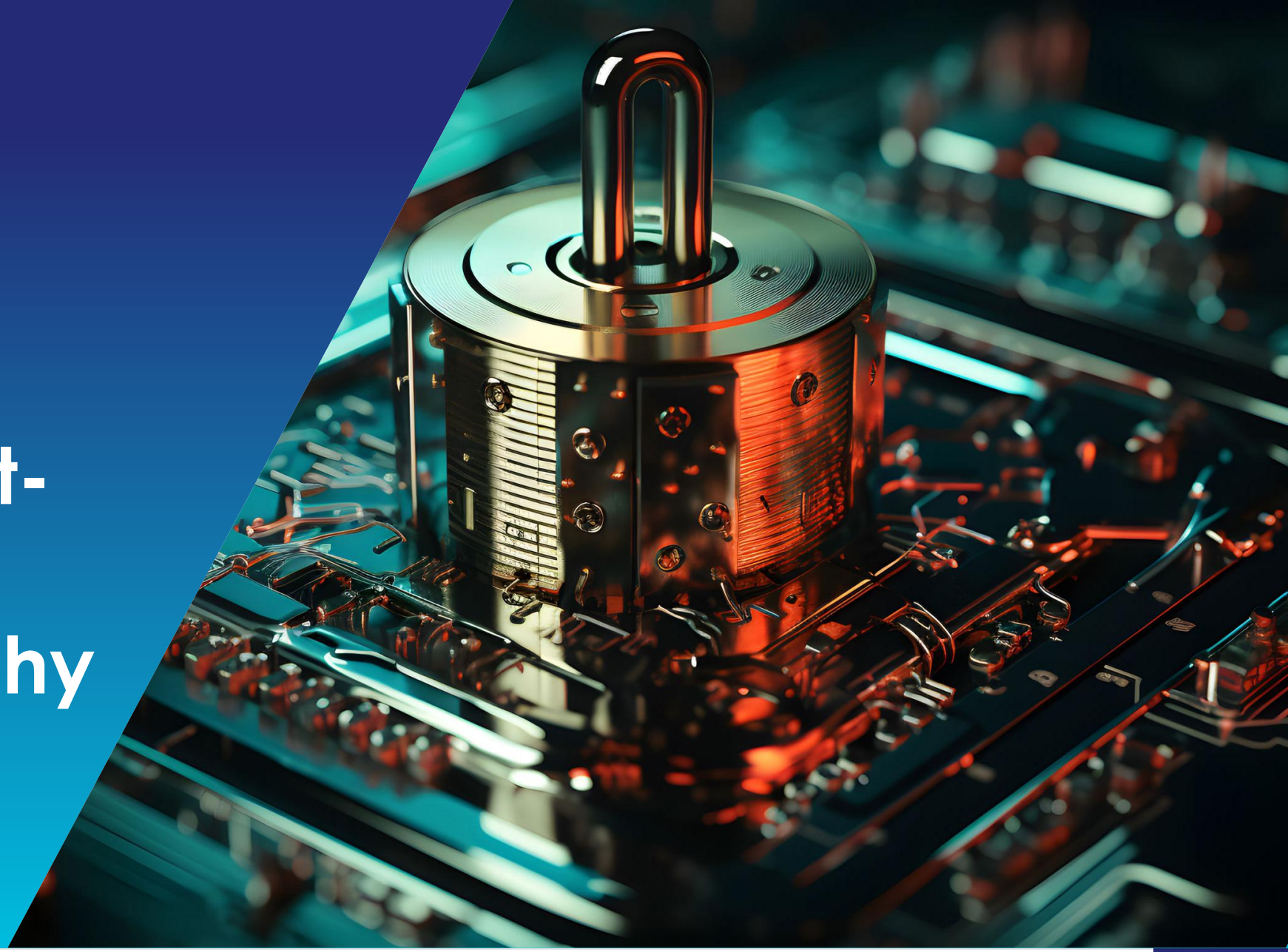
THALES
Building a future we can all trust

Planning for Global Specifications: Agility

Yves LE BOBINNEC
Cybersecurity Architect, Thales

GlobalPlatform CVF
Munich | October 21, 2026

A Growing Consensus Around Post-Quantum Cryptography



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

When will it be a problem?

