SPIE

X-SPIErience Day 2020

DIGITALE SOUVERÄNITÄT

cisco Partner

FORTINET

HUAWEI

SPIE, sharing a vision for the future

X-SPIErience Day 2026
DIGITALE SOUVERÄNITÄT

SPIE

Ensuring Data Sovereignty by Switching to Quantum-Safe Cryptography

GILBERT CABALLER

Information Security & Data Privacy Consultant
SPIE ICS

Objective and agenda

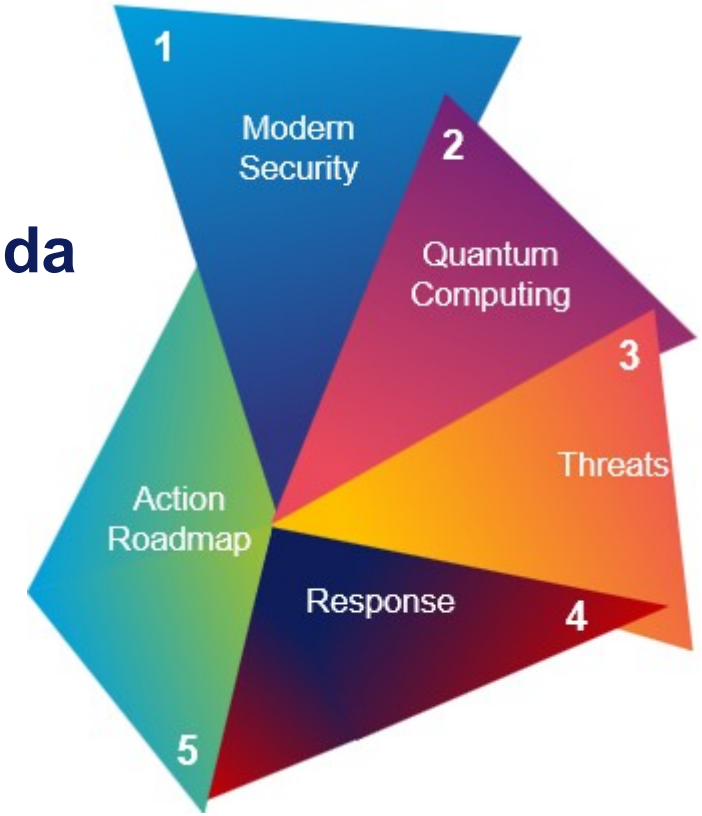
“Digital sovereignty” is the capacity of an organization to be in control of its data and digital infrastructures and is put at risk with emergence of quantum computers.

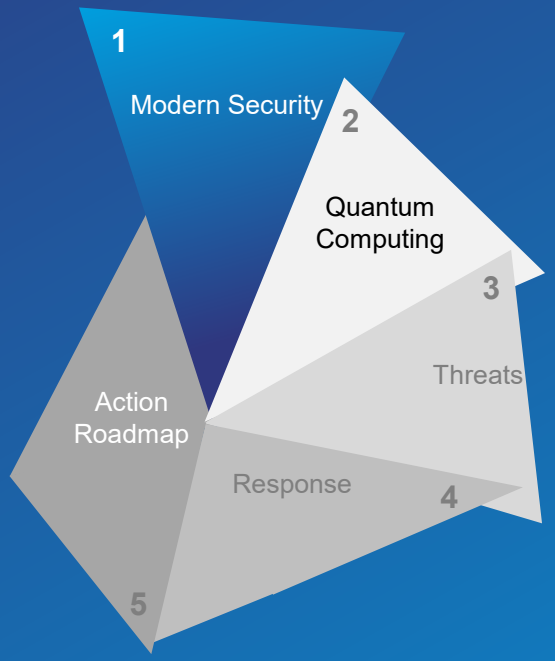
Objectives

Learn risks pose by Quantum Computers and solution to mitigate it.

- **Q-Day**
- **Quantum Computing**
- **Post-Quantum Cryptography (PQC)**
- **Cryptoagility**

