Building Digital Trust For The Post-Quantum Era

THALES
Building a future we can all trust

Building Digital Trust For The Post-Quantum Era

With leading security agencies now urging organisations to complete their transition to post-quantum cryptography by 2030 for critical systems and no later than 2035 for broader infrastructures, it has become urgent to plan and execute quantum-safe migration strategies today.

The asymmetric cryptography that underpins today's digital identity solutions, mobile networks, cloud infrastructures, and critical data exchanges will be vulnerable to quantum attacks. The threat is no longer theoretical: adversaries have already adopted Harvest Now, Decrypt Later (HNDL) strategies to capture long-lived encrypted data today, anticipating the ability to decrypt it in the future. To maintain trust in a rapidly evolving digital world, organisations must begin their migration to quantum-safe cryptography now.

Thales made Post-Quantum Cryptography (PQC) a strategic priority across all product domains, combining deep cryptographic expertise, decades of sovereign security leadership and an extensive partner ecosystem. This cross-industry effort builds on more than 10 years of PQC research and standardisation activity and today positions Thales as one of the most active contributors to the global quantum-safe transformation.

Thales has chosen a comprehensive approach by not only integrating these required functionalities into its products, such as PQC algorithms with hybridisation capabilities, but also by contributing directly to the definition of NIST standards and by participating in various international forums and projects to prepare institutions and businesses for this threat.

TABLE OF CONTENTS

Driving Global PQC Standardisation

Thales plays a significant role in shaping the future of global cryptographic standards and actively contributes to the major post-quantum cryptography (PQC) standardisation forums.

1. Core PQC Standards and Migration Guidance

NIST & NCCoE

- **NIST:** Active participation in PQC working groups and algorithm evaluation, including the co-development of the Falcon digital signature algorithm selected by NIST for standardisation (FN-DSA, FIPS 206).
- **NCCoE:** Collaboration within NIST's Migration to Post-Quantum Cryptography project, contributing to reference architectures, cryptographic inventory frameworks, and HSM testing working groups.

2. Interoperability Layers

OASIS PKCS#11, GlobalPlatform, ISO

- **OASIS PKCS#11 Technical Committee:** Contribution to the evolution of the PKCS#11 standard—foundational for secure key storage, authentication tokens, and HSM-based cryptography—to support PQC algorithms and new key management models.
- **GlobalPlatform:** Chairmanship of the Cryptography Task Force, driving recommendations related to the integration and use of PQC algorithms in secure element and trusted execution environments.
- **ISO:** Contributions to the enhancement of the ISO 7816-x series, enabling quantum-safe cryptography support and interoperability at the card interface level.

3. Industry Ecosystem Standards

ETSI, GSMA, 3GPP, ICAO, Java Card

- **Telecom Industry (ETSI, GSMA, 3GPP):** Active leadership in global telecom PQC standardisation, shaping quantum-safe communication protocols, authoring GSMA guidance, and contributing to PQC-enabled eSIM and Remote SIM Provisioning specifications (including SGP.22 and SGP.32). Thales also contributed its PQC-based SUCI solution to 3GPP TR 33.703, with major mobile operators as co-signers.
- **Java Card Forum:** Leadership of PQC activities within the Technical Committee, defining a new interoperable Java Card API for ML-KEM and ML-DSA keys and algorithms. A new Java Card standard release (v3.3) with formal PQC support is planned for 2026.
- **ICAO:** Contribution to the ICAO Doc 9303 Technology Working Group, helping define quantum-safe specifications for next-generation electronic Machine Readable Travel Documents (e.g. ePassports and eID cards).
- **FIDO Alliance:** Co-chair of the PQC Study Group, supporting the integration of post-quantum cryptography into strong authentication standards.

4. Implementations

PQC Alliance

- **PQC Alliance:** Collaboration with industry, academia, and government to develop high-assurance reference implementations of standardized PQC algorithms and to support ongoing algorithm evaluation and validation.