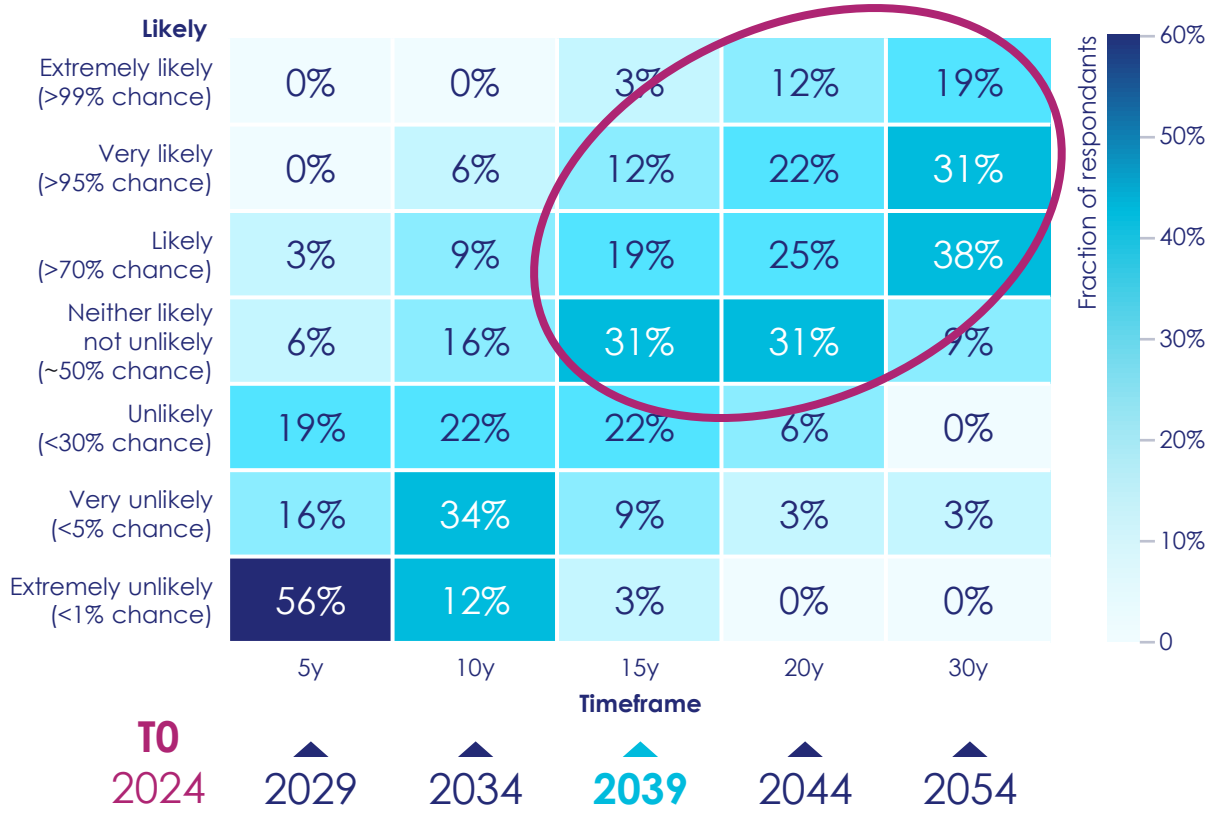
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

Likelihood of RSA-2048 break in 24 hours by a Quantum Computer

2024 Experts' views

The experts indicated their estimate for the likelihood of a quantum computer that is cryptographically relevant – in the specific sense of being able to break RSA-2048 quickly – for various time frames, from a short term of 5 years all the way to 30 years

Fraction of experts who indicated a certain likelihood in each indicated timeframe



Source: ***Michele Mosca, Marco Piani, Quantum Threat Time Line Report 2024.*** *https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/*

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

The most urgent: protect against HNDL

HARVEST NOW AND DECRYPT LATER (HNDL)

> Data is collected NOW for later decryption, when quantum computers are available.

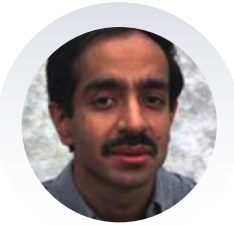
HNDL is already a threat to sensitive data that must remain confidential for many years.

