Oct 24/25th, 2024

Post Quantum Cryptography Update

Olivier Van Nieuwenhuyze

GlobalPlatform Policies

Please be aware that this meeting is being held in accordance with **GlobalPlatform's Bylaws and GlobalPlatform policies issued thereunder,** including but not limited to:

- Antitrust Policy
- IPR Policy
- Member Confidentiality Requirements
- Meeting Protocol and Guidelines

Above policies are set forth in the **GlobalPlatform Process and Procedures Manual** or **IPR Policy v5.0**, available on the Member website: Resources → Documents

Patent Call

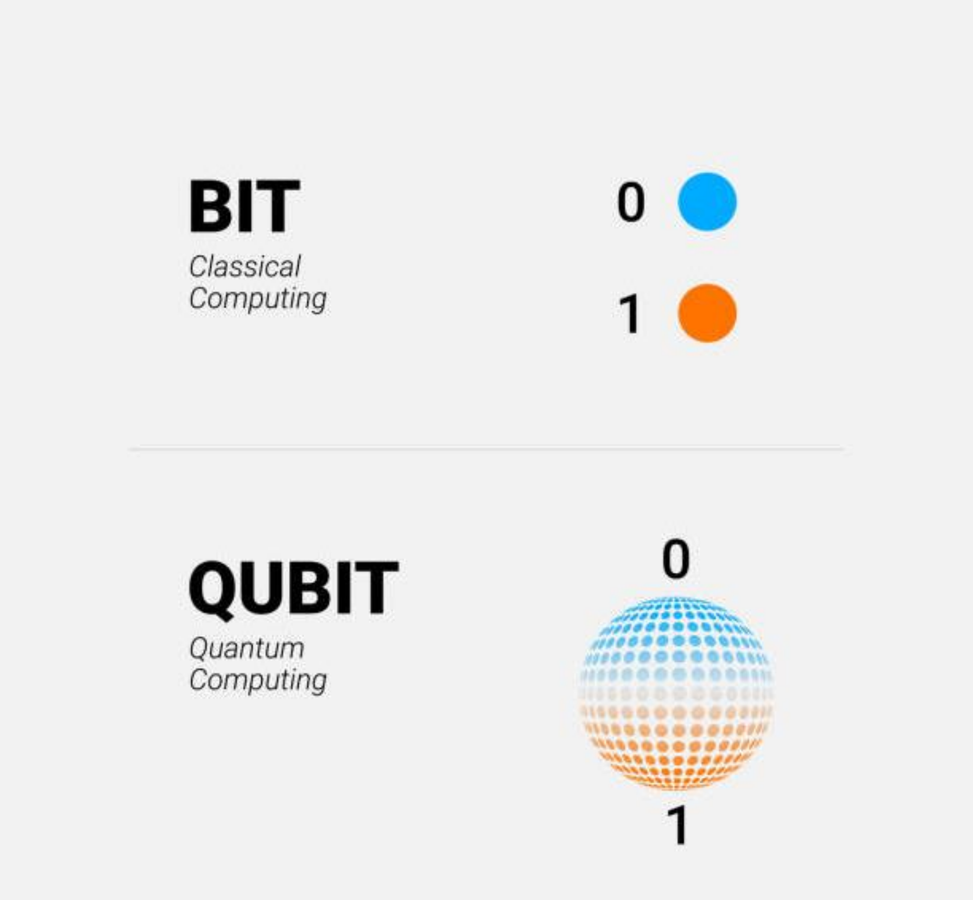
"Please be aware that this meeting is being held under the GlobalPlatform Intellectual Property Rights Policy. If you do not have a copy of this policy, please contact (or inform) the chairperson during this meeting. You may also view and download a copy of the policy at the Membership section of the GlobalPlatform Website.

At this time, each person in attendance is required to inform the chairperson if they are personally aware of any claims under any patent applications or issued patents which would be likely to be infringed by an implementation of any specification or other work product which is the subject of this meeting. You need not be he inventor of such patent or patent application in order to inform GlobalPlatform of its existence, nor will you be held responsible for expressing a good faith belief which proves to be inaccurate."

Global Platform™

The Quantum Computer

QUBIT

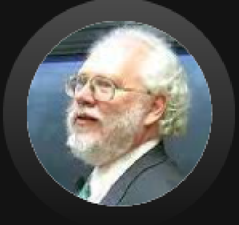


How Quantum Computer Impacts Cryptography?

