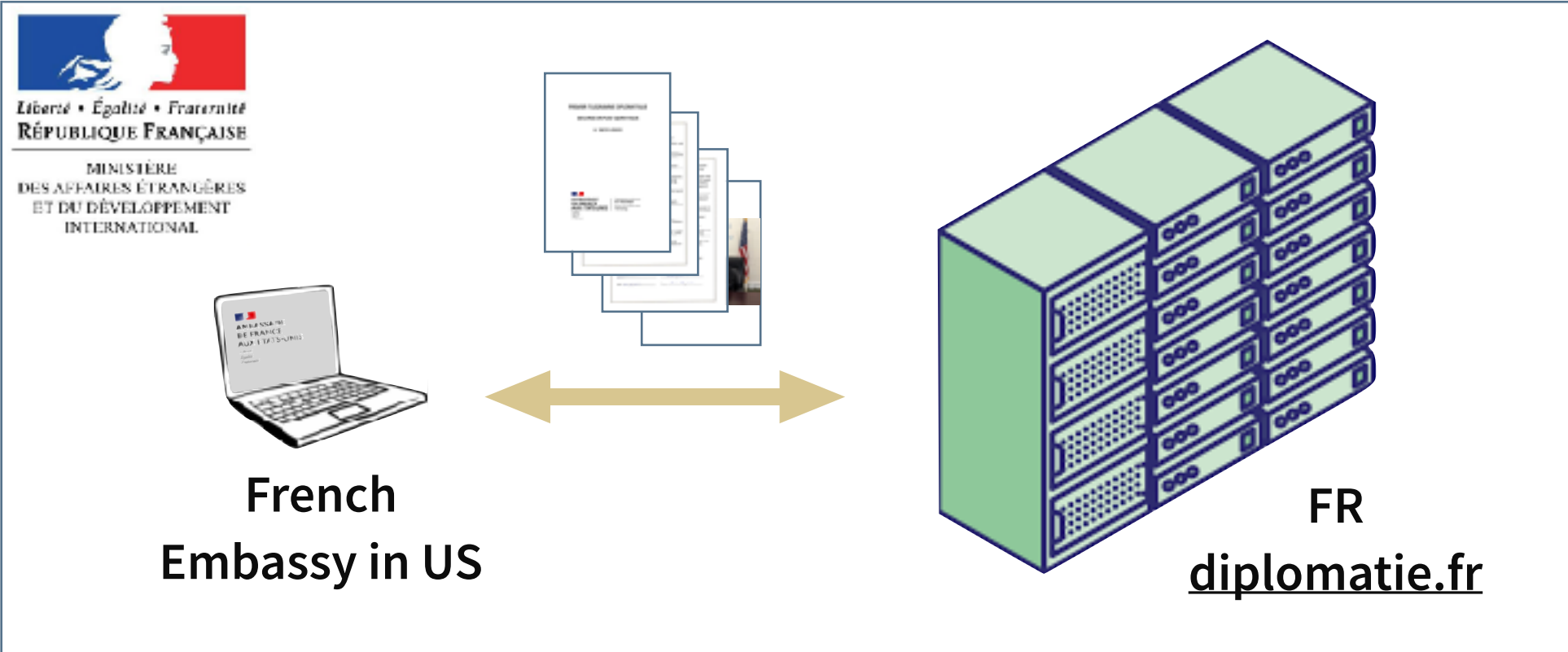
CUSTOMER SOLUTIONS & USE CASES

Post-Quantum Remediation

Effective . Simple . Sustainable



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



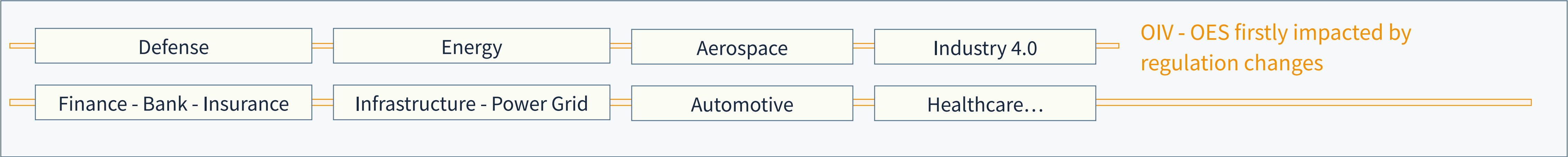
Press release of French Ministry of Foreign Affairs quoting CryptoNext Security technology



