Post-Quantum Cryptography:
Status & financial industry updates

December 8th, 2025

ENISA webinar
Engineering Data Protection in the wake of PQC

Dr Maria CHRISTOFI
BNPP Cryptography expert
Member of ENISA Advisory Group

EVOLUTION

IT GROUP

70s — Micro-processors

- First micro-processor developed containing 2300 transistors and operating at a frequency of 740 kHz.
- Micro-processors capacities goes from 8-bit to 16-bit.
- Computers go from room-sized systems to desktop models.
- Memory rarely exceeded 64 Kb.
- By 1975, the first PCs go out to the market
- By the end of the decade, the cost of microchips dropped by 90%, paving the way for mass production.

80s — Personal computers

- Personal computers become accessible to everyone with 50 million units in use by 1989.
  - Even if PC exist since 60s-70s
- Processors reached speeds of up to 25 MHz and RAM expanded to 1 MB.
- Micro-processors capacities goes from 16-bit to 32-bit.
- Graphical interfaces replaced text-based commands.
- In 1983, the first portable computers weighting up to 10 kg were introduced.
- By the end of 1980s, the software market exceeded $15 billions.

90s — Internet

- In 1991, the World Wide Web arrived.
- Internet users went from 26 millions in 1995 to 400 millions in 2000. And to 1,5 billions in 2010.
- Processors surpassed 1 GHz and hard drives reached 10 Gb
- Laptops weighted less than 3 kg.
- By 1999, 35% of homes in developed countries had a PC.

00s — Digital era

- Internet users reached 1,5 billions in 2010.
- Multi-core processors arrived, and hard drives reached 1 Tb.
- Smartphones & tablets began competing PCs.

AI & quantum

- AI processes exabytes of data (1Eb=1 billion Gb).
- Quantum computers reached 1000 qubits (by 2023).
- Cloud services store 60% of the word's data.

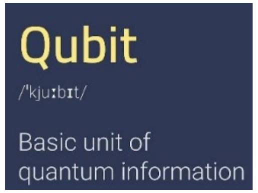
SOME DEFINITIONS…

IT GROUP

A technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers.

The basic information unit in quantum computation and communication.

It is equivalent of a binary bit in classical computation.



Physical qubit

- A qubit physically realized on a computer.
- Physical qubits are prone to errors.

Logical qubit

- A group of physical qubits used as a single qubit in a computation.
- Logical qubits are encoded into multiple physical qubits so that errors affecting the underlying physical qubits can be detected and corrected, and logical information be protected.

A set of techniques expected to be secure against a quantum computer. Based in (very difficult) mathematical problems.

Software-based solutions for digital signature and encryption.

Use of properties of quantum mechanics to fulfill cryptographic tasks. Need of specialized software.

Examples: QKD, QRNG

DOES IT AFFECT ALL MY CRYPTOGRAPHY?

Symmetric cryptography

- 1 unique key for encryption and decryption
- Examples: AES

Use cases

- Encryption for data at rest or in transit
- Key wrapping

Asymmetric cryptography

- A pair of keys
- Based on mathematical problems: one-way functions, such as prime numbers factorization or discrete logarithm problems
- Examples: RSA, ECDSA, DH

Use cases

- Establishing an encrypted communication channel
- Authentication
- Signature

DOES IT AFFECT ALL MY CRYPTOGRAPHY?

Symmetric cryptography

- 1 unique key for encryption and decryption
- Examples: AES

Vulnerable to Grover algorithm

Mitigation: Doubling lengths

Use cases

- Encryption for data at rest or in transit
- Key wrapping

Asymmetric cryptography

- A pair of keys
- Based on mathematical problems: one-way functions, such as prime numbers factorization or discrete logarithm problems
- Examples: RSA, ECDSA, DH