CRYPTOGRAPHIC ALGORITHM TARGETED	TYPE	PURPOSE	IMPACT FROM LARGE SCALE QC
RSA	Public key	Signatures, Key establishment	No longer secure
Digital Signature Algorithm		Signatures, Key exchange	
ECDSA (Elliptic Curve DSA)			

CRYPTOGRAPHIC ALGORITHM TARGETED	TYPE	PURPOSE	IMPACT FROM LARGE SCALE QC
AES	Symmetric key	Encryption	e.g. longer keys needed
SHA-2, SHA-3	----------	Hash functions	e.g. larger output needed

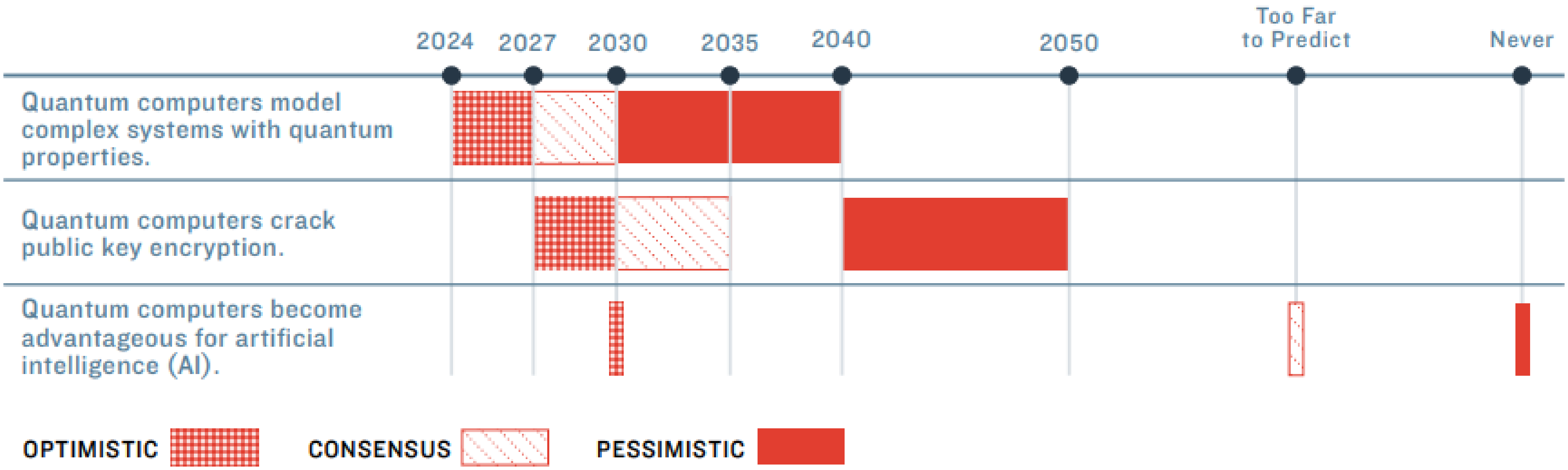
Peter SHOR



Lov GROVER

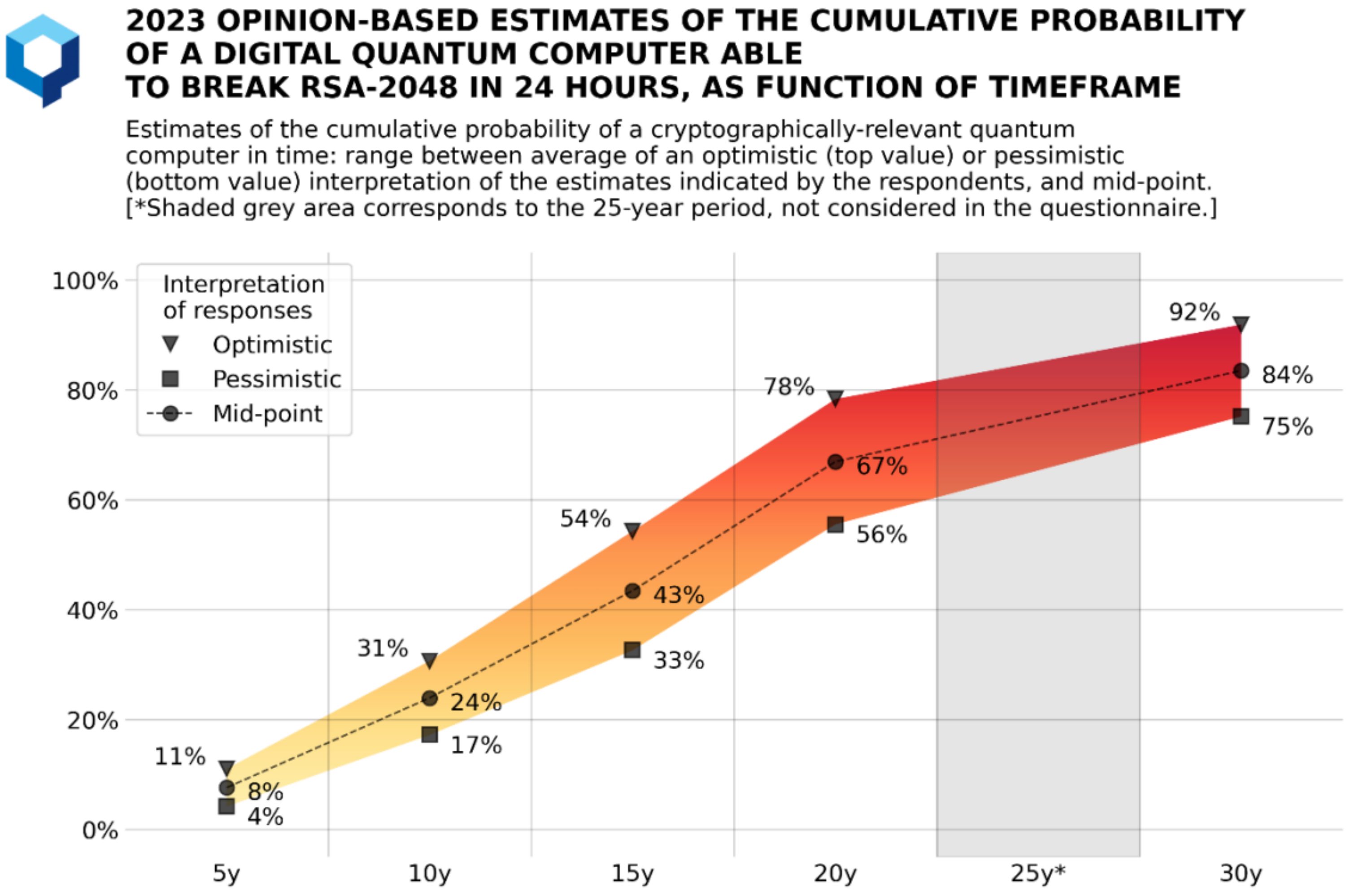
Global Platform™

PQC predictions (2022)