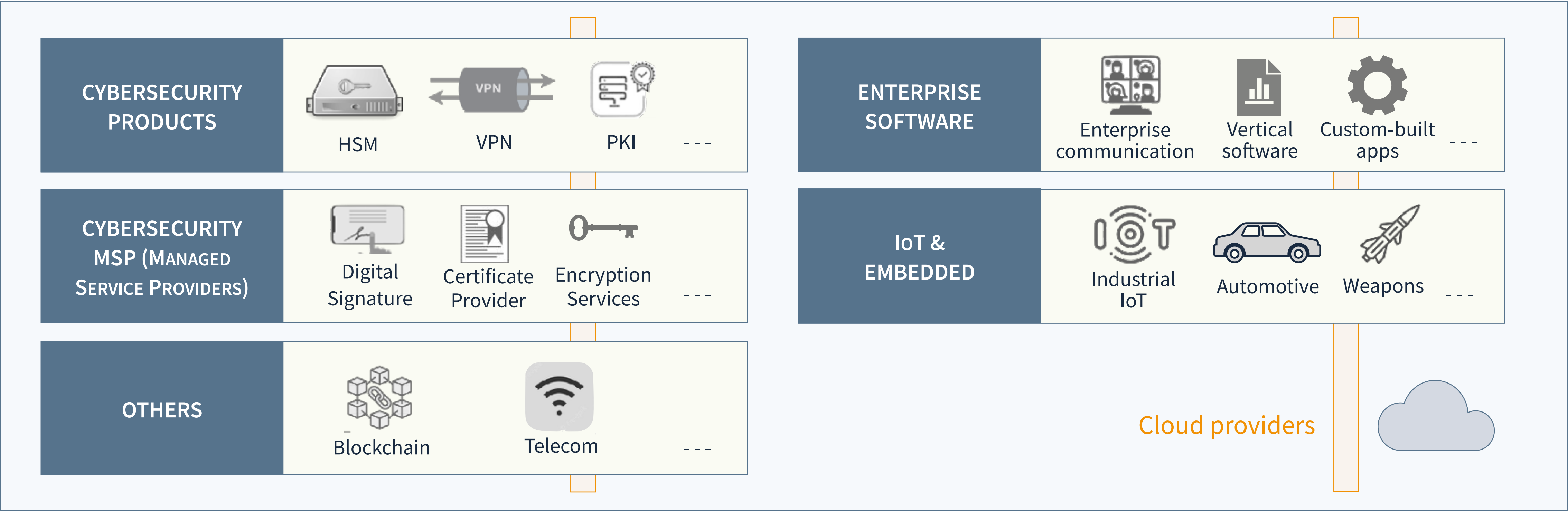
Tweet of President Macron

PRIORITY MARKETS SENSITIVE TO THE QUANTUM THREAT


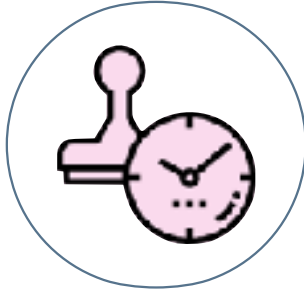


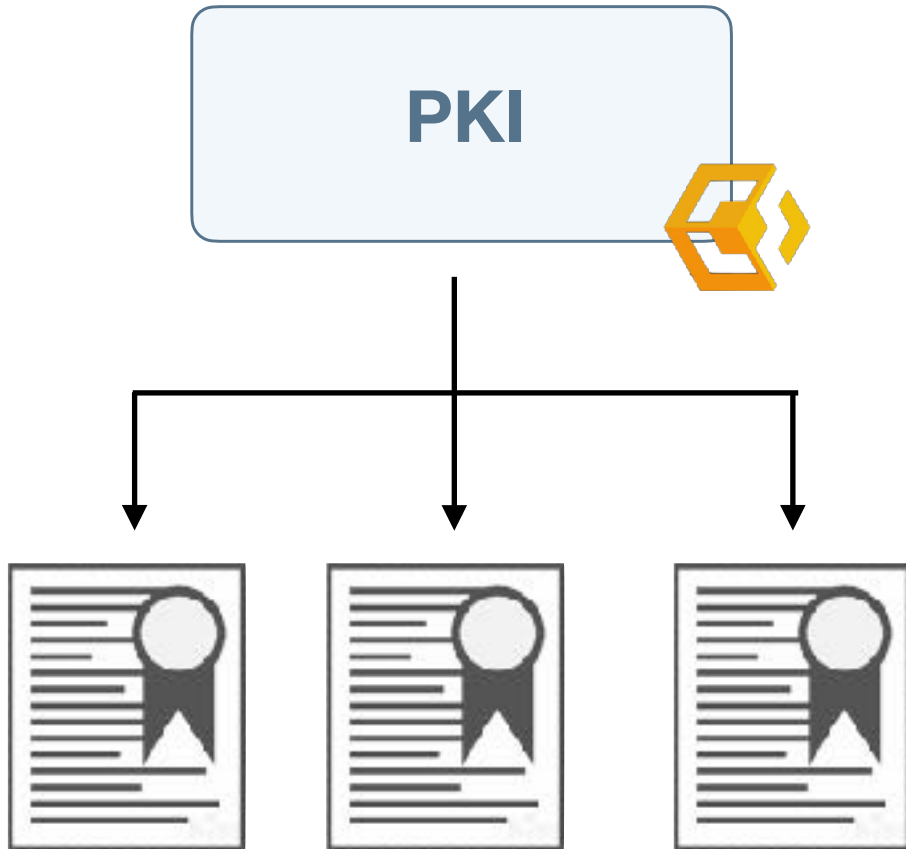



VERTICAL MARKETS



TECHNOLOGIES AND SOLUTIONS MIX

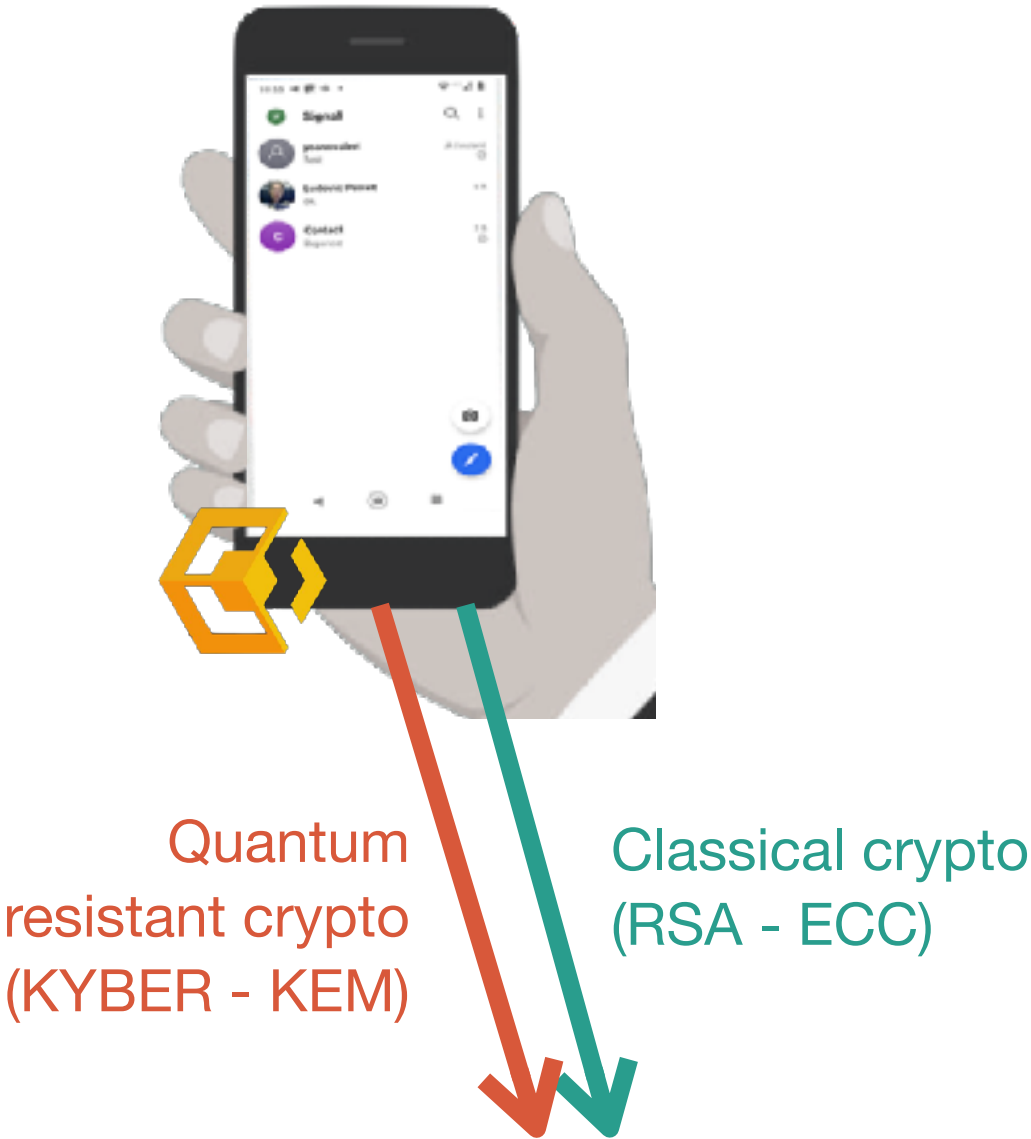


VARIOUS USE CASES AND SUCCESSFUL PILOTS

INTEGRITY OF DIGITALLY SIGNED CONTRACTS	INTER-BANKING COMMUNICATIONS	PUBLIC KEY INFRASTRUCTURE (PKI)	CERTIFICATE PROVIDER
<div><p>DIGITAL SIGNATURE PLAYER</p><p>CRYPTONEXT SECURITY</p></div> <div></div>	<div><p>VPN IPSec</p></div>	<div><p>PKI</p><p>PQ X.509 various PQ format</p></div>	<div><p>CERTIFICATE PROVIDER APP</p><p>HSM PKI</p><p>CRYPTONEXT SECURITY</p></div> <div><p>Backward PQ Certificates</p></div>
LEADING EU BANK	 	LEADER DEFENSE INDUSTRY LEADING EU BANK	LEADING CERTIFICATE PROVIDER