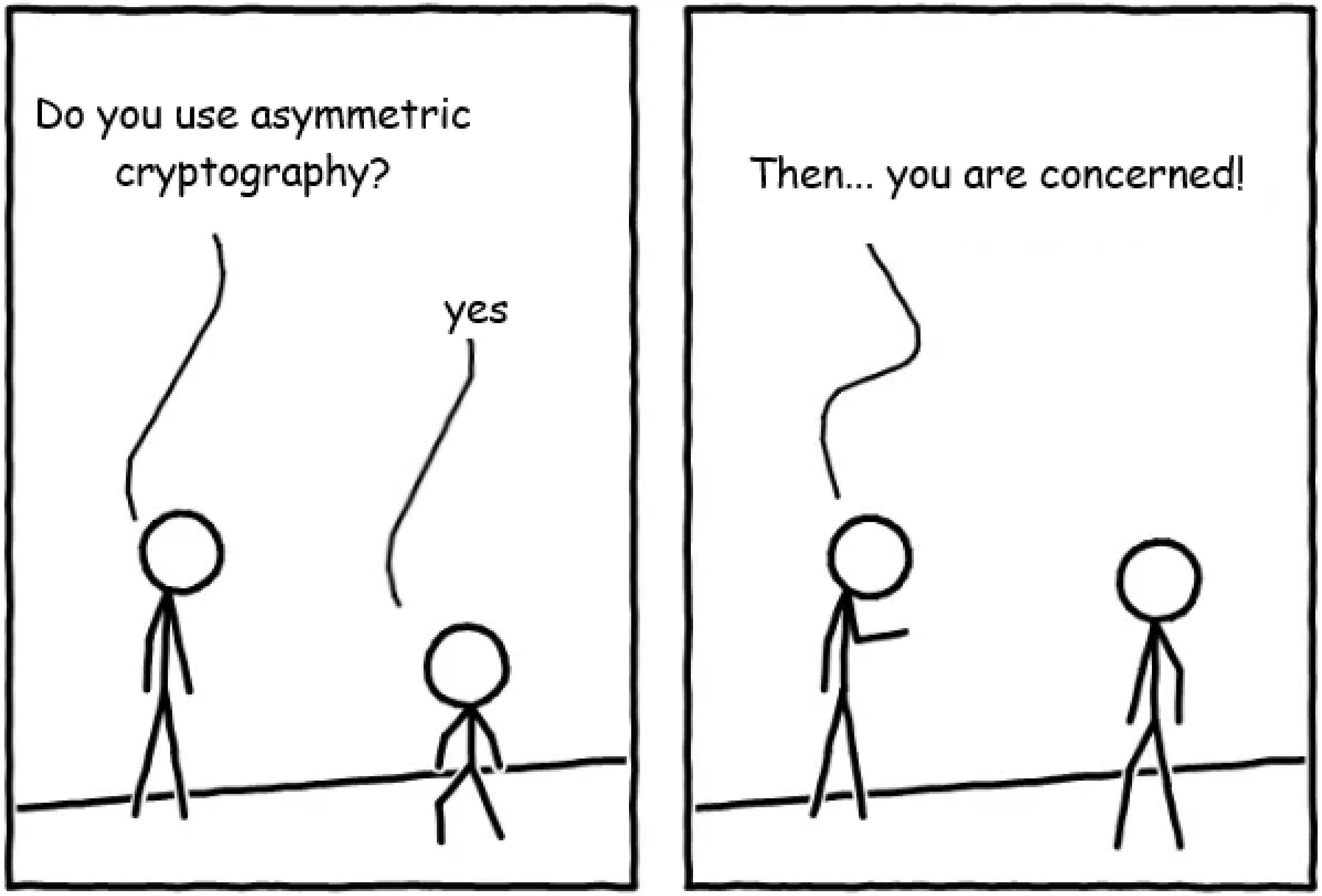
Vulnerable to Shor algorithm

Mitigation: Unknown → Replacement by quantum-safe algorithms

Use cases

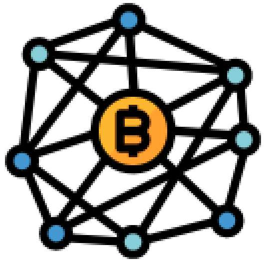
- Establishing an encrypted communication channel
- Authentication
- Signature

DOES IT AFFECT ALL MY CRYPTOGRAPHY?

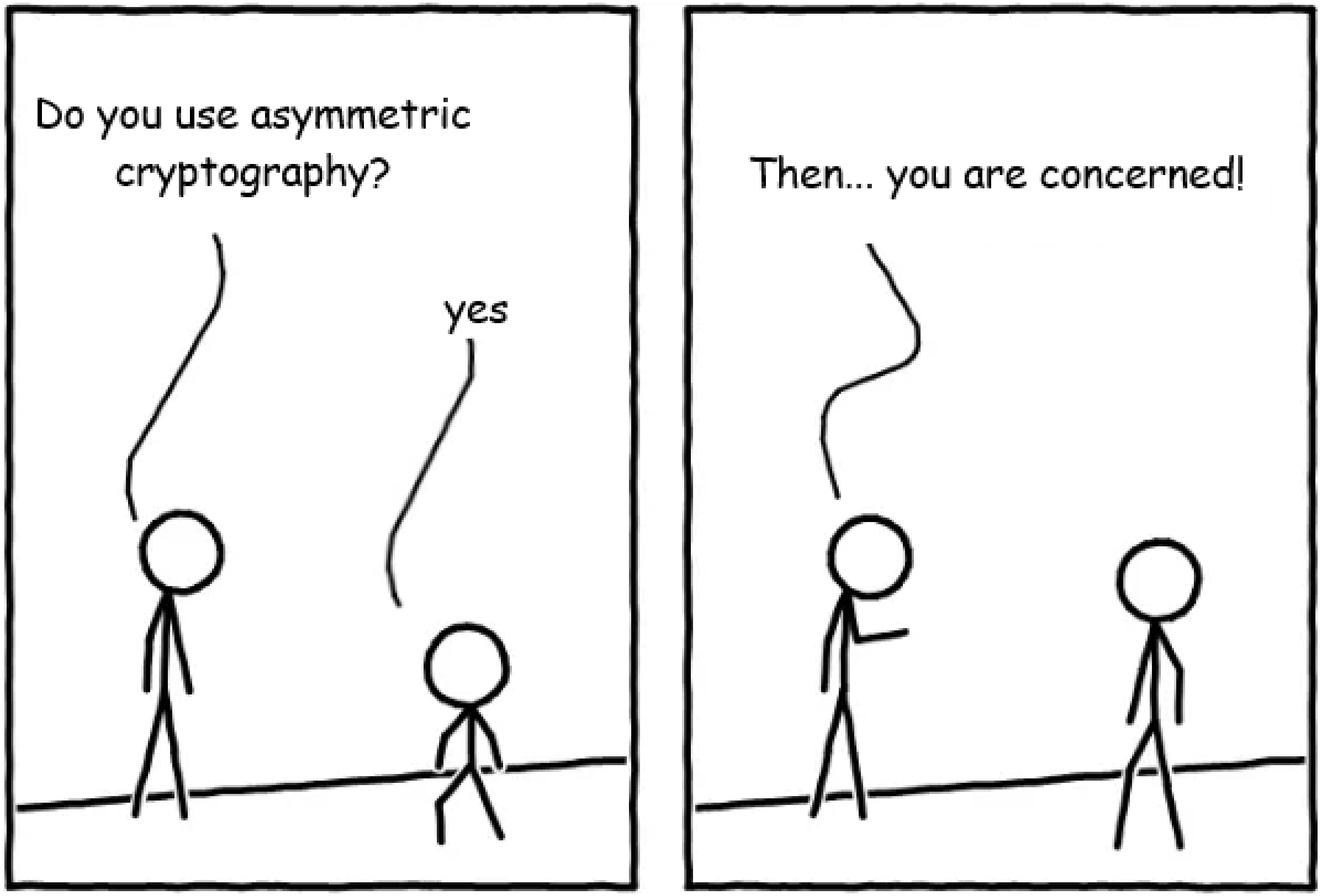


DOES IT AFFECT ALL MY CRYPTOGRAPHY?