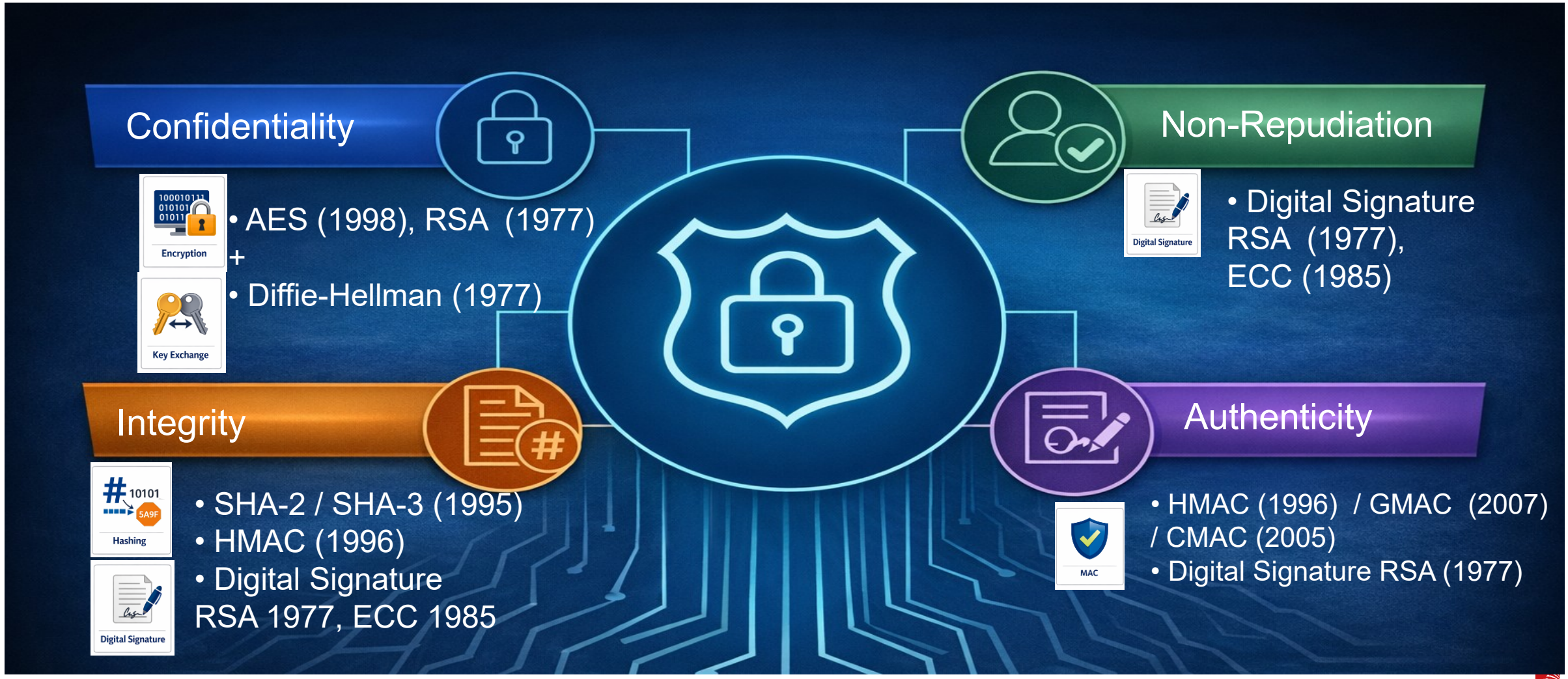
Agenda





Modern Security

Cryptography



Classic Cryptography and impact of Quantum theories

1970s–1980s

RSA (1977) | Diffie–Hellman (1976) | ECC (1985)
Asymmetric (public-key) cryptographic algorithms.
Based on the assumed computational infeasibility of solving certain mathematical problems with classical computers.

Impact

Classical Cryptography

Attacks computationally infeasible (> Age universe to break)

✓ RSA-2048, DH, ECC secure in practice

1994

Shor's Algorithm

Peter Shor demonstrated that a sufficiently powerful quantum computer could **solve integer factorization** and **discrete logarithms** with computation efficient scale (polynomial time).

Impact

Quantum Breakthrough

× RSA, DH, ECC are no longer secure
New algorithm needed

1996

Grover's Algorithm

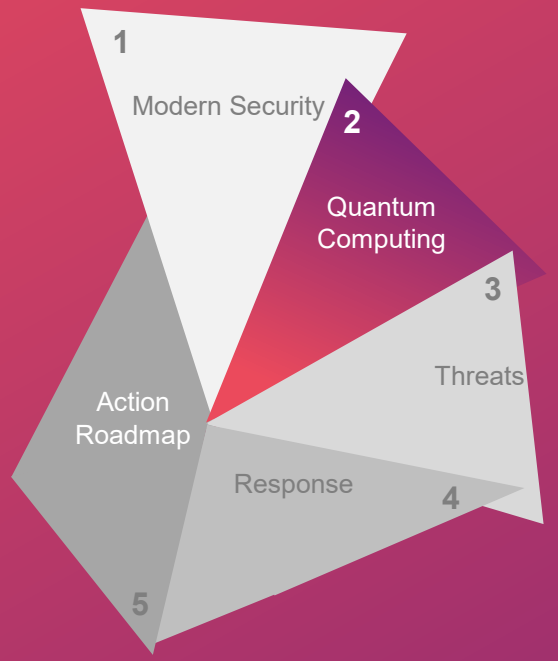
Lov Grover demonstrated how quantum computers can speed up trial-and-error searches.

Impact

Quantum Speed Up

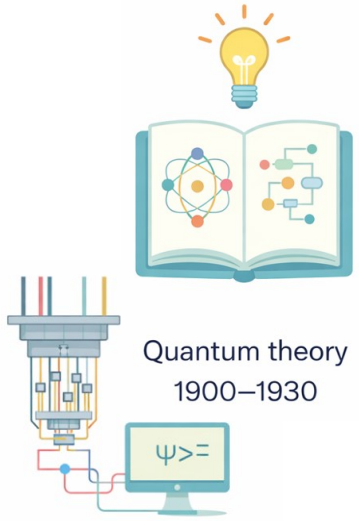
Security reduced
× AES-128
× HMAC SHA 256

Recommended
✓ AES 256 ->
✓ HMAC SHA 384,
✓ SHA 512
Key Increase

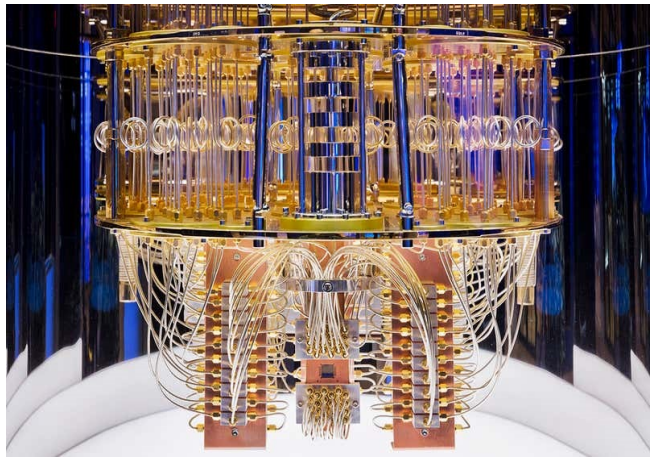


Quantum Computing

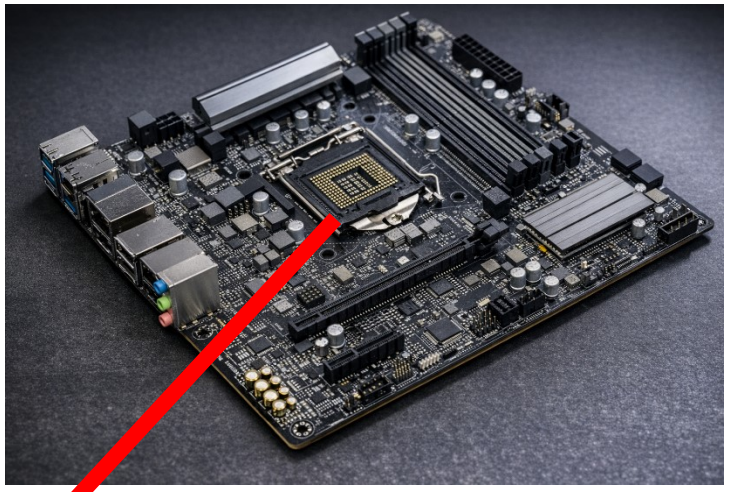
Quantum Computing and classical Computing



Experimental computers
1990s–2000s

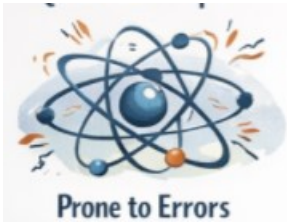


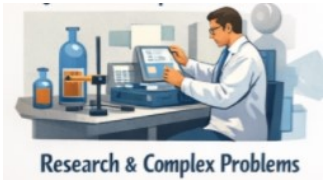
Source : ESA Agency IBM quantum computer

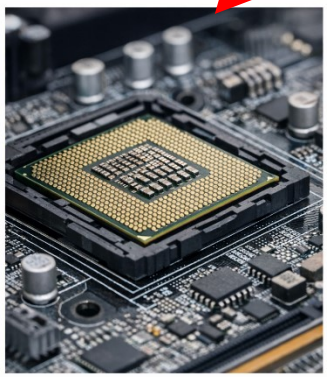


Source : IA Classical Motherboard

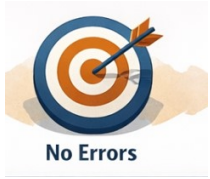
Digital Classical computers started in 1940. e.g. Eniac 1945.