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

How a 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)			
AES	**Symmetric key**	**Encryption**	**e.g. longer keys needed**
SHA-2, SHA-3	----------	Hash functions	**e.g. larger output needed**

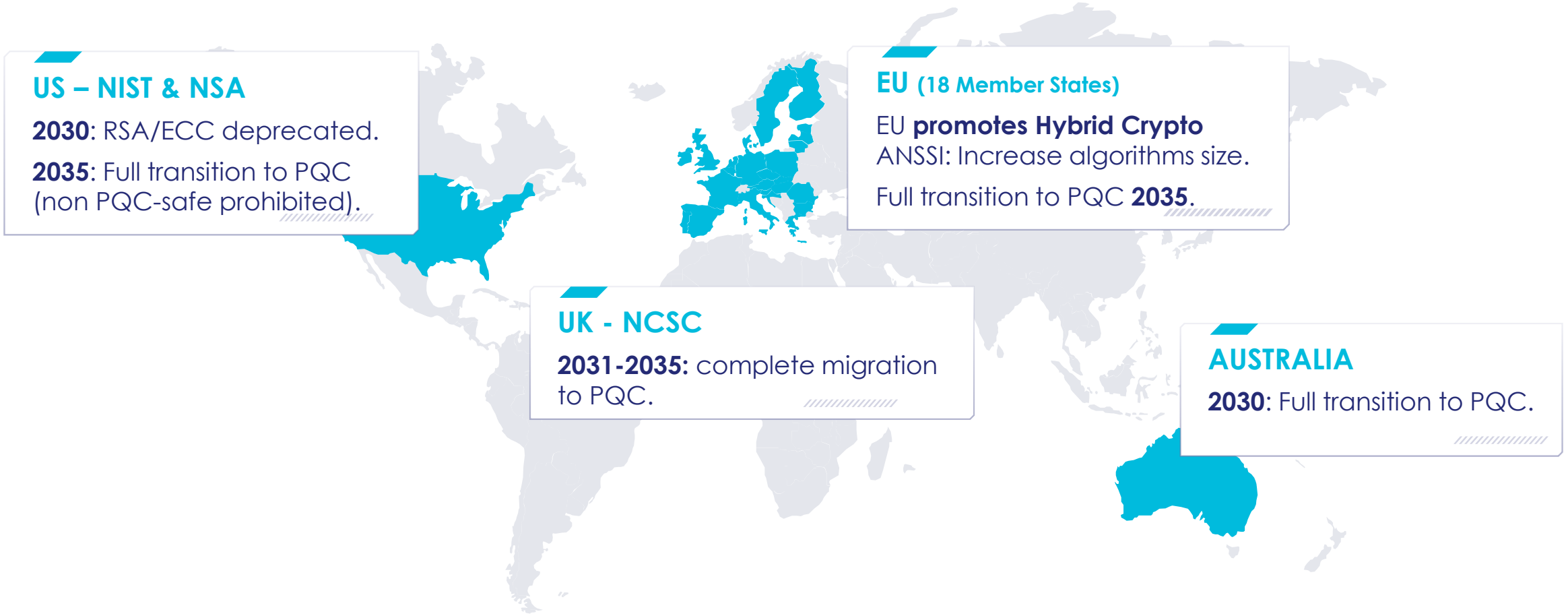
Peter **SHOR**



Lov **GROVER**

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

Transition recommended by national regulations



US – NIST & NSA

2030: RSA/ECC deprecated.

2035: Full transition to PQC (non PQC-safe prohibited).

EU (18 Member States)

EU **promotes Hybrid Crypto**
ANSSI: Increase algorithms size.

Full transition to PQC **2035**.

UK - NCSC

2031-2035: complete migration to PQC.