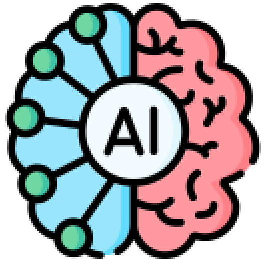
Sensitive data collection & decryption



Blockchain attacks (e.g. on the wallet authentication)

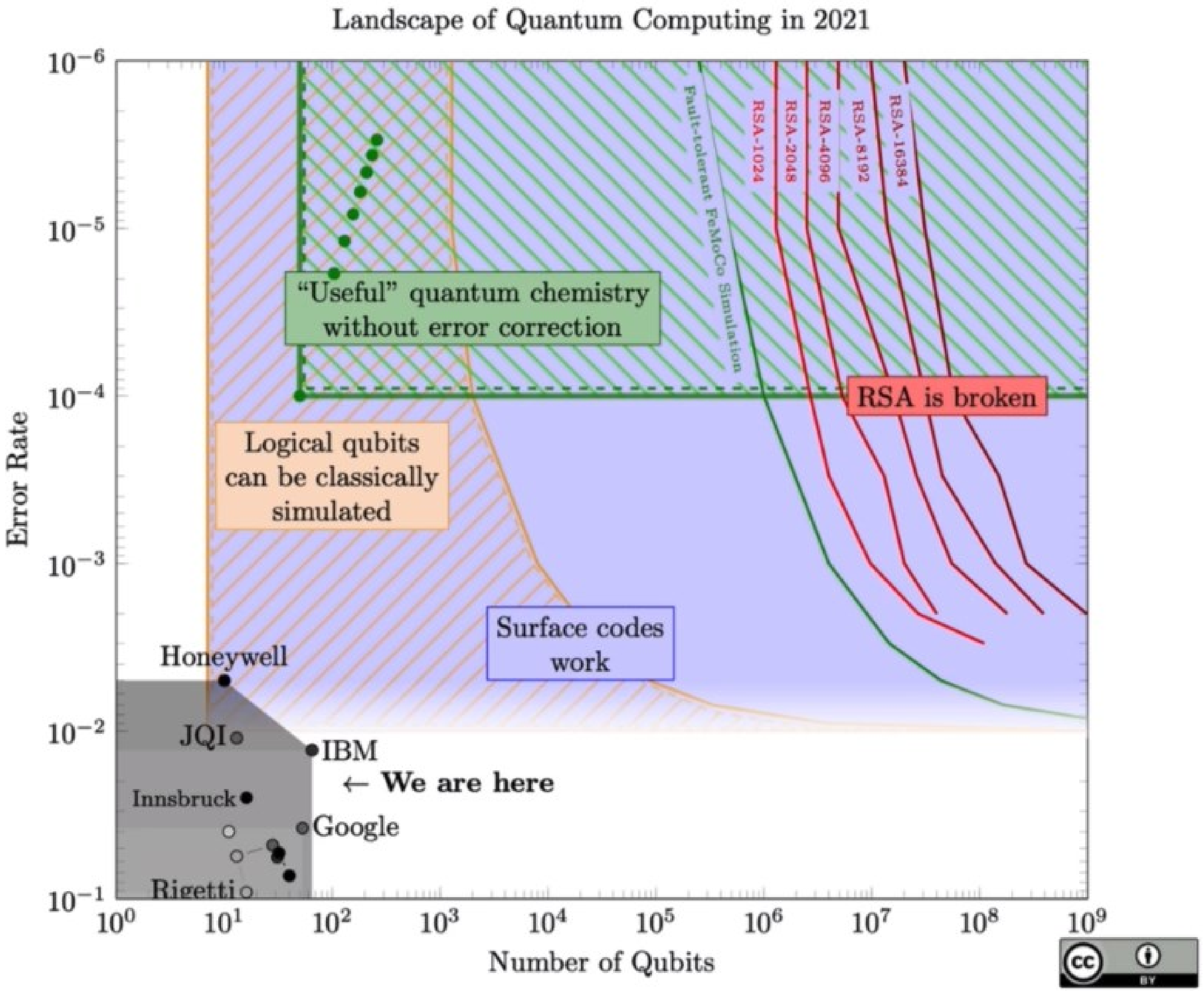


Digital signature manipulation



AI combined to quantum

WHERE ARE WE TODAY?



As for today no efficient methods to break current cryptography using quantum computers is found....

Source: Quantum Landscape

SO…SHOULD WE ACT NOW?