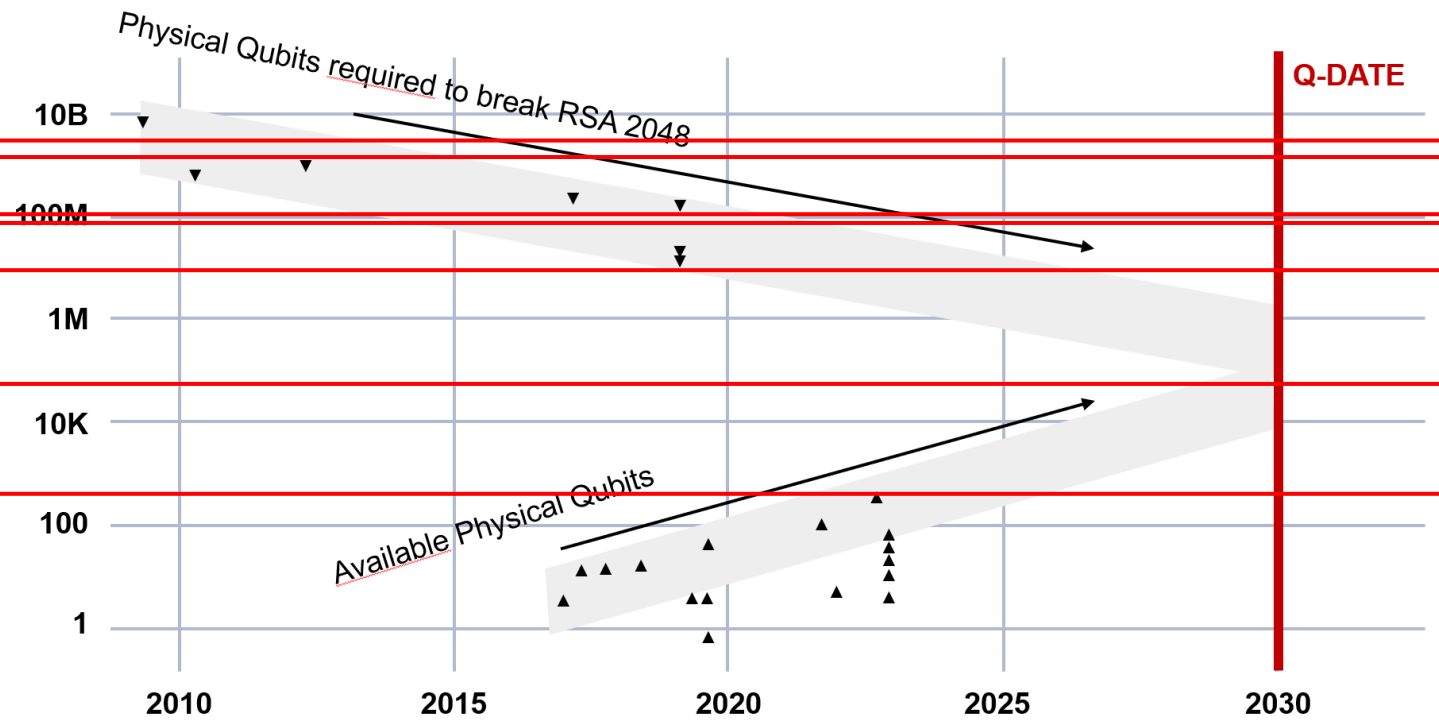
Source : IA



Evolution Quantum computers and Q-Day

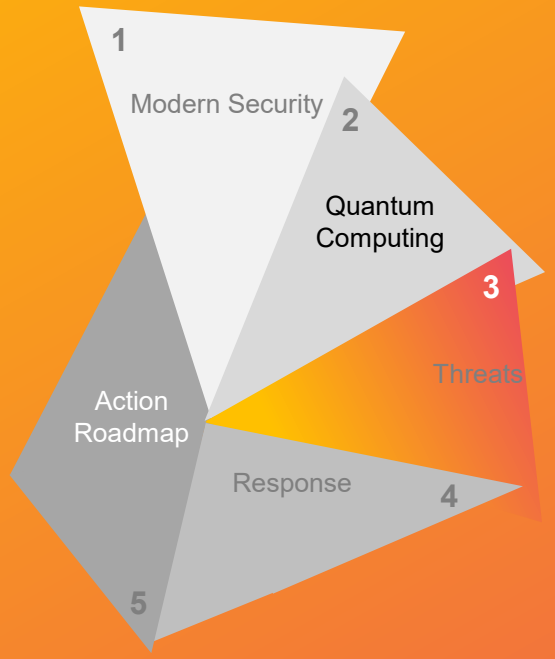
Year	Qubit Physical	Qubit Logical	Error rate	Errors per operation	Notes
2000	1–5				
2005	~5				
2010	~10				
2015	~50				
2020	~100				
2022	~400				
2023	~1 000				
2025	1 000–5 00				
2030	10 000 – 100				

Source: *Data synth*
(2000–2026.