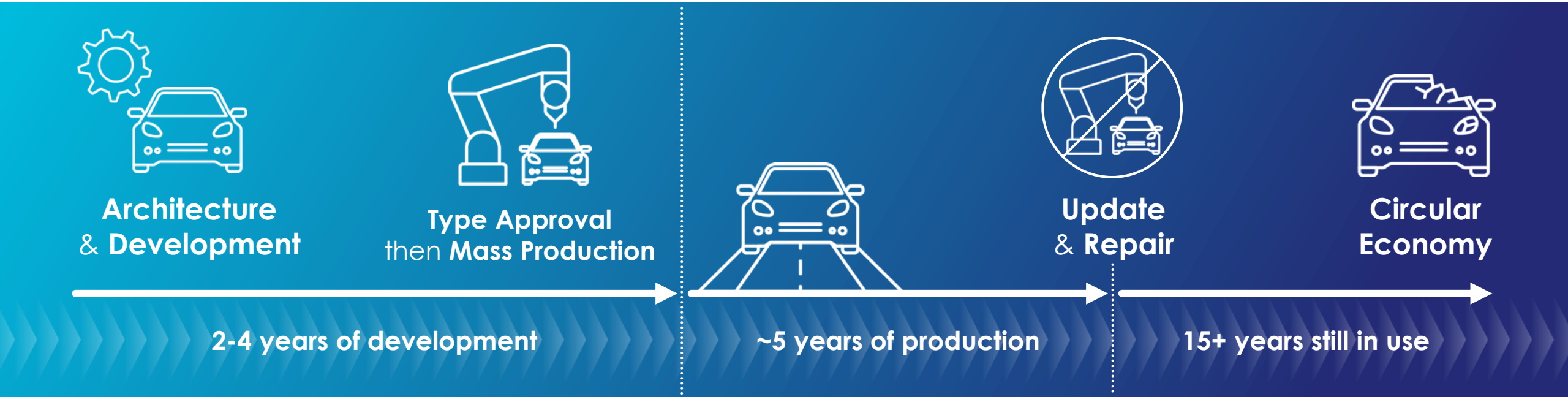
AUSTRALIA

2030: Full transition to PQC.

PQC-READY BY 2030 >> PQC-FULL BY 2035

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

The long development and lifespan of vehicles



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

Two Quantum Threats to Automotive Public-Key Cryptography

PUBLIC-KEY CRYPTOGRAPHY IS USED IN:

Vehicle PKI, cloud connectivity, OTA updates, Plug & Charge, V2X communications and secure boot.

HARVEST NOW, DECRYPT LATER

CONFIDENTIALITY

- Capture encrypted traffic today
- Decrypt sensitive data in the future

TRUST NOW, FORGE LATER

INTEGRITY & AUTHENTICITY

- Forge identities and messages
- Insert malicious firmware
- Bypass authentication mechanisms
- Compromise trust across vehicle fleets

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

Thales's recommendation: a step-by-step approach

AUDIT AND PROTECT YOUR DATA

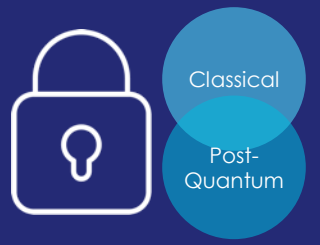
Assess risks and activity

Safeguard sensitive information

HNDL risk?

- **Adapt protocols and key management**
- **Adapt standards** when relevant

ANTICIPATE IN YOUR SOFTWARE & HARDWARE



Hybrid cryptography

Crypto Agility

- **Hybrid cryptography:** Combination of classical cryptographic algorithms with post-quantum algorithms in a single protocol or operation.
- **Crypto agility:** Ability of a system to support cryptographic evolution.

HNDL: Harvest Now Decrypt Later

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

GlobalPlatform Crypto Sub-Task Force

01 MONITOR
Regional developments and recommendations from agencies worldwide

02 ALIGN
Timelines, security levels, algorithms and hybrid constructions

03 GUIDE
Cryptographic Algorithm Recommendations
GP_TEN_053

CRYPTOGRAPHIC TRANSITION PATH

DEPRECATED	LEGACY USE	RECOMMENDED	HYBRID PQC	PQC ERA
Do not use	Until 2030	At least		At least
• DES / 3DES • SHA-1, SHA-224 • RSA-1024 • ECC < 224 bits • TLS v1.0 & TLS v1.1	• RSA-2048	• AES-128 / SHA-256 • RSA-3072 • ECDSA-256 • TLS 1.2 / TLS 1.3	• Classical + PQC algorithms	• AES-128 • SHA-256 • ML-KEM* • ML-DSA* • LMS / XMSS * NIST Category 3 or 5

Plan the transition from legacy cryptography to hybrid, then standalone PQC, while preserving interoperability.