Watch & prepare

- Follow technological & strategical watch
- Prepare old systems for the change
- Be sure new systems include PQC (either through crypto-agility or PQC readiness)
- Challenge current & new providers to ensure that they align internal strategy

Identify impact

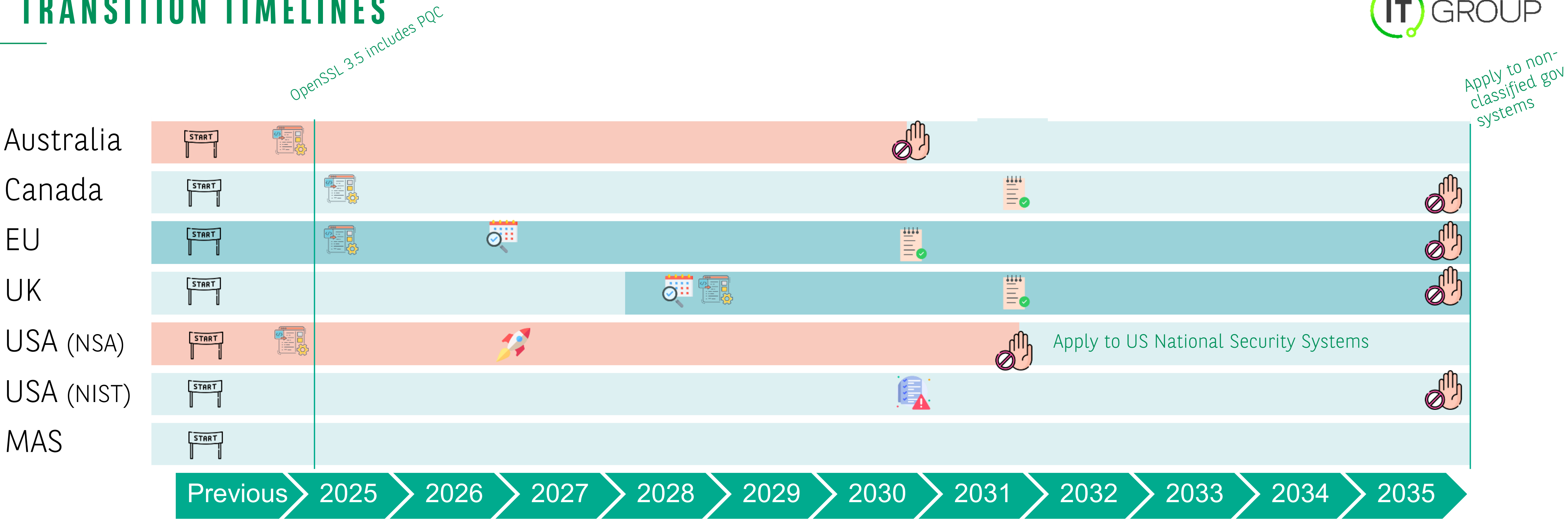
- Identify vulnerable protocols & their usage
- Identify vulnerable data
- Prioritize migration depending on data sensitivity
- Discuss migration to quantum-safe solutions with suppliers

Adopt quantum solutions

- Implement solutions that are not yet mature can be dangerous!
- Whenever quantum-proof solutions are approved by the experts (in terms of security & performances):
  - Switch to quantum-proof protocols
  - Switch to quantum-based encryption & signature mechanisms when necessary

What are the agencies thinking about migration?

TRANSITION TIMELINES



Recommandations and guidelines

Policies and guidelines

Planning activities
- Start planning activities
- Complete planning activities

Implementation activities
- Start implementation activities
- New deployment must use PQC
- Complete the migration on most sensible use cases
- Stop using pre-quantum cryptography
- Use of deprecated algorithms according to a risk assessment

NIST(*)

IT GROUP

Proposed migration planning

NIST
National Institute of Standards and Technology

1. Identify standards & consortium
2. Identify critical applications & protocols
3. Determine use characteristics of the public-key cryptography implemented
4. Identify interoperability issues and information sensitivity
5. Consider user/customer requirements
6. Identify appropriate algorithms among the standardized ones

Sources:
[Getting ready for post-quantum cryptography](#) (2021)
[Migration to post-quantum cryptography – draft](#) (2023)

(*) NIST (National Institut of Standards and Technology) is a USA national agency whose aim is to promote American innovation and industrial competitiveness by advancing measurement science, standards, and technology.

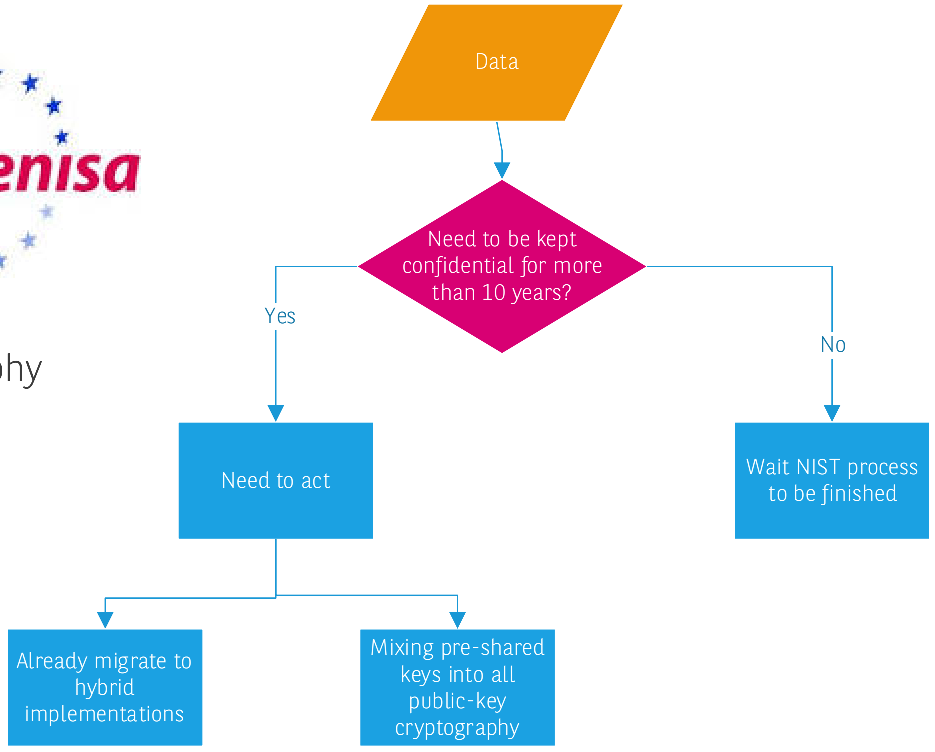
NIST: ANNOUNCED COLLABORATORS FOR THE MIGRATION