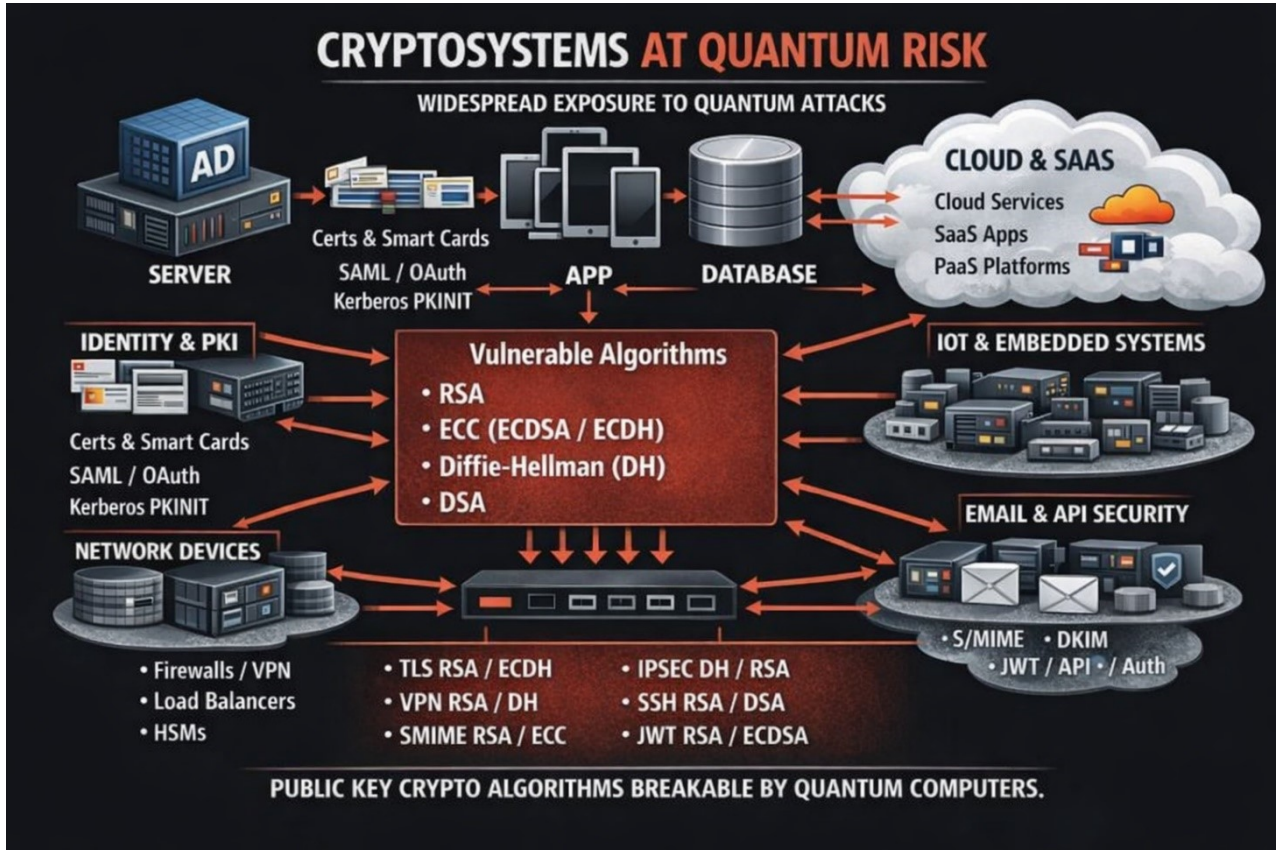
Break RSA 2048

Year	Physical Qubits	Logical Qubits	Notes
			theoretical; no error correction
			surface-code assumptions
			ved QEC models
			nized **Shor's algorithm (Gidney/Ekerå)**
			ware Circuit + scheduling optimizations
			st plausible FT convergence combination s and error rates


1
Modern Security
2
Quantum Computing
3
Threats
4
Response
5
Action Roadmap

Threats

What systems are at risk ?



Source : IA

Cryptography is embedded throughout infrastructure.

Network : Firewalls, routers, switches, proxy

Protocols: VPN tunnels (IPsec), Secure web traffic (HTTPS/TLS), remote management (SSH).

Security Infrastructure: HSMs & Smart Cards:

Trust : Public Key Infrastructure (PKI), Certificate

App & DB: In-house Software code with cryptographic libraries / hard-coded secrets db with (PII) at rest.

Endpoints & IoT: Embedded Industrial Systems (OT).

Cloud Services: APIs and SaaS platforms that manage their own encryption keys.

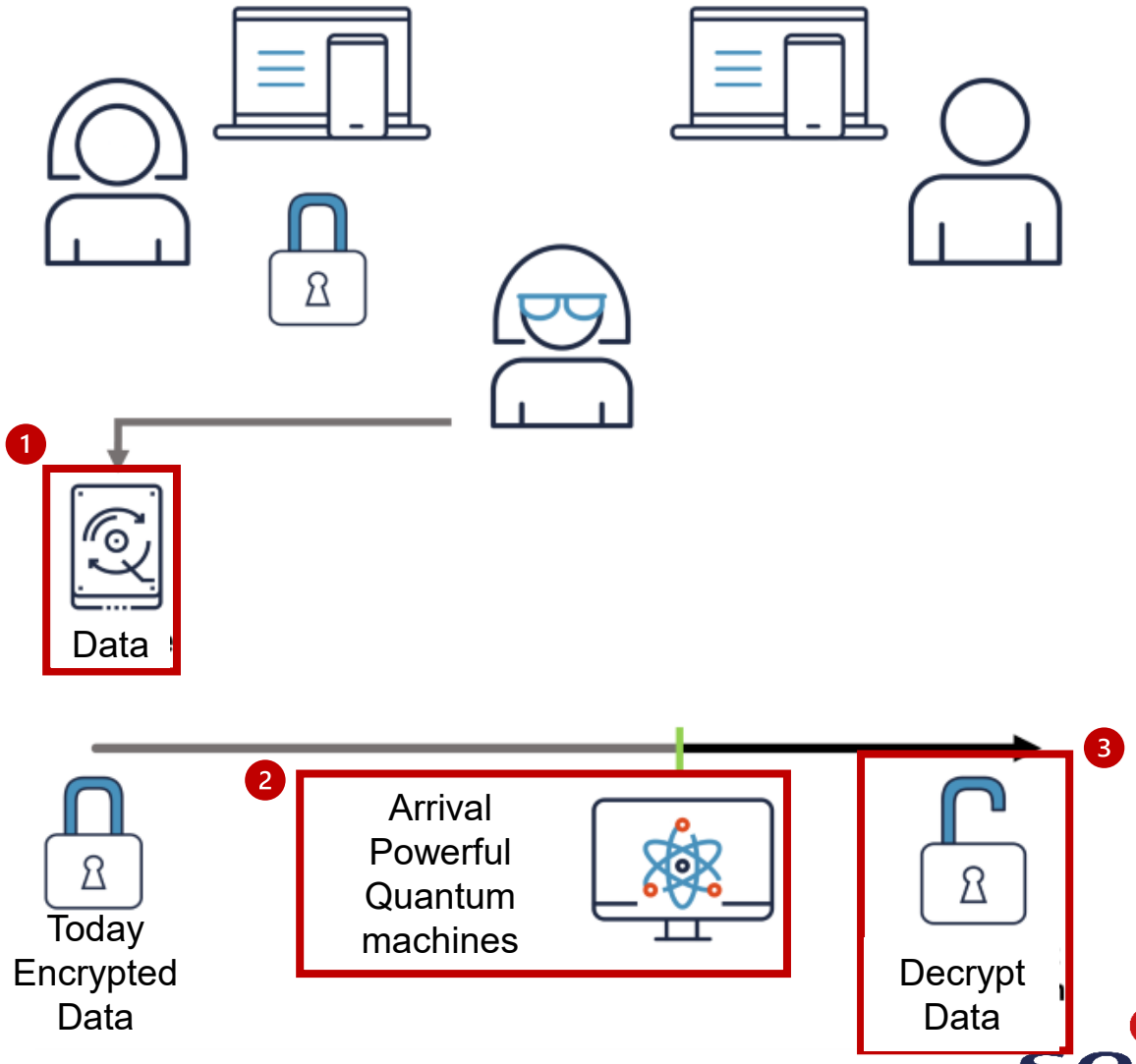
Risque: Harvest Now, Decrypt Later (HNDL)