Driving Global PQC Standardisation

Core PQC Standards and Migration Guidance

- NIST: PQC working groups and algorithm evaluation, co-development of Falcon digital signature algorithm
- NCCoE: Migration to Post-Quantum cryptography project collaboration

Industry Ecosystem Standards

- Telecom Industry (ETSI, GSMA, 3GPP): PQC communication protocols and eSIM specifications
- Java Card Forum: PQC API and 2026 standard
- ICAO: Quantum-safe specifications
- FIDO Alliance: PQC Study Group

Interoperability Layers

- OASIS PKCS#11: PQC cryptography support
- GlobalPlatform: Cryptography Task Force
- ISO: Quantum-safe updates to ISO 7816-x

Implementations

- PQC Alliance: Collaborative development and validation of standardized PQC algorithms

Through these engagements, Thales ensures that upcoming PQC standards remain technically robust, interoperable, and suitable for high-assurance mobile, identity, cloud and embedded environments.

Ecosystem Partnerships & Customer Enablement

A successful quantum transition requires collaboration. Thales partners with global mobile network operators, cloud providers, quantum technology companies, and integrators to support PQC adoption in real environments.

1. Ecosystem alliances & enablement: PQC Enablement for Enterprises

PQC Enablement for Enterprises

As PQC moves from planning to implementation, Thales enables customers to adopt quantum-safe cryptography without changing platforms. Luna HSMs and Thales High Speed Encryptors support quantum-safe and hybrid modes on production-proven systems, enabling PQC profiles for PKI, TLS, code signing, key management, and data-in-motion protection respectively, while preserving existing integrations and processes. What began as PQC starter kits has evolved into a broader enablement program, combining built-in capabilities with reference architectures, proven integration patterns, and ecosystem partner support to help teams move from pilots to repeatable deployment with confidence.

Quantum-Safe 360 Alliance

Thales acts as a core technology partner and founding member, together with IBM, Keyfactor, and Quantinuum, helping enterprises assess cryptographic exposure (including cryptographic inventories), plan migration strategies, and implement PQC-ready infrastructures.

PQShield collaboration

Co-development of the Falcon (FN-DSA, FIPS 206) algorithm and ongoing support for high-assurance PQC implementations.

2. Customer proof points & co-authored industry work

Wells Fargo – commercial PQC at scale

Thales worked with Wells Fargo and Quantinuum on what Wells Fargo describes as the first quantum-safe cryptography solution for commercial use, using quantum-entropy-hardened keys inside Thales Luna HSMs as part of a broader PQC program.

HSBC – cryptographic inventory as a PQC on-ramp

HSBC, InfoSec Global, and Thales jointly authored the Cryptographic Inventory: Deriving Value Today, Preparing for Tomorrow white paper, positioning crypto discovery and hygiene as a practical first step toward quantum-ready financial infrastructures.

3. Network and telecom quantum-safe initiatives

5G Quantum-Safe Networks (SK Telecom)

In partnership with SK Telecom, Thales conducted one of the world's first PQC trials on a commercial 5G standalone network using a PQC-enhanced SIM. This demonstrated quantum-safe subscriber identity protection against future Harvest Now, Decrypt Later attacks.

Canada's DIGITAL / NDEC – quantum-safe critical infrastructure

Through Canada's DIGITAL innovation cluster and Thales' National Digital Excellence Centre (NDEC), Thales is partnering with Quantum Bridge and Metropolitan Technologies to test and commercialise quantum-safe network encryption and key-distribution architectures for defence and critical infrastructure.

4. Secure elements, digital identity & sovereignty programs

PQC4eMRTD

A European-funded consortium uniting Thales, Infineon, CryptoNext, the Barcelona Supercomputing Center, and the Institute of Cooperative Law. The objective is to develop PQC protocols protecting the integrity and authenticity of personal data in electronic passports and future identity documents. This project strengthens European digital sovereignty and prepares the next generation of quantum-safe travel and identity documents.

Samsung security chip

Thales' secure operating system (OS) supports Samsung's security chip, the first embedded Secure Element (eSE) to integrate PQC, and winner of the *CES 2026 Best Cybersecurity Innovation Award*.

Thales leadership in shaping a trusted PQC ecosystem through standards, alliances, and partnerships.