Source: Collaborators list by NIST

ENISA(*)

- [1] provides description of each family being part of NIST candidates
  - For each algorithm (encryption and signature) participating in the NIST contest (round 3), the following are presented
    - Design of the algorithm
    - References for the existed implementations
    - A short cryptanalysis with the corresponding references
    - Advantages and disadvantages of the algorithm
  - Quantum mitigation: two options are proposed (and developed)
    - Already migrate to hybrid implementation
    - Mixing pre-shared keys into all key established via public-key cryptography

- [2] provides a study on integrating post-quantum systems into existing protocols



Proposed workflow for migration

Sources:
[1] Post-quantum cryptography: current state and quantum mitigation (2021)
[2] Post-quantum cryptography: Integration study (2022)
[3] Post-quantum cryptography: anticipating threats and preparing the future (2022)

(*)ENISA (European Network and Information Security Agency) is the European union agency for Cybersecurity dedicated to achieving a high common level of cybersecurity across Europe.

EU JOINT COMMUNICATION

- Joint statement from 18 EU members about the quantum threat

- Call to all industry to make the transition to post-quantum cryptography a top priority to be ready latest by the end of 2030!

- EU proposed roadmap for the transition

Perform a **quantum threat analysis** consisting of an inventory of the assets they need to protect as well as the applications that use cryptography

Develop a **risk-oriented roadmap** for executing the transition (considering sensitivity, data protection period, crypto-agility)

Plan the **migration** (including prioritisation, budget, business processes)

Promote the continuation of the extensive **research** on PQC & **standardisation**

Sources:

[BSI - Quantentechnologien und quantensichere Kryptografie - Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography]() (2024)

[A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography | Shaping Europe's digital future]() (2025)

Focus on financial industry...

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Protocols and encryption strengths may quickly change or be deprecated due to identification of vulnerabilities or design flaws. In order to support current and future data security needs, entities need to know where cryptography is used and understand how they would be able to respond rapidly to changes impacting the strength of their cryptographic implementations. **Good Practice** Cryptographic agility is important to ensure an alternative to the original encryption method or cryptographic primitive is available, with plans to upgrade to the alternative without significant change to system infrastructure. For example, if the entity is aware of when protocols or algorithms will be deprecated by standards bodies, proactive plans will help the entity to upgrade before the deprecation is impactful to operations. **Definitions** "Cryptographic agility" refers to the ability to monitor and manage the encryption and related verification technologies deployed across an organization. **Further Information** Refer to *NIST SP 800-131a, Transitioning the Use of Cryptographic Algorithms and Key Lengths*.
12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • Documentation of a plan, to respond to anticipated changes in cryptographic vulnerabilities.	**12.3.3** Examine documentation for cryptographic suites and protocols in use and interview personnel to verify the documentation and review is in accordance with all elements specified in this requirement.	
Customized Approach Objective		
The entity is able to respond quickly to any vulnerabilities in cryptographic protocols or algorithms, where those vulnerabilities affect protection of cardholder data.		
Applicability Notes		
The requirement applies to all cryptographic cipher suites and protocols used to meet PCI DSS requirements, including, but not limited to, those used to render PAN unreadable in storage and transmission, to protect passwords, and as part of authenticating access. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0.1 *June 2024*
 Page 299

- Up-to-date inventory of all cryptographic cipher suites and protocols in use
- Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites & protocols in use
- A documented strategy to respond to anticipated changes in cryptographic vulnerabilities

IT GROUP

SECTION IV

ENCRYPTION AND CRYPTOGRAPHY

Article 6

Encryption and cryptographic controls

4. Financial entities shall include in the policy on encryption and cryptographic controls provisions to, where necessary, on the basis of developments in cryptanalysis, update or change the cryptographic technology to ensure they remain resilient against cyber threats and considering the information resources referred to in Article 10(2), point (a). Where the financial entity cannot update or change the cryptographic technology, it shall adopt mitigation and monitoring measures to ensure they remain resilient against cyber threats.

- Crypto-agility

Article 7

Cryptographic key management

4. Financial entities shall create and maintain a register for all certificates and certificate-storing devices for at least ICT assets supporting critical or important functions. The register shall be kept up-to-date.

- Certificate inventory

And from a technical perspective?

Algorithms, sizes etc

NIST ALGORITHMS-WHAT CHANGES (IN LENGTH SIDE)?