Adversaries

1. **Intercept and store data encrypted with RSA/ECC based cryptography**
2. **Wait Quantum computer becomes available**
3. **Decrypt later the stolen data**

Data could contain

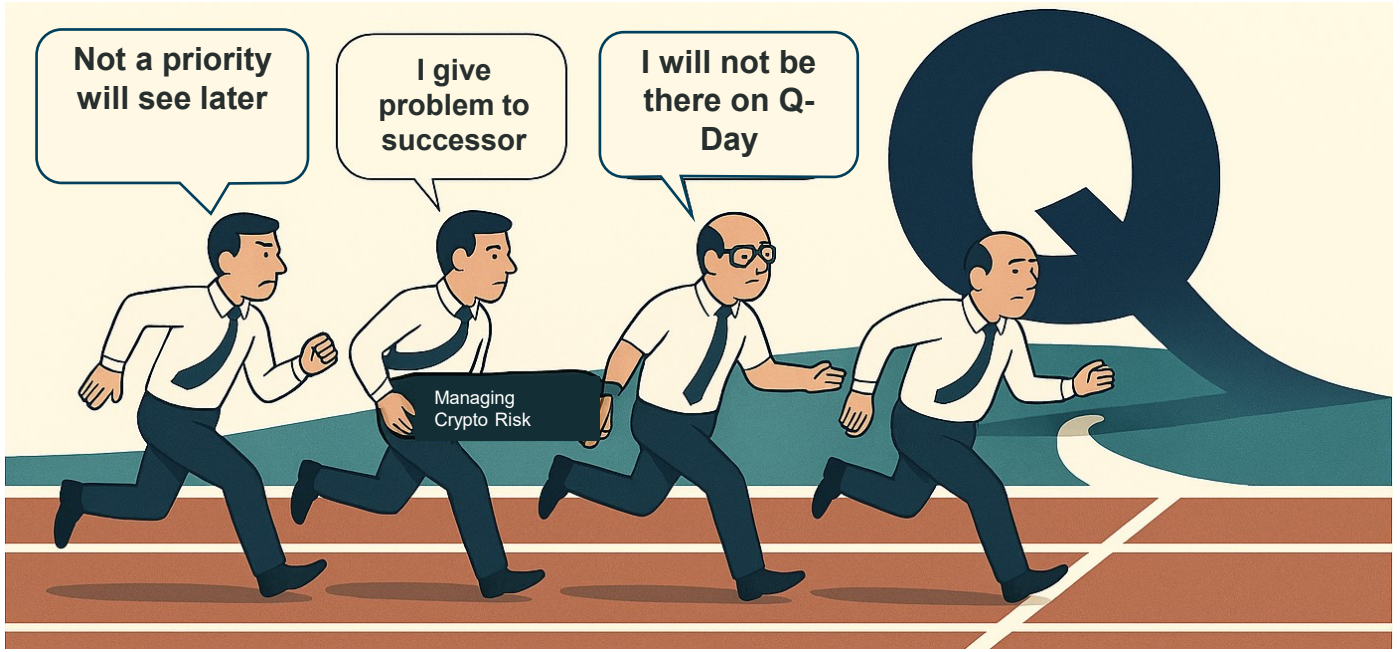
- Sensible Personal Data
- Intellectual Property
- Secret and Strategic Information

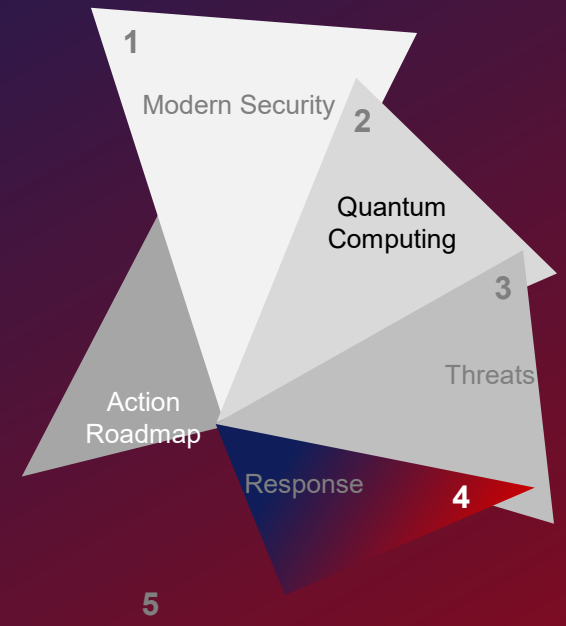


Not resolving risk

- Future noncompliance with EU Laws NIS, DORA
- Cyber Espionage (Government)
- Third Party Chain Risk
- Blockchain Risk
- Compromised Digital Identity and Critical Infrastructure

Crypto risk requires actions today not when Q-Day arrives.




1
Modern Security
2
Quantum Computing
3
Threats
Action Roadmap
Response
4
5

Response

NIST Response: Post Quantum Cryptography (PQC)

2016
Identify Risks

NIST IR 8105
- Quantum will break RSA, DH, ECC
- Long-term encrypted data already at risk

2017
PQC Program

Launch Post Quantum Cryptography program

2022
Select solutions

Kyber (encryption)
Dilithium, Falcon, SPHINCS+ Signature)

2024
Publish Standards

PQC Algorithms

Post Quantum Cryptography (PQC) : cryptographic algorithms designed **to resist attacks** from **both classical and quantum computers** to secure electronic information against the future threat of quantum computers

PQC are **designed to run on conventional computers** while remaining secure against attacks by a quantum computer.