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

GlobalPlatform Secure Element Committee

01 PROTECT
Critical management operations

- Application and content loading
- Key provisioning
- Management commands
- Software and configuration updates

02 EVOLVE
Cryptographic mechanisms

- Certificates and signatures
- Authentication and key establishment
- Secure channel protocols
- Hybrid and standalone PQC modes

03 SPECIFY
GlobalPlatform response

- Amd K SCP04: crypto-agile symmetric secure channel
- Amd O SCP12: PQC-capable asymmetric secure channel
- Amd P: PQC certificates and signatures
- Amd A: Confidential Card Content Management

Crypto agility must be designed into protocols, not added after deployment.

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

PQC Migration Requires an Ecosystem-Wide Effort

01	**ALGORITHMS** **NIST · ETSI · ISO**	PQC algorithms, security levels, hybrid schemes and migration guidance
02	**SECURE ELEMENT PROTOCOLS & APIs** **GlobalPlatform · Java Card Forum**	Secure channels, certificates, signatures, APIs and on-card mechanisms
03	**CONNECTIVITY & DIGITAL IDENTITY** **GSMA · ETSI · 3GPP · IETF**	eSIM, telecom, authentication and connected services
04	**AUTOMOTIVE INTEGRATION** **Automotive ecosystem ·OEMs ·suppliers**	Vehicle architectures, long-lifecycle products and deployment use cases

Crypto agility only works if specifications evolve consistently and remain interoperable across the ecosystem.

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

The PQC toolbox is becoming clearer

Hash-based
- Merkle signatures
- Sphincs

Multivariate
- Multivariate quadratic

Lattice-based
- NTRU
- Learning with errors
- Ring-LWE

Isogenies
- Supersingular elliptic curve isogenies

NIST PUBLISHED FIPS STANDARDS (August 2024)

- **Key Exchange Mechanism (KEM)**
  - **FIPS 203**: Module-Lattice-Based Key-Encapsulation Mechanism Standard (**ML-KEM**)
  - **HQC** selection (March 2025) as a backup for ML-KEM (standard expected in 2027)
- **Signature**
  - **FIPS 204**: Module-Lattice-Based Digital Signature Standard (**ML-DSA**)
  - **FIPS 205**: Stateless Hash-Based Digital Signature Standard (**SLH-DSA**)
  - To come by end 2026 **FIPS 206 FN-DSA** (Falcon)
  - More to come, (possibly non-lattice-based) selection is ongoing

Special Publication NIST SP 800-208 (October 2020) LMS/XMSS

- **Stateful Hash-Based Signature Schemes**
  - Specific constraints of implementation
  - Niche use cases such as **Firmware or Software signatures**

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

ML-KEM-768: Engineering Impact for Key Establishment

SECURITY ROBUSTNESS
NIST Category 3

eSE BENCHMARK CONTEXT
FULL-SW | ARM Cortex-M3 | 24 KB RAM

COMPARISON BASELINE
ECDH-256 = 1

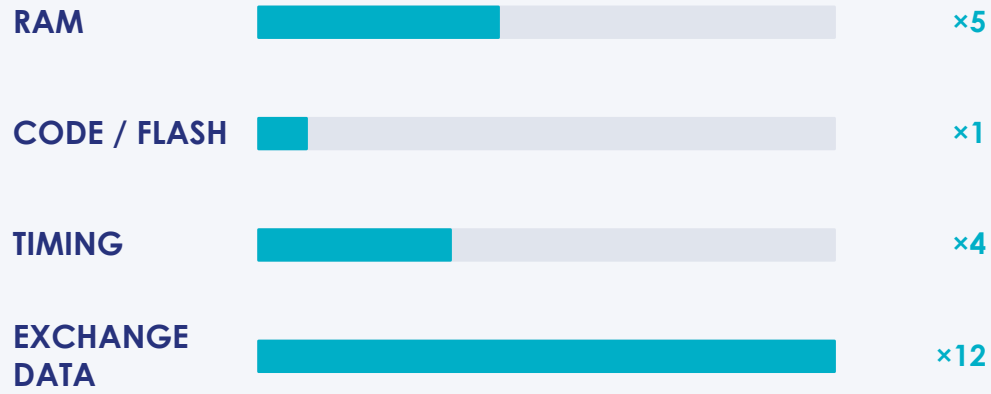
FUNCTION
KEM / shared-secret establishment

OBJECT SIZES

PUBLIC KEY	1,184 B
CIPHERTEXT	1,088 B
PRIVATE KEY	2,400 B

Main pressure: exchanged data, APDU/message sizing and temporary buffers.