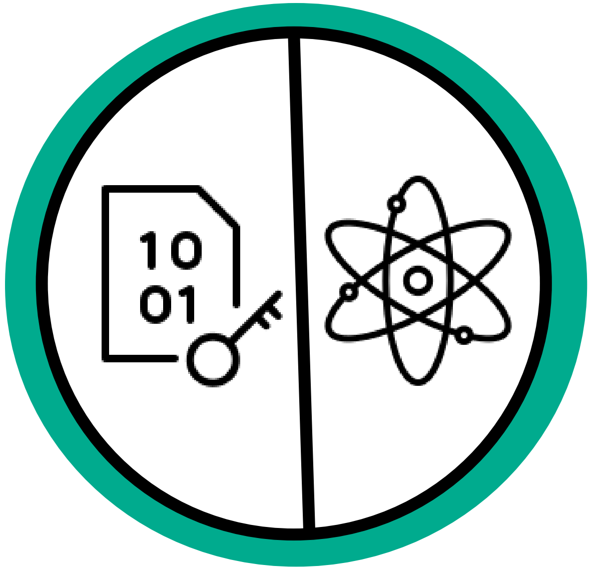
IT GROUP

	Algorithm	Theory based on	Quantum-safe	Public key length	Exchanged data length
KEM	X25519	ECC	No	32 bytes	32 bytes
	ML-KEM512	Lattice	Yes	800 bytes (factor: 25)	768 bytes (factor: 24)
	ClassicMcEliece384464	Code; candidate	Yes	261 120 bytes (factor: 8160)	128 bytes (factor: 4)
	BIKE	Code; candidate	Yes	1 540 bytes (factor: 48)	1 572 bytes (factor: 49)
Signatures	Ed25519	ECC	No	32 bytes	32 bytes
	ML-DSA II	Lattice	Yes	1 312 bytes (factor: 41)	2 420 bytes (factor: 76)
	Falcon-512	Lattice	Yes	897 bytes (factor: 24)	666 bytes (factor: 21)
	SPHINCS+ 128s	Hash functions	Yes	32 bytes (factor: 1)	7856 bytes (factor: 246)
	SPHINCS+ 128f	Hash functions	Yes	32 bytes (factor: 1)	17 088 bytes (factor: 534)

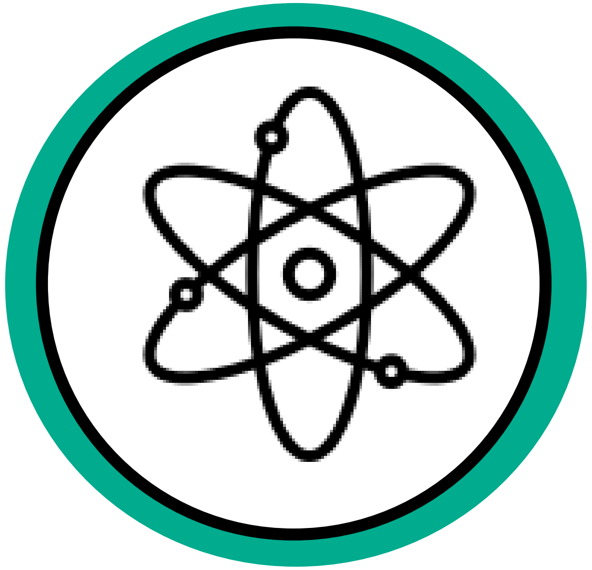
DIFFERENT ORGANISATIONS, DIFFERENT RECOMMENDATIONS

	Organisations	Pre-quantum		KEM recommendations	Signature recommendations
		AES requirements	Hash functions requirements		
USA	NIST	AES 128 (even for quantum-safe)	SHA 256 or higher	ML-KEM One more to be standardized after round 4	ML-DSA, FN-DSA, SLH-DSA Falcon, HQC (to be standardized)
USA	CNSA 2.0	Requires: AES 256	SHA 384	ML-KEM 1024 (level 5) for NSS (National Security Systems)	ML-DSA-87 (Level 5) as a general signature and LMS/XMSS (single-tree) for firmware/software signing
Europe	NCSC (UK)	AES 128	SHA 256	ML-KEM-768 (Level 3)	ML-DSA-65, SLH-DSA, and LMS/XMSS for long-term signatures
Europe	BSI (Germany)	Recommends: AES 128	SHA 256	FrodoKEM (976 and 1344), McEliece (460896, 6688128, 8192128) (will include ML-KEM (768 and 1024) once standardized by NIST)	SLH-DSA or ML-DSA (Levels 3 and 5), and LMS/XMSS in multi-tree variants for long-term signatures
Europe	ANSSI (France)	Recommends: AES 256	SHA 384	ML-KEM (768 and 1024) FrodoKEM as a conservative option	ML-DSA, FN-DSA (Levels 3 and 5), SLH-DSA, and LMS/XMSS
Europe	NLNCSA (Netherlands)	AES 256	SHA 256	ML-KEM-768 Acceptable: Classic McEliece and FrodoKEM	all NIST signatures and LMS/XMSS
Asia	South Korea and China	-	-	Their own PQC algorithms (unknown for the moment)	

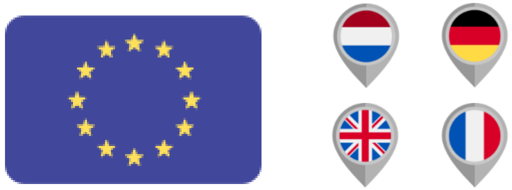
At least, do we all agree to go for quantum-safe cryptography ?