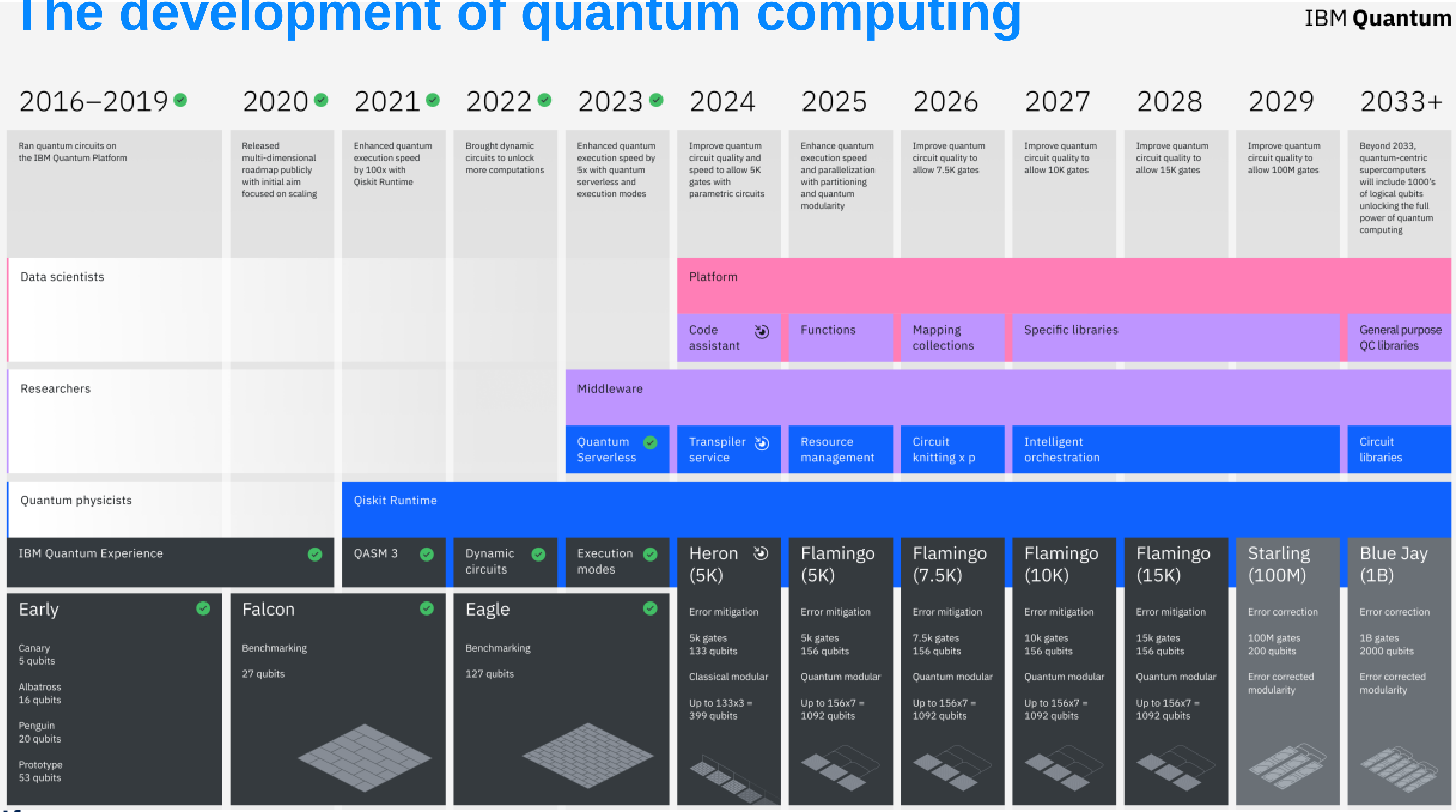
*Source: https://www.cisoforum.com/wp-content/uploads/2022/01/chinese-threats-quantum-era.pdf

PQC Predictions (2023)



Source : https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

The development of quantum computing



*Source: https://www.ibm.com/quantum/technology

The challenges facing current cryptography

The limitations of current cryptographic systems	Vulnerability to quantum attacks Long-Term security concerns
The threat posed by quantum computers	Quantum supremacy Risk of data breaches
The impact on security infrastructure	Re-evaluation of security protocols Urgency of the transition

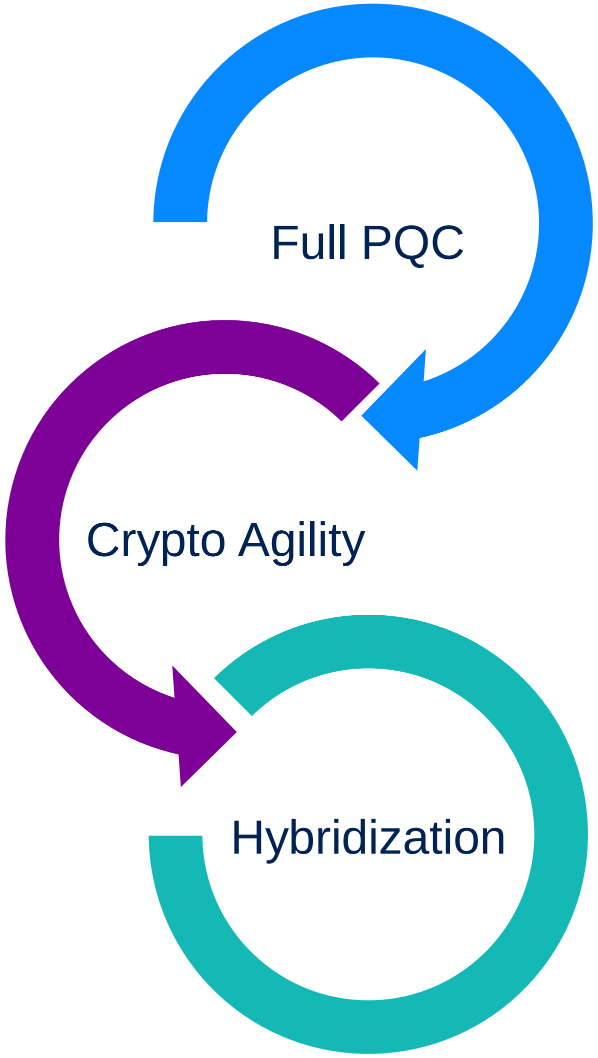
PQC: is it really a problem?