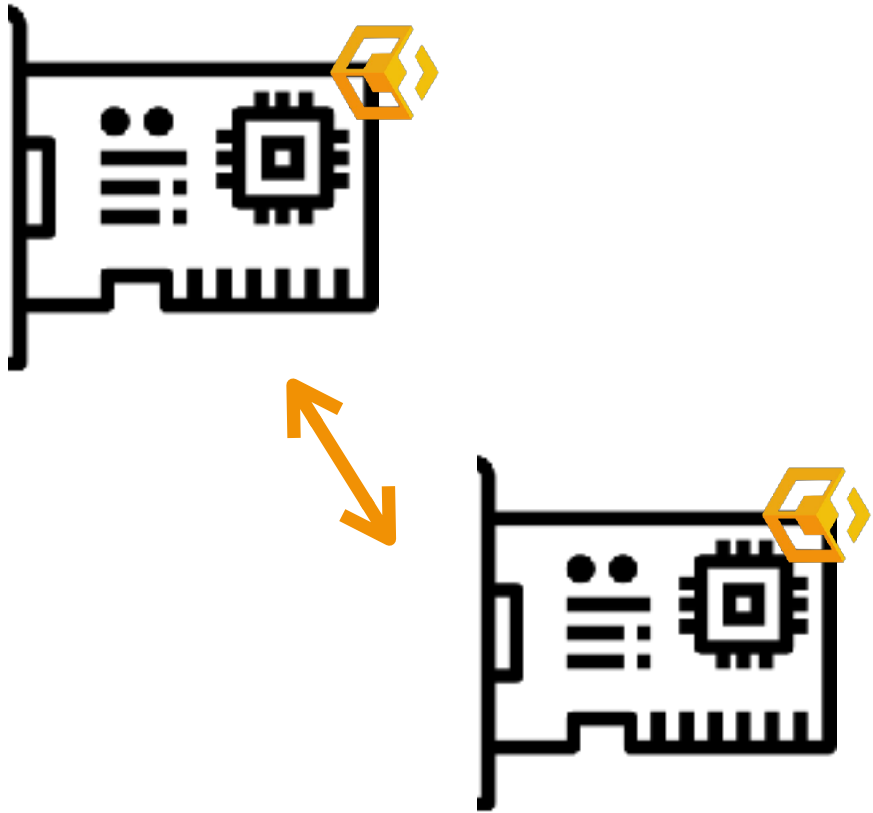
VARIOUS USE CASES AND SUCCESSFUL PILOTS

MOBILE MESSAGING AND COM APP



US PLAYER ENERGY

QUANTUM RESISTANT IoT & EMBEDDED



PQ Key Exchange between cards with Arm Cortex M4

LEADER IN
DEFENSE INDUSTRY




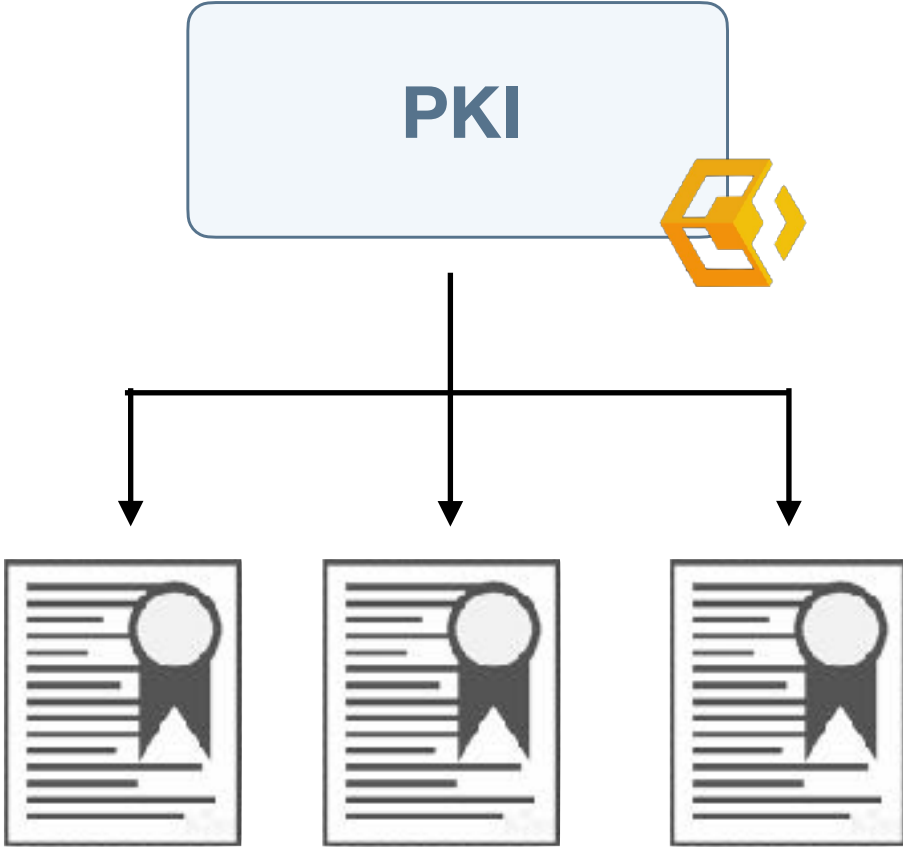
PQC - QKD INTEGRATION



Hybridization of PQC - QKD
ParisRegionQCI - EuroQCI



TECHNICAL PARTNERS (ALLIANCE, OEM)

QUANTUM RESISTANT HSM	QUANTUM RESISTANT HSM	QUANTUM RESISTANT VPN (CLIENT)	QUANTUM RESISTANT PKI
 <p>Available Post Quantum FM (Functionality Module) on HSM Thales Luna 7</p>	 <p>Post Quantum Option On HSM Atos Proteccio</p>		 <p>PQ X.509 various PQ format</p>
THALES	EVIDEN an atos businessAtos	THEGREENBOW	EVERTRUST Digital. Trust. Ever. ...



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>