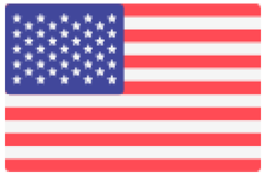
YES! Even if we have some disagreements on the "how"…



Hybridation



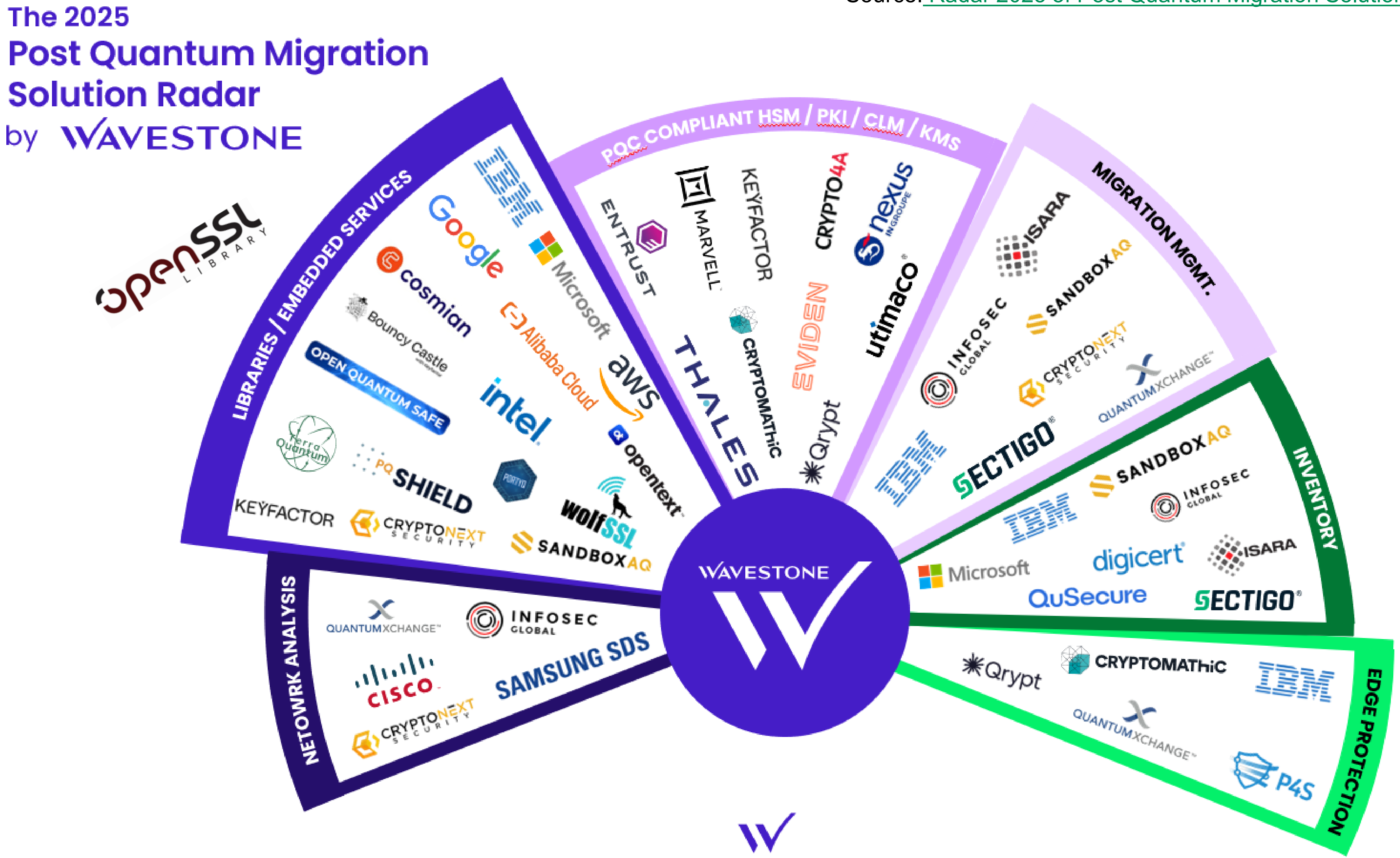
PQC standalone

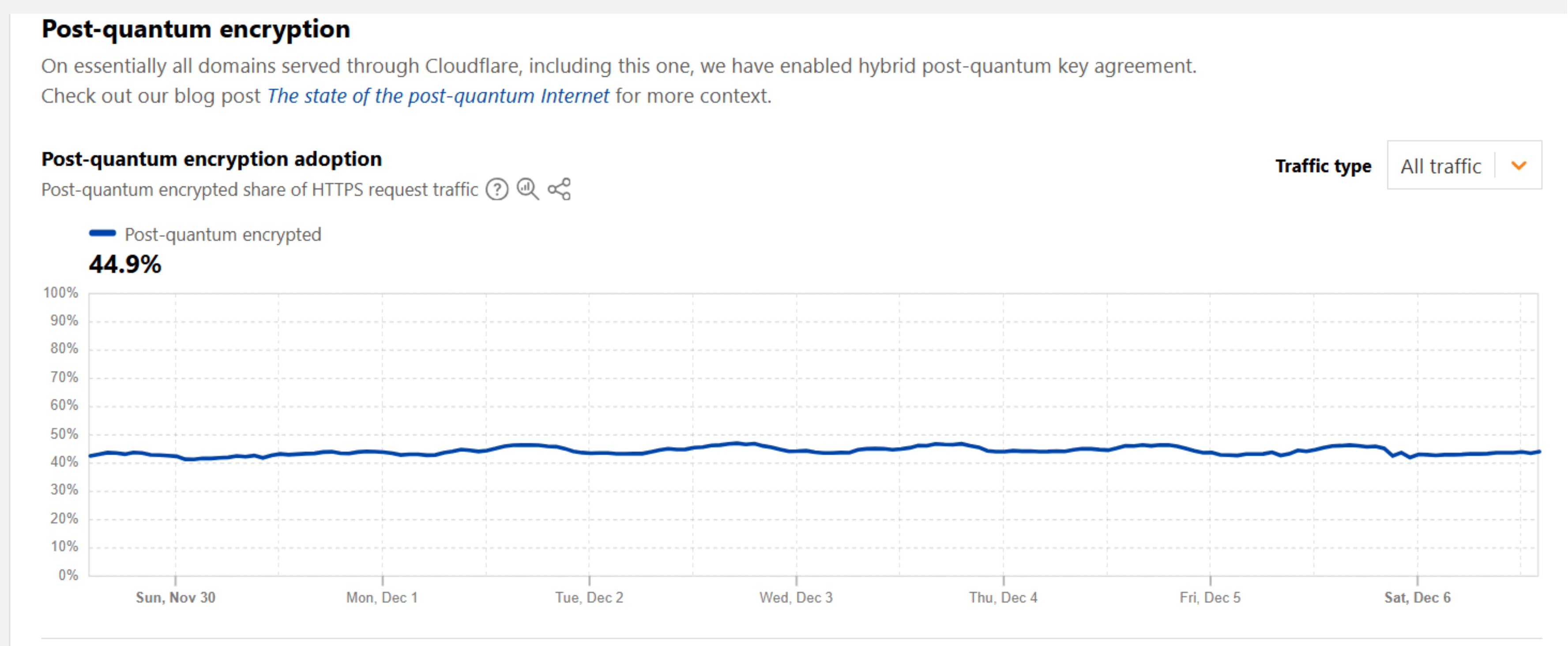


Has anyone REALLY started migration?

PROVIDERS WITH MIGRATION SOLUTIONS

Source: Radar 2025 of Post Quantum Migration Solutions - RiskInsight





- Cloudfare: ~45 % of HTTPS requests traffic are PQC protected

Messaging applications

- Signal : PQXDH (end to end encryption protocol) - 2024
- Apple/iMessage: PQ3 (PQC messaging protocol) - 2024

"QUANTUM-SAFE CRYPTOGRAPHY" : FINANCIAL EXPERIMENTATIONS

BANQUE DE FRANCE (2023)

- Joint work with: Cryptonext
  - Experimentation on: testing the implementation of a VPN

BIS(*) INNOVATION HUB'S EUROSYSTEM CENTER (2024)

- Project Leap
- Joint work with: Banque de France & Deutsche Bundesbank
  - Experimentation on: testing the implementation of quantum-safe cryptographic protocols between two central banks
    - Tested with hybridization mechanisms (a traditional public-key algorithm with several quantum-resistant algorithms)
    - Tested with payment messages

(*) Bank for International Settlements

BANQUE DE FRANCE/MAS (Monetary Authority of Singapore) (2024)

- Exchange of signed and encrypted email
  - Experimentation on: mail signature & encryption
  - Tested on: outlook email with a PQC plugin made available by CryptoNext
- More info: Here

BANQUE DE FRANCE/ALLIANZ FRANCE (2025)

- Securing central bank regulatory files transfers with PQC
- More info: Here

AM I ALONE?

FS-ISAC

- Financial Services - Information Sharing and Analysis Center
- Aim: A working group specific for PQC between international financial institutions
- Deliveries (Post-Quantum Cryptography Report (fsisac.com))
  - Business guidances
  - Technical guidances

Campus Cyber

- PQC Working Group
  - Streams
    - Awareness
    - Crypto-agility: Establish a questionnaire to measure companies' crypto-agility maturity
    - Panorama of (French) PQC providers (work in progress)
    - Guide for migration (work in progress)

Non exhaustive list

COMMON (WRONG) IDEAS

It is too early