Yes.

- Finding the right solution can require significant effort.
- Migrating / deploying the solution is difficult and time-intensive.
- It is also urgent. There is a real risk today of “store now, decrypt later” attacks.

Global Platform™

What is the solution?



Global Platform™

What are the challenges of PQC migration?

Compatibility issues

- Legacy systems
- Interoperability

Performance concerns

- Computational overhead
- Resource constraints

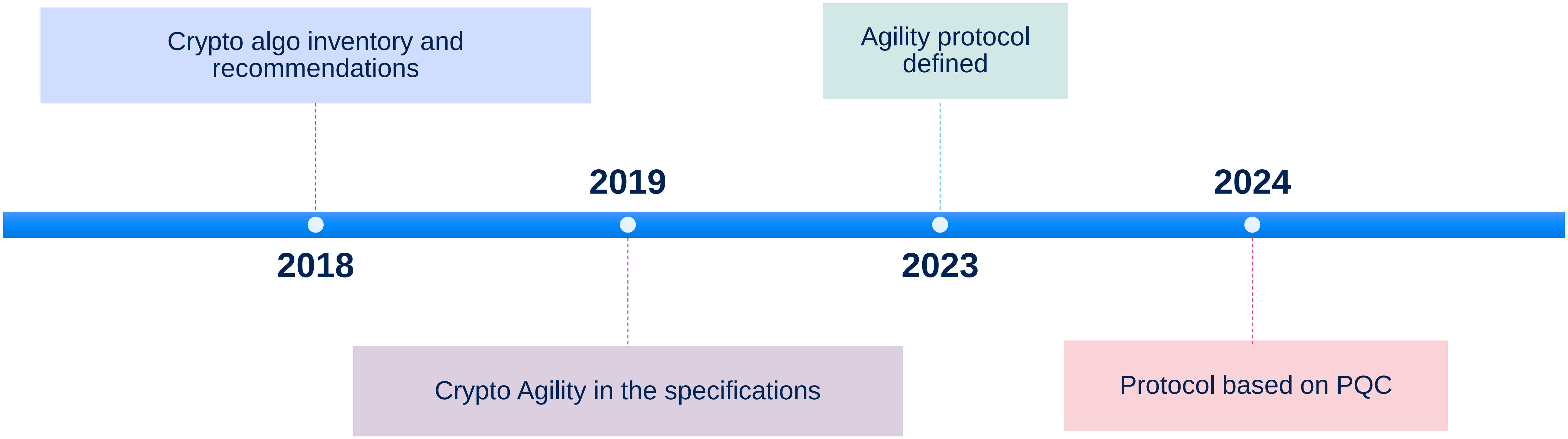
Implementation complexities

- Algorithm selection
- Security assurance

Transition strategy

- Phased approach
- Training and awareness

Timeline


Crypto algo inventory and recommendations
2018
2019
Crypto Agility in the specifications
Agility protocol defined
2023
2024
Protocol based on PQC

NIST Solution

Full PQC

Standard

- **ML-KEM - FIPS 203**: Published August 2024.
- **ML-DSA - FIPS 204**: Published August 2024.
- **SHL-DSA FIPS 205**: coming soon.

Additional round with remaining algorithms

New Round for Additional Round for Digital Signature

Global Platform™

PQC development challenges

- Availability of standardized PQC algorithm (e.g. : ML-KEM, ML-DSA …)
- Replacing existing protocols such as Diffie Hellman to other mechanism (modify the exchange dynamic)
- Cryptography security strength vs the HW feasibility

Security strength / Crypto algos	Symm. Algos	Factoring (RSA)	DLP (DSA, DH)	ECC (ECDSA, ECDH)	Hash	ML-KEM	ML-DSA
≤ 80 bits	3DES 2 keys	1024	1024	160	SHA-1		
112 bits	3DES 3 keys	2048	2048	224	SHA-224		
128 bits	AES-128	3072	3072	256	SHA-256	ML-KEM-512	ML-DSA-44
192 bits	AES-192	7680	7680	384	SHA-384	ML-KEM-768	ML-DSA-65
256 bits	AES-256	15360	15360	512	SHA-512	ML-KEM-1024	ML-DSA-87