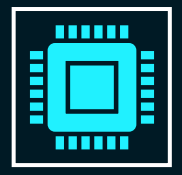
* NIST CSRC – Post-Quantum Cryptography Project

NIST Response: Post Quantum Cryptography (PQC)

FIPS 203: Module-Latice-Based Key-Encapsulation Mechanism (**ML-KEM**)

Purpose: Key exchange / encryption

Replaces : RSA-OAEP, Diffie-Hellman, ECDH



FIPS 204: Module-Latice-Based Digital Signature Standard (**ML-DSA**)

Purpose: General-purpose digital signatures

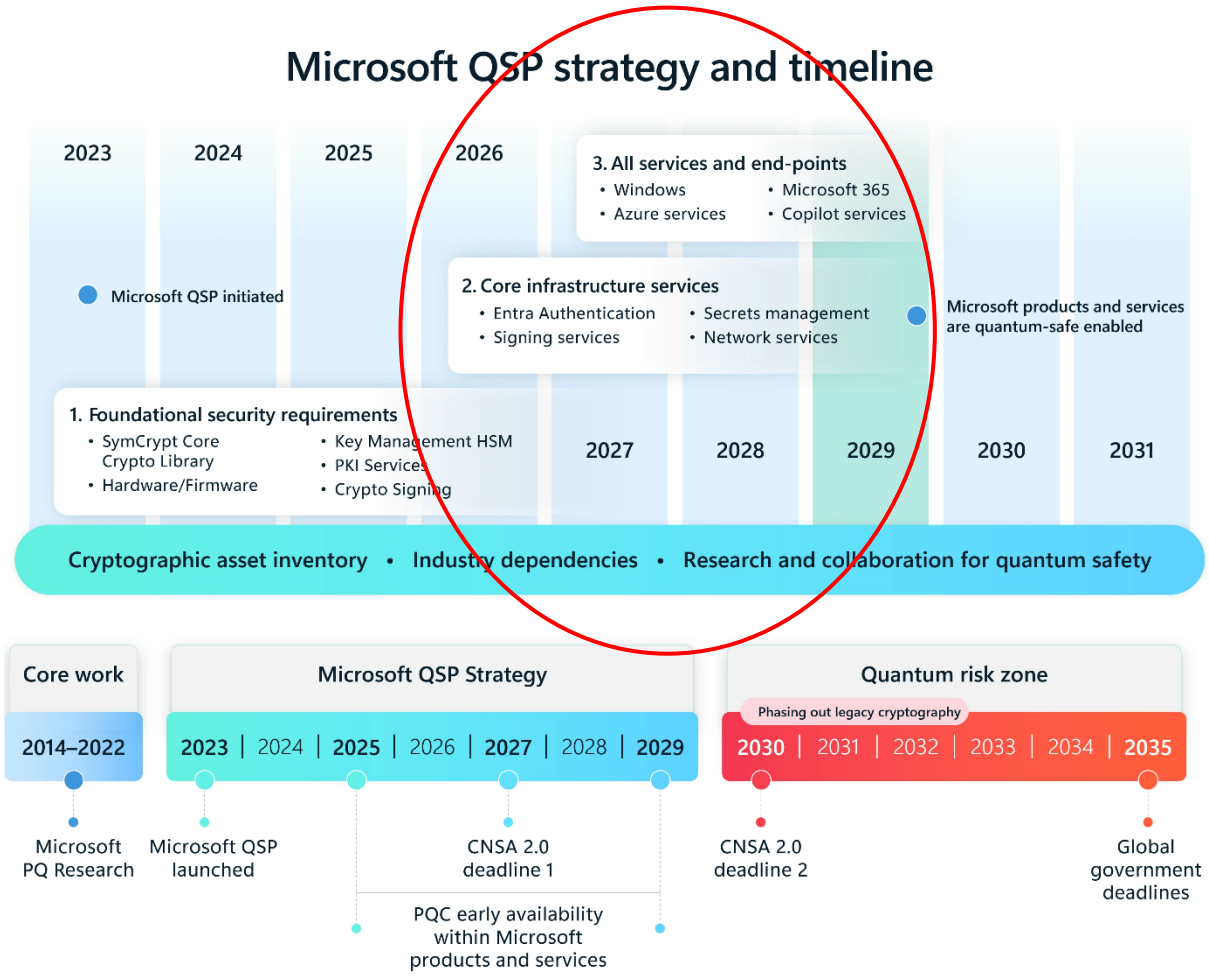
Replaces : RSA-PSS, DSA, ECDSA, EdDSA

FIPS 205: Stateless Hash-Based Digital Signature Standard (**SLH-DSA**)

Purpose: Hash-based fallback / diversity

Replaces: RSA / ECC signatures (conservative alternative)

Roadmap type (example Microsoft)



Microsoft Quantum Safe Program (QSP)

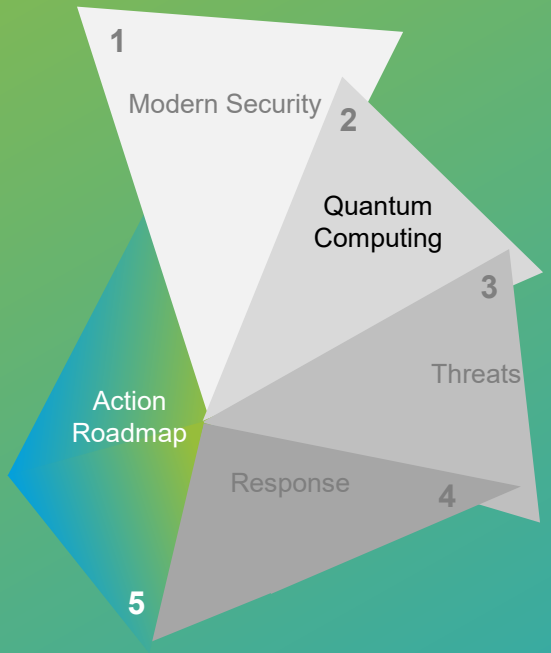
Multi-year initiative launched publicly in 2023–2025

- Transition all Microsoft products and services to post-quantum cryptography (PQC)
- Protect against “Harvest Now, Decrypt Later” (HNDL) attacks
- Align with NIST, NSA CNSA 2.0, OMB, CISA, EU / global timelines

QSP targets:

- 2029 for PQC **broadly available** and **deployable**.
- 2033 for complete across all Microsoft products

Action Plan Roadmap



CEG G7 Cyber Expert Group

“Quantum Risk is a resilience risk today not a future IT Problem”

“Make critical systems quantum-resilient < 2030”