INDICATIVE RATIOS VS ECDH-256



Ratios are benchmark-specific and depend on implementation, optimization and countermeasures.

ML-KEM is already viable on current Secure Element technology.

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

ML-DSA-65: Engineering Impact for Digital Signatures

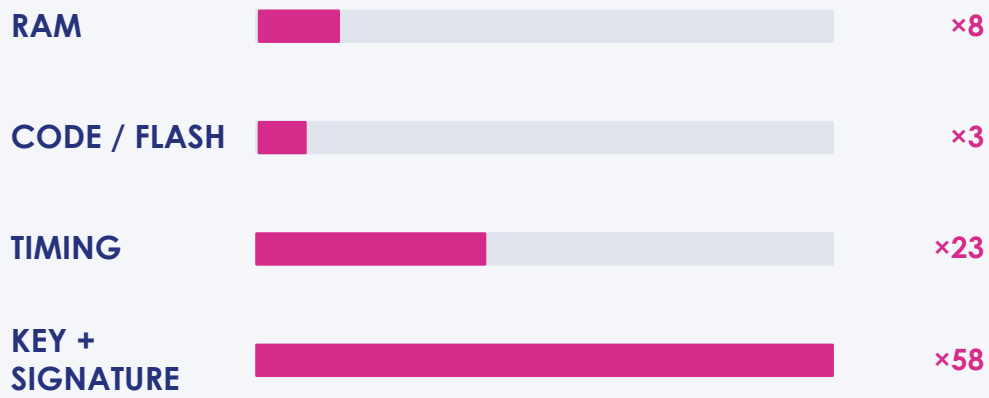
SECURITY ROBUSTNESS	eSE BENCHMARK CONTEXT	COMPARISON BASELINE	FUNCTION
NIST Category 3	FULL-SW | ARM Cortex-M3 | 24 KB RAM	ECDSA-256 = 1	Signature generation / verification

OBJECT SIZES

PUBLIC KEY	1,952 B
SIGNATURE	3,309 B
PRIVATE KEY	4,032 B

Main pressure: certificates, signed objects, NVM/Flash and verification flows.

INDICATIVE RATIOS VS ECDSA-256 SIGN / VERIF



Verification is significantly faster (~ x3 to x4 compared to ECDSA)

Ratios are benchmark-specific and depend on implementation, optimization and countermeasures.

ML-DSA is feasible on Secure Element technology, but signature generation remains demanding.

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

Secure Elements Enable Crypto Agility Across the Vehicle Lifecycle

SECURE KEY LIFECYCLE

- Secure key provisioning
- Manufacturing to operation
- Field renewal and replacement

SECURE CONTROL

- Protected execution of critical security services
- Controlled use of keys and cryptography
- Isolation of security functions