PQC migration into the existing infrastructure

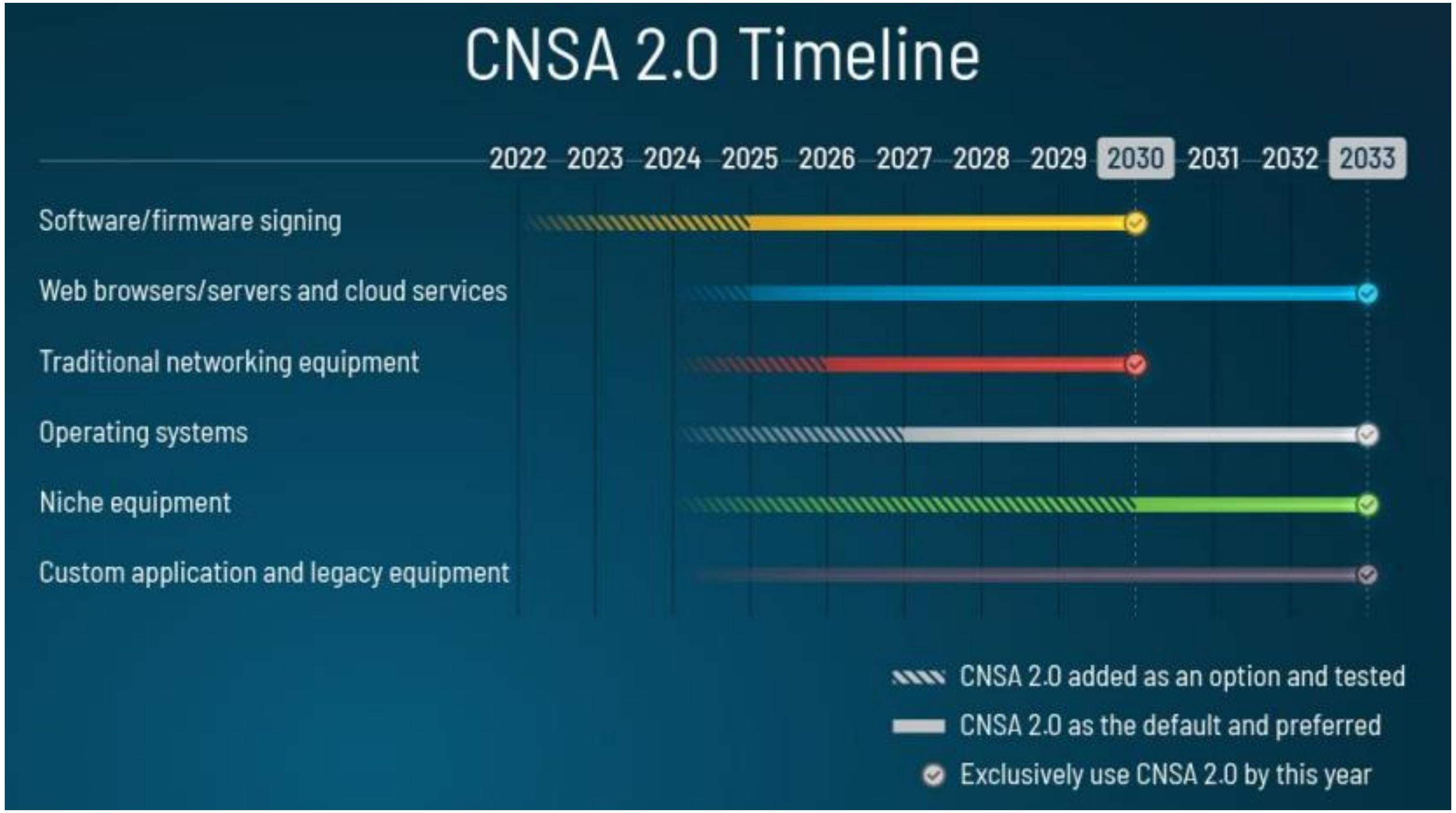
CONSTRAINT OF THE DEPLOYMENT

CRYPTOGRAPHY AGILITY

REGULATION

USAGE OF THE HYBRIDIZATION

Regulations Increase the complexity



EU required different security levels (than US) but some countries mandate the hybridization

Conclusions

CHALLENGE TO MIGRATE AND DEPLOY SYSTEM ON THE CURRENT INFRASTRUCTURE

CHALLENGE TO BE COMPLIANT WITH THE REGULATION

TECHNOLOGY DEPLOYMENT AND FEASABILITY

Global Platform™

The standard for secure digital services and devices

→globalplatform.org