Not really… Processes are long and planning is important!

We don't have budget
And this is why schedule is important!

We don't have standardized algorithms
Now we have!

We still cannot handle with shadow IT and obsolete software. We cannot add another threat
And that was already a problem.. So, try to not create new obsolete solutions!

We don't have compatible protocols
Maybe for some cases, but the work is in progress

We lack of experts
Education (continuously or not) is very important

OK, but I don't want to be the first industrial going forward
But.. You are not alone ;)

THANK Q !

IT GROUP

BNP PARIBAS

The bank for a changing world

EXTERNAL REFERENCES

TIMELINES & GOVERNEMENTAL RECOMMANDATIONS

- Europe
  - EU
    - A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography | Shaping Europe's digital future
    - BSI - Quantentechnologien und quantensichere Kryptografie - Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography
    - ENISA: Agreed cryptographic mechanisms
  - France: Etat de la prise en compte de la cryptographie post-quantique | ANSSI
  - Germany: BSI - Quantum Technologies and Quantum-Safe Cryptography
  - UK: Timelines for migration to post-quantum cryptography - NCSC.GOV.UK
- America
  - NSA: NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems > National Security Agency/Central Security Service > Article
  - NIST: IR 8547, Transition to Post-Quantum Cryptography Standards | CSRC
- North America
  - Canada: Quantum-Readiness Best Practices - v04 - 10 July 2024.pdf
- Asia
  - Singapore: MAS/TCRS/2024/01 : Advisory on Addressing the Cybersecurity Risks Associated with Quantum
- Australia
  - Australian guidelines: Guidelines for cryptography | Cyber.gov.au
- Worldwide
  - Post Quantum Government Initiatives by Country and Region - Newsroom

IT GROUP

ADDITIONAL EXTERNAL REFERENCES PER DOMAIN

- GSMA : Telecom use cases (Oct 2024)
- G7 : G7 expert group statement on planning for the opportunities and risks of quantum computing (Sept 2024)
- Eurosmart: Eurosmart position on quantum safe cryptography actions (June 2024)
- FS-ISAC: Guidance to help the payment card industry to mitigate risks of quantum computing (Feb 2025)