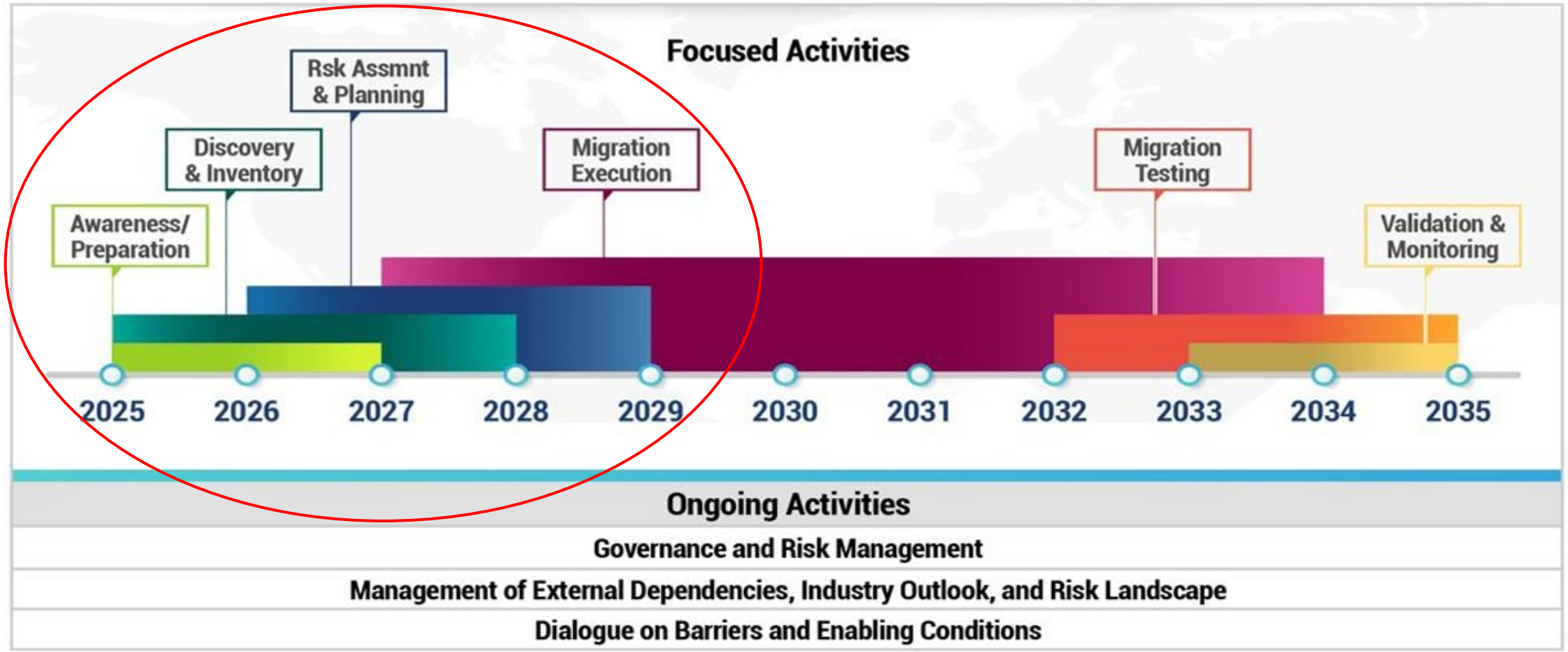
Immediate preparation for PQC migration to protect against ***decryption of harvested data***

Key Migration Activities and Outcomes	Potential Activities for Financial Entities
1. Awareness & Preparation	Executive-level risk awareness and initial post-quantum resilience strategy, and defined key roles.
	Mapped critical systems, functions, sensitive data, and communication protocols.
2. Discovery & Inventory	Comprehensive inventory of cryptographic assets, communication protocols, and relevant third-party dependencies.
	Identified gaps in people, processes, organization, and technology capabilities.
3. Risk Assessment & Planning	Tailored migration plans for critical and less critical functions, including tools, standards and interoperability.
	Adapted internal processes for capability building, governance and risk management.

Key Migration Activities and Outcomes	Potential Activities for Financial Entities
4. Migration Execution	Quantum-resistant solutions progressively deployed, starting with priority functions.
	Transition pace adapted to evolving quantum threat landscape.
5. Migration Testing	Migrated functions are tested.
	Ecosystem-oriented quantum-resilience exercises performed.
6. Validation & Monitoring	Continuous validation and ongoing improvement.
	Incorporation of new cryptographic standards.

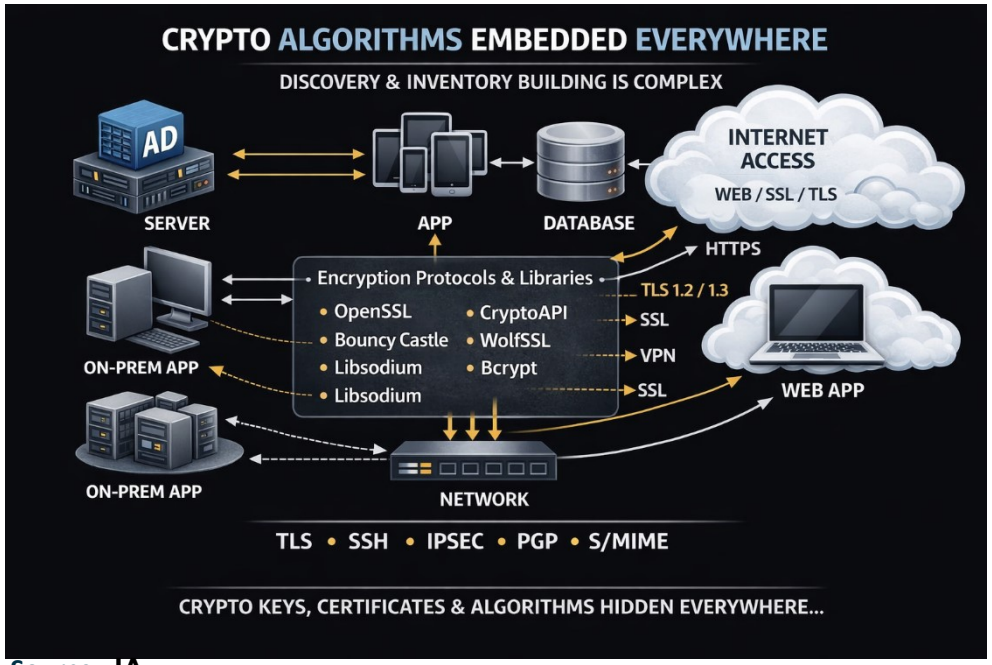
Source : G7 CYBER EXPERT GOUP : Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector