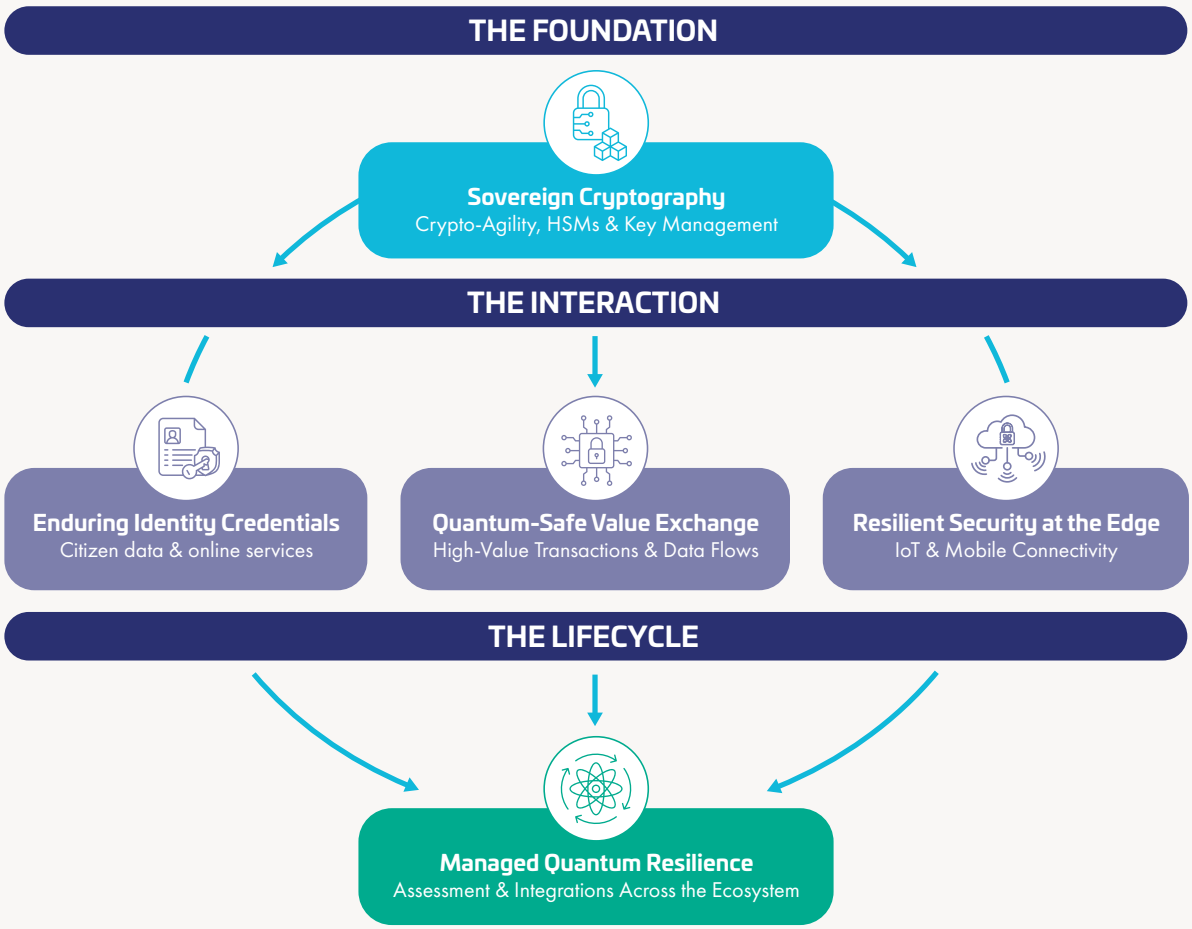
PQC-Ready Solutions Across Thales Technologies

Thales brings PQC out of the lab and into production by embedding quantum resistance and crypto-agility by design across its technology stack today. Here is a selection of our leading PQC-ready products (not an exhaustive list):