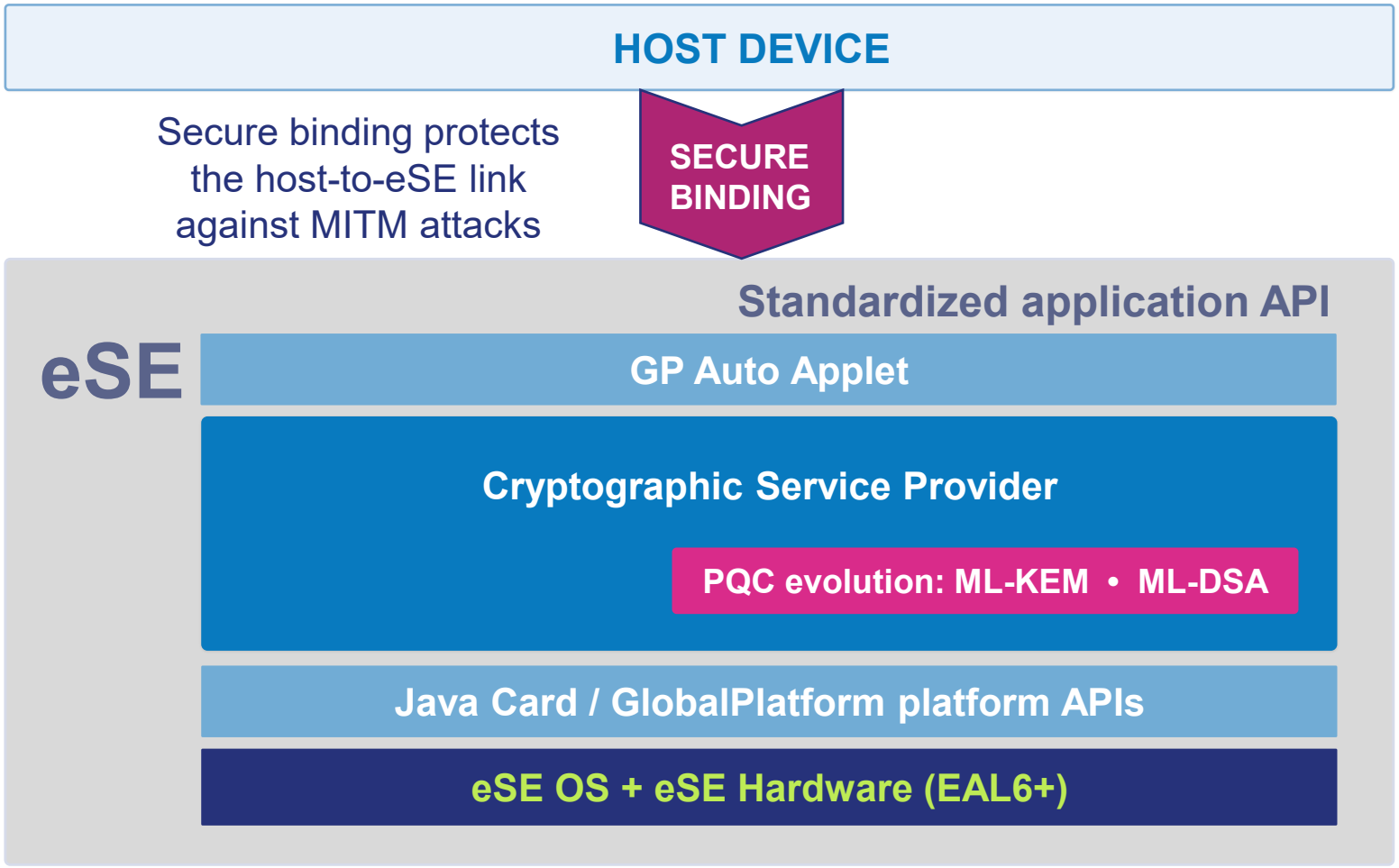
PROVIDE CRYPTO AGILITY

- Support for algorithm migration
- Secure OS and applet updates
- Long-term PQC readiness

Secure Elements turn specification agility into deployable automotive solutions.

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

Secure Element Architecture for Crypto Agility



STABLE APPLICATIONS, EVOLVING CRYPTOGRAPHY

- GP Auto Applet provides a standardized API
- GP Auto Applet relies on CSP interfaces
- CSP evolves to support ML-KEM and ML-DSA
- CSP avoids platform-specific certification of the GP Auto Applet

Architecture supporting cryptographic evolution

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

Key Takeaways

ENABLE CRYPTO AGILITY

> **AUDIT:**
Assess cryptographic dependencies across systems, protocols and lifecycles.

> **PRIORITIZE:**
- Protect long-lived data exposed to Harvest Now, Decrypt Later
- Protect critical trust mechanisms (secure boot, firmware updates)

> **PLAN THE TRANSITION:**
Define a phased migration path toward PQC

> **ANTICIPATE:**
Plan for additional memory, processing time, communication overhead and implementation resources

> **ENABLE CRYPTO AGILITY:**
Prepare deployed systems for cryptographic evolution
Consider embedded SE as a complement to HSMs and TrustZone

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales © 2023 THALES. All rights reserved.

THALES
Building a future we can all trust

Thank you

www.thalesgroup.com