CEG G7 Cyber Expert Group

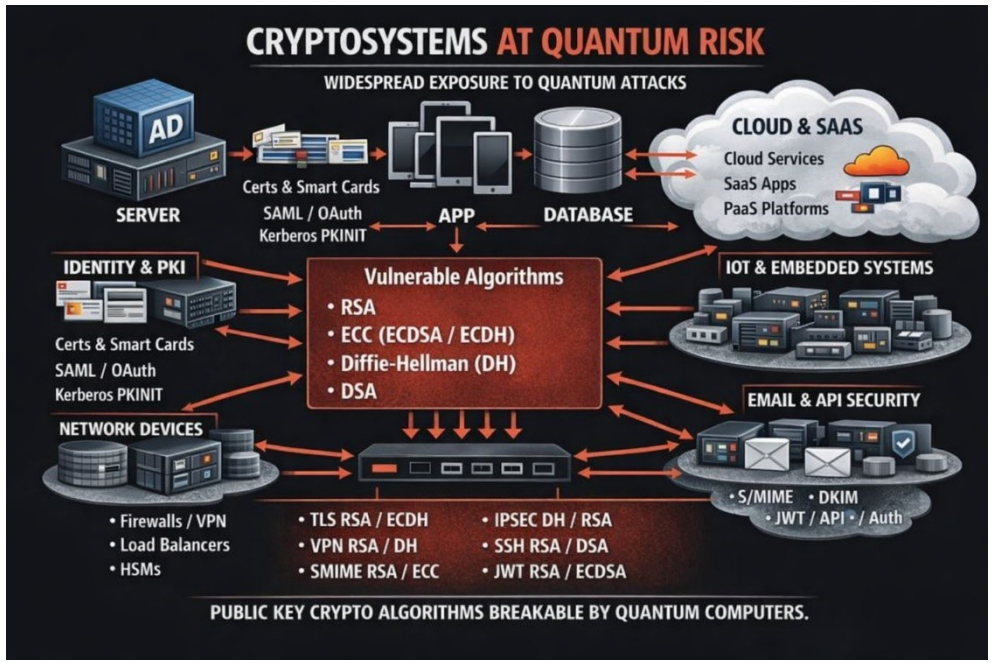


Source : G7 CYBER EXPERT GOUP : Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector

Discovery & Inventory



Source : IA



Source : IA

Discovery & Inventory

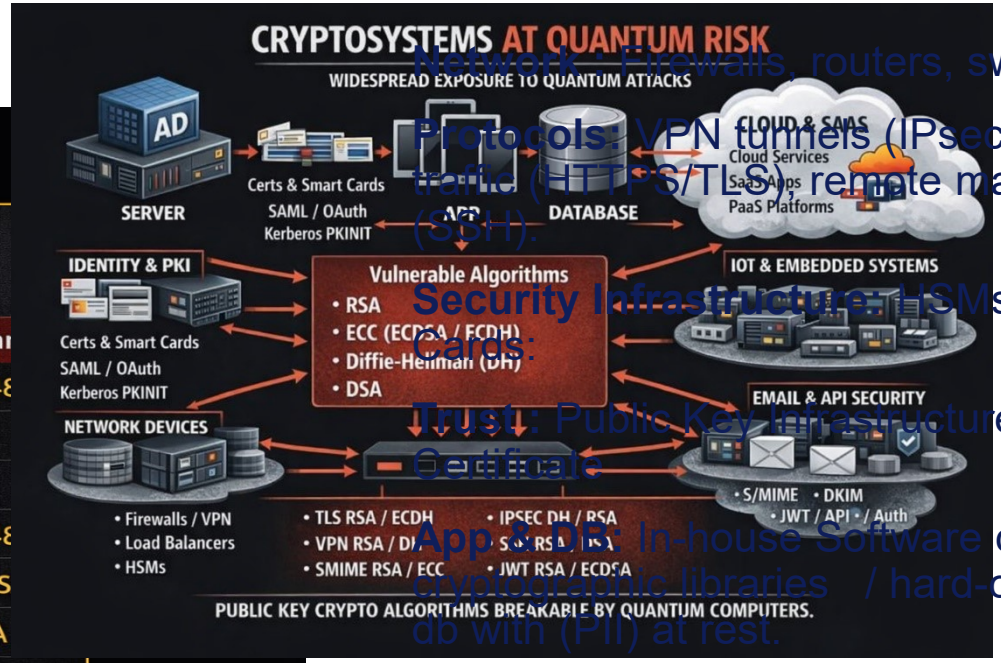
CRYPTO INVENTORY

Inventory for all cryptographic algorithms

Device	Name	Type	Algorithm	Algorithm
Web Server	Prod-Web01	HTTPS Cert	RSA-2048	RSA-2048
User Laptop	Dev-Laptop07	VPN Key	ECDH	ECDH
Application	Finance-App	JWT Signing	ECDSA	ECDH
Database	Customer-DB	TLS Connection	RSA-2048	RSA-2048
IoT Device	Sensor-Unit23	ECC ECDSA	ECC ECDSA	ECC ECDS
Firewall	Corp-FW03	IPsec Tunnel	DH / RSA	DH / RSA
Email Server	Mail-GW01	S/MIME Cert	RSA-1024	RSA-1024
Cloud Service	SaaS-Portal	API Auth	ECH / ECDSA	ECH / ECDSA

113 Vulnerable Crypto Assets Discovered

Source : IA



Source : IA

Network : Firewalls, routers, switches, proxy

Protocols: VPN tunnels (IPsec), Secure web traffic (HTTPS/TLS), remote management (SSH).

Security Infrastructure: HSMs & Smart Cards:

Trust: Public Key Infrastructure (PKI), Certificate

App & Data: In-house Software code with cryptographic libraries / hard-coded secrets db with (PII) at rest.

Endpoints & IoT: Embedded Industrial Systems (OT).

Cloud Services: APIs and SaaS platforms that manage their own encryption keys.

Lifecycle Certificates

Prior 2012 → **10 years**

2012 → **5 years**

2015 →**3 years**

2018 → **2 years**

2020 → **398 days**

2026 → **200 days**

2027 → **100 days**

2029 → **47 days**

SPIE Services

Key Migration Activities and Outcomes
1. Awareness & Preparation
2. Discovery & Inventory
3. Risk Assessment & Planning

Key Migration Activities and Outcomes
4. Migration Execution
5. Migration Testing
6. Validation & Monitoring

Key Take Away

- Cryptographically relevant quantum computers are approaching, they will be capable to break today's encryption algorithms (RSA, DH, ECC) → Q-Day,
- "Harvest Now, Decrypt Later" is a current and active threat
- Certificate lifecycle is shortening trend (≈47 days), Manual certificate management is no longer viable.
- Action must be taken before Q-Day—not when it arrives
- Remediation :
  - Replace RSA, DH, ECC with Post-Quantum Cryptography (PQC) algorithms
  - Increase Key Size for AES-256, HMAC-SHA 384, SHA 512
  - Crypto-agility strategic capability to automate Certificate Lifecycle Management
  - Project Governance, Risk Assessment, Inventory.

SPIE can help you !!

Next Steps

- Schedule a meeting Assessment, Roadmap, Governance)
- 1 Selection of your first priority use case
- Proposal of a tailored solution ensuring certificate management
- Design pathway toward Post-Quantum Cryptography (PQC)

Ready to activate your transition to PQC ? Let’s talk !

Ihr Ansprechpartner bei SPIE ICS

Let’s identify the first use cases together!

spie.ch/govern

Gilbert Caballer

Information Security & Data Privacy Consultant

Tel. +41 79 740 07 41

Mail gilbert.caballer@spie.com