- **MultiApp v5.2 Premium PQC,** the first common criteria certified quantum-safe smartcard ever (ANSSI-certified at CC EAL6+), foundation for future-proof electronic passports and IDs.
- **Luna Hardware Security Modules (HSMs)** are among the first FIPS 140-3 Level 3 platforms to integrate NIST-standardised PQC algorithms ML-KEM, ML-DSA and LMS/HSS directly in firmware through partnership. This lets organisations run quantum-safe key management, TLS, PKI and code signing on the same Luna HSMs they already rely on in production.
- **High Speed Encryptors (HSE)** are one of the first commercially deployed, standards-aligned quantum-resistant network encryption solutions, using FPGA-based, crypto-agile architectures to deliver hybrid PQC/classical protection for data in motion at Layers 2–4, with optional QKD and QRNG integration for the most demanding networks.
- **Quantum-safe secure elements (eSE)** protecting identities and credentials inside mobile, automotive and IoT devices.
- **Cryptosmart Mobile**, the world's first sovereign solution capable of encrypting mobile voice communications with post-quantum algorithms - already proven in operational field trials.

These solutions combine advanced PQC algorithms with Thales' longstanding expertise in countering physical and logical attacks, ensuring secure implementation even in constrained embedded environments. We will delve into each of them in the coming chapters.

Thales PQC vision is developed in 3 layers: **The foundation** setting the base of sovereign Cryptography, **The Interaction**, protecting Identities, transactions and securing connections at the edge, and finally **The lifecycle**, assessing the ecosystem evolution.



Next Steps in PQC Readiness

Commitment to a Quantum-Safe Future

Global standards and regulatory guidelines have reached the maturity required for organisations to formally evaluate and mitigate their quantum exposure. With the first PQC standards now published and implementation guidance accelerating across jurisdictions and industries, teams can move from awareness to structured testing and program planning. Companies should launch the multi-year transformation programs necessary to secure their long-term digital integrity. The urgency is not tied to predicting a single "Q-Day," but to risks such as the Harvest Now, Decrypt Later reality: data captured today may be exposed in the future, making your confidentiality horizon the real deadline.

The critical path begins with a comprehensive inventory, risk assessment, and the prioritisation of assets, followed by the implementation of future-proof, agile designs and strategic vendor engagement. In practice, with the support of our consultancy teams, that means proving where cryptography is actually used (applications, PKI, certificates, protocols, signing, and data flows), standing up a PQC test environment to validate performance and interoperability, and turning results into a prioritized migration backlog and architecture requirements.

Because application and PKI changes take time, many organisations also reduce exposure in parallel by strengthening protection on the most sensitive data flows in transit while broader migrations progress.

With deep involvement in global standardisation, leadership in sovereign PQC research, and a portfolio of operational quantum-safe solutions, Thales is fully committed to ensuring trust in the digital world — today and for the quantum era ahead.

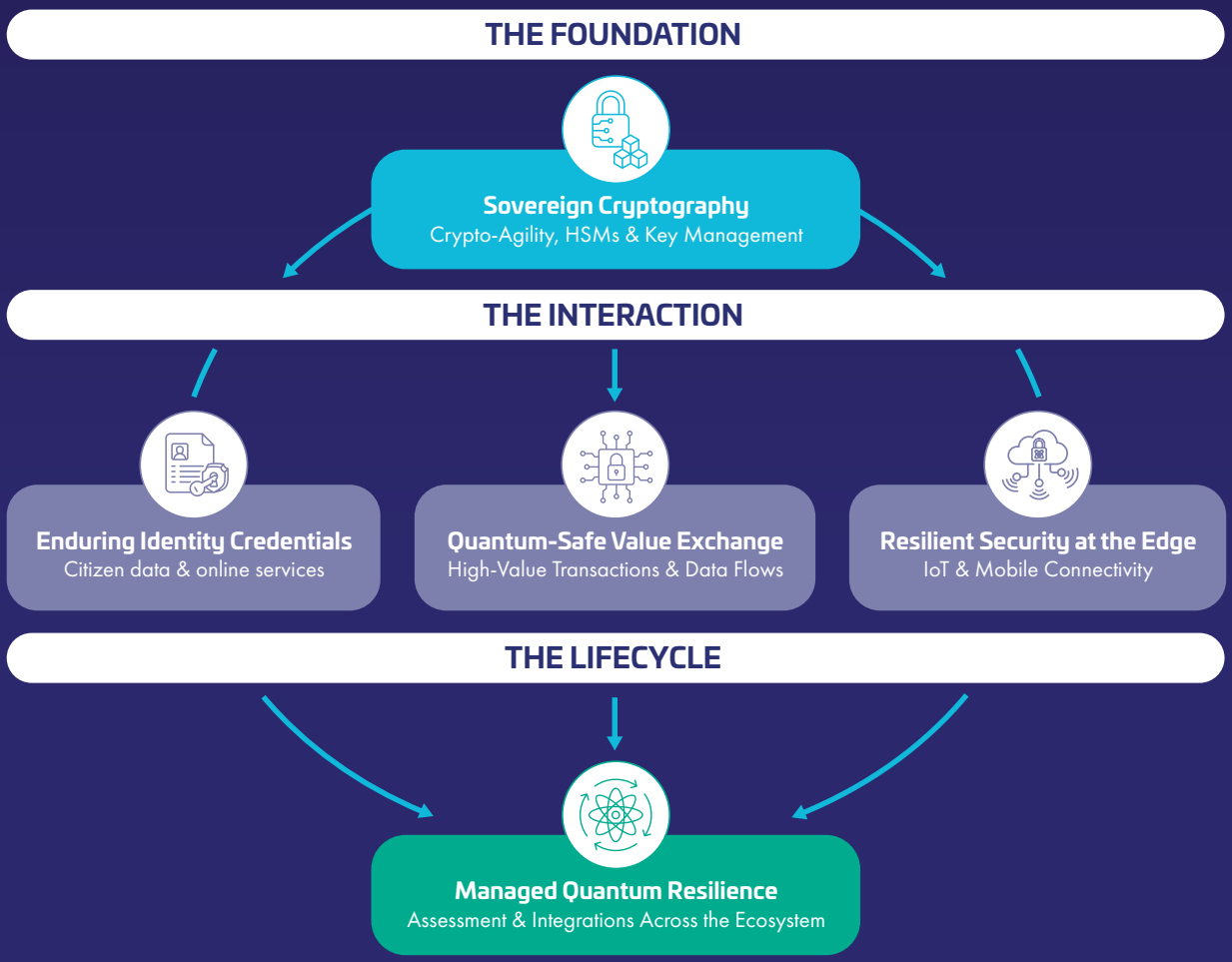
APPENDIX

This appendix complements the main Post-Quantum Cryptography (PQC) paper by providing detailed technical context, solution descriptions, and illustrative use cases across Thales' quantum-safe portfolio.

It brings together reference architectures, product capabilities, sector-specific applications, and migration services that demonstrate how crypto-agility and PQC readiness are implemented in practice—across data protection, identity, connectivity, embedded systems, mobile networks, and critical infrastructures.

The content is intended as supporting material for readers seeking deeper insight into how organisations can secure keys, identities, and data flows today while executing a controlled transition from classical cryptography to hybrid and fully post-quantum architecture.

Thales' conception of the PQC development and vision breaks down into three levels (foundation, interaction and life cycle) and five sections. We will discuss each of those sections.



Sovereign Cryptography - Crypto-Agility, HSMs & Key Management

Secure keys and cryptographic operations, identities, and critical data flows across the networks today, with a controlled migration path to PQC.

Thales provides high-assurance, crypto-agile protection for data, identities and networks across digital business, critical infrastructure and connected services. With hardware, software, on-premises, hybrid and cloud-delivered solutions, the company helps organisations discover and classify sensitive data, protect it at rest, in motion and in use, and maintain end-to-end control of keys and cryptographic processes. From key generation inside certified HSMs through encryption of data as it moves across the network, and policy enforcement across on-premises, hybrid and multi-cloud environments, Thales' products are designed for crypto-agility: algorithms, key lengths and policies can evolve without redesigning applications or networks. This underpins Thales' quantum-safe portfolio, which already delivers PQC capabilities in shipping products and provides a clear migration path from today's classical public-key cryptography to hybrid and, over time, fully post-quantum architectures.

Luna Hardware Security Modules (HSMs)

Thales Luna HSMs are FIPS 140-3 Level 3 validated, certified to Common Criteria EAL4+ and classified NATO Secret, with support for eIDAS Protection Profile EN 419 221-5. Luna HSMs provide a crypto-agile, quantum-safe hardware root of trust for a wide range of applications from the CipherTrust Data Security Platform and broader Thales solutions, to mobile and telecom workloads. Luna HSMs are among the first FIPS 140-3 Level 3 platforms to integrate NIST-standardised PQC algorithms directly in firmware, as well as extending crypto-agility to support new or sovereign algorithms. Support for ML-KEM and ML-DSA, together with quantum-safe hash-based signatures such as LMS/HSS and existing classical algorithms, enables hybrid modes so organisations can leverage PQC for key management, TLS/SSL, key exchange, PKI and code signing with minimal change to applications. PQC capabilities are available on the same Luna HSMs already in production, with the option to use external entropy sources such as quantum random number generators (QRNGs). By reusing existing integrations and tooling, organisations in long-lived, regulated environments can choose their own path to being quantum-safe – whether by starting with hybrid deployments or moving directly to full PQC solutions. Thales is working on its next-generation HSM for the quantum era. It is designed to be quantum-safe from the ground up, with a new PQC-ready crypto processor - custom-designed by Thales - to ensure high-efficiency operation, crypto agility, supply chain sovereignty while being highly scalable and multi-tenant with strong security isolation.

High Speed Encryptors (HSE)

Thales High Speed Encryptors (HSE) provide quantum-ready protection for data in motion across enterprise, government, defence and critical infrastructure networks. Designed to drop into a wide range of network architectures, from simple point-to-point links to meshed, hub-and-spoke and SD-WAN topologies, HSE is available as both physical and virtual platforms and delivers line-rate encryption at Network Layers 2, 3 and 4. PQC and hybrid modes have been built into certified HSE platforms for several years, so customers can introduce quantum-resistant protection without adding external components or redesigning their networks.

Building on a long track record in high-assurance WAN and data-centre protection, HSE hardware uses crypto-agile, FPGA-based designs so quantum-safe capabilities can be enabled and updated via in-field firmware and policy changes. With NIST PQC algorithms implemented, HSE supports the transition from today's classical environments to PQC-ready networks, enabling hybrid classical/PQC tunnels so organisations can add quantum-safe protection while maintaining interoperability with existing devices and services.

HSE appliances carry a broad set of third-party validations, including FIPS 140-3 Level 3 validation (Level 1 for virtual models), Common Criteria EAL4+ certification, and approvals for government, defence and critical-infrastructure use via NATO NIAPC and the U.S. DoDIN APL, providing proven drop-in protection for traffic across public and private networks. Transport Independent Mode (TIM) delivers out-of-band key material using NIST-specified key-derivation functions, separating key delivery from the data plane to help mitigate Harvest Now, Decrypt Later threats. Optional Quantum Key Distribution (QKD) integrations and the ability to use QRNG-sourced entropy for key generation give customers additional design choices to align data-in-motion security with their preferred quantum-safe strategy.

CipherTrust Data Security Platform and Data Security Posture Management

The CipherTrust Data Security Platform provides a data-centric foundation for PQC adoption, with Data Security Posture Management (DSPM) as a core capability. DSPM in CipherTrust continuously discovers, classifies and protects sensitive data across databases, files, applications, cloud services and SaaS environments, to reduce data security risk. The platform centralises key management, policy enforcement, tokenisation, encryption, and supports quantum-safe key establishment in TLS servers and application environments using KEM-based key exchange, while continuing to rely on Luna HSMs as the quantum-ready hardware root of trust for key generation, storage and critical cryptographic operations. This gives organisations a crypto-agile control plane to inventory cryptography, rotate keys, and re-encrypt sensitive data as PQC and hybrid algorithms are adopted.

Identity and Access Management

Thales Identity and Access Management (IAM) solutions extend quantum-ready security principles to digital identities and access control, addressing both current identity-based threats and the long-term cryptographic risks introduced by quantum computing. In modern zero-trust architectures, IAM must ensure trust not only in users, but also in the cryptographic mechanisms that underpin authentication, federation and secure access.

Thales IAM roadmaps, including PQC-ready authentication devices, hybrid-cloud credentials and identity management systems, are designed to accommodate the evolution of quantum-safe FIDO, PKI and TLS profiles, ensuring that passwordless authentication can be progressively aligned with post-quantum cryptographic foundations as standards mature. This approach enables organisations to adopt phishing-resistant authentication today, while preparing for future PQC-enabled authentication devices and protocols.

PQC Enablement and Migration

Thales post-quantum readiness has evolved from isolated pilots into a broader enablement and migration programme. With PQC available in current Luna HSM firmware and well established in Thales High Speed Encryptors, and expanding to the rest of the portfolio, customers can enable quantum-safe and hybrid modes on their existing platforms in both non-production and production environments. Security and architecture teams can trial standardized algorithms such as ML-KEM, ML-DSA, LMS/HSS and hybrid profiles for PKI, TLS, code signing, key management and network encryption using existing integrations, tools, and operational processes, then roll validated configurations into deployment. Thales complements this with optional services for quantum risk and impact assessment, cryptographic posture review, and solution architecture, pilots and phased rollout, helping organisations introduce PQC in practical, low-risk steps. Together, these products, services and ecosystem partnerships mean Thales is helping customers reduce exposure now by actively enabling them to deploy quantum-safe, crypto-agile architectures today.

Enduring Identity Credentials: citizen data & online services

Trust That Outlasts the Quantum Shift

Modernize identity issuance with crypto-agile solutions, secure credentials and long-lived trust controls for regulated access and authentication.

Post-Quantum Cryptography intersects with multiple aspects related to eGovernment services:

Secure Communication

PQC algorithms can be employed to secure communication channels between citizens and government servers. This ensures that data transmitted during online interactions, such as filling out forms or submitting documents, remains confidential and cannot be intercepted or tampered with by malicious actors.

Data Integrity

By implementing PQC algorithms for digital signatures, eGovernment services can verify the authenticity and integrity of data exchanged between parties. This helps prevent unauthorized modifications to government records and ensures that only legitimate transactions are accepted.

Long-Term Security

As eGovernment services often involve storing sensitive data for extended periods, it's crucial to employ cryptographic algorithms that remain secure in the face of future advancements in computing technology. PQC algorithms are designed to withstand attacks from both classical and quantum computers, providing long-term security for government systems and data.

Compliance to Standards and Regulations

Governments worldwide are increasingly recognizing the importance of cybersecurity in eGovernment initiatives. Many regulatory bodies and standards organisations are beginning to mandate the use of PQC algorithms for securing sensitive data and communications.

Research and Development

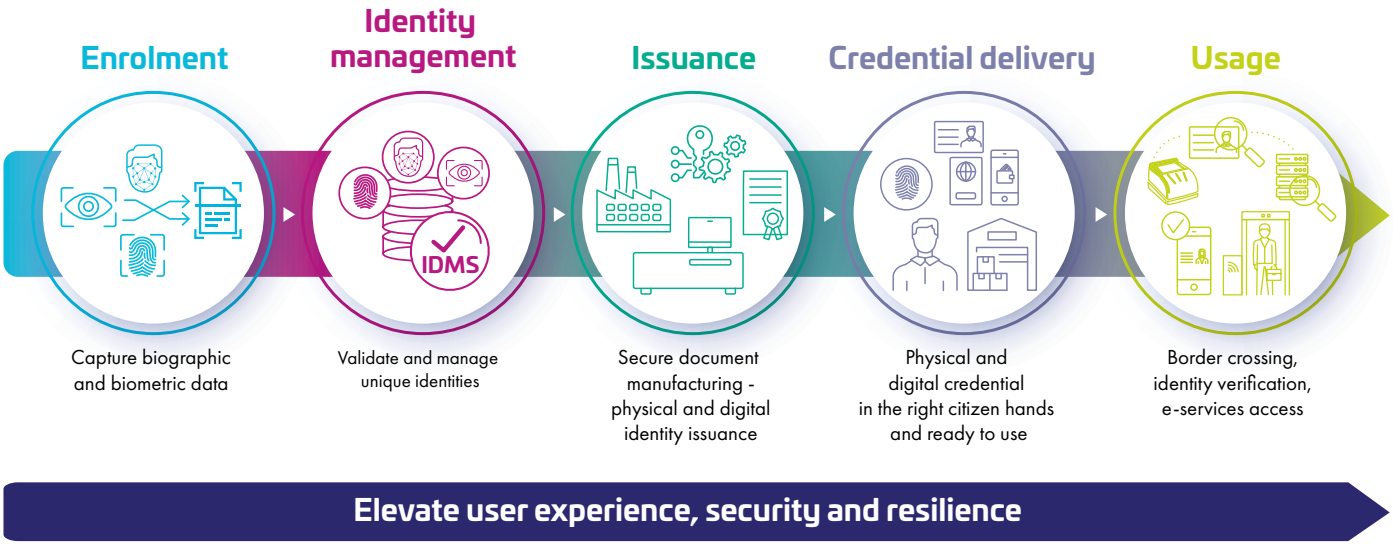
Government agencies, companies, and research institutions are actively involved in the research and development of PQC algorithms and protocols. By investing in cutting-edge cryptographic research, governments can stay ahead of emerging threats and ensure that eGovernment services remain resilient against future cryptographic attacks.

A dynamic approach

Post-Quantum Cryptography is going to play a vital role in safeguarding eGovernment services against evolving cyber threats and ensuring the confidentiality, integrity, and authenticity of sensitive data exchanged between citizens and government entities. As quantum computing technology continues to advance, integrating PQC into eGovernment systems will become increasingly critical for maintaining trust and security in digital government interactions.

With the release of the groundbreaking MultiApp 5.2 Premium PQC product, Thales is making available to its customers a first major step on the way towards a quantum-safe world. Backward compatible with conventional algorithms from the pre-quantum era, this new product features quantum-safe capabilities designed to be used for government applications having use cases corresponding to the European regulation on Digital Signature (eIDAS).

Capitalizing on Thales' expertise, the MultiApp 5.2 Premium PQC can be bundled within a complete solution suite where all services can be made quantum-safe, from the Enrolment step to Civil Registry verifications and Usage in the field.



The next major step for our design team is to continue its active contributions to the evolution of the ICAO DOC 9303 standard, major interoperable specification in the eDocument area in order to be able to offer as quickly as possible new products and solutions integrating a fully interoperable way of managing digital identities. The ICAO NTWG body is actively working on the matter and we can reasonably expect that a new specification, ready to be used in new product developments, will be released within the next 24 months.

Quantum-Safe Value Exchange: High-Value Transactions & Data Flows

Protect payment ecosystems and high-value signing by strengthening cryptographic controls across transaction flows and digital asset platforms.

Quantum threat is considered in the banking card environment, not with the same urgency as in other sectors: we are not in the context of Harvest Now, Decrypt Later. Nevertheless, this threat is actively monitored and included within the roadmap depending on the use of the banking cards.

A wide majority of our customers worldwide are using Online Authentication, based on symmetric algorithm. So, to address to the quantum threat, products supporting AES with different key sizes are available, migration plans are in place, adapted to the different regions and customers. Focusing on the Online Authentication, our quantum migration is eased by the fact that we are relying on existing and well-known symmetric algorithm. This is really a point that sets the payment card market apart from the others.

Some other customers are considering an additional use case for resilience, the ability to perform an offline transaction, for example in case of network outage. In this context, the computation is based on asymmetric algorithms, current ones are considered weak against quantum computation. A change to PQC resistant algorithm is needed. First evaluations of the technical feasibility and integration had been conducted with good results: no technical blocking points are foreseen. A noticeable point is that payment cards are embedded products, and we must keep it in mind when developing asymmetric algorithm to reach acceptable performance and memory consumption. In addition, as the products are in the field for some years, we must base our solution on robust algorithm design and implementation. We are moving on with our different partners on this topic, on a more mid-term implementation.

Beyond payments, the quantum security challenge extends across the entire financial infrastructure, encompassing interbank messaging systems, clearing and settlement networks, and digital central bank operations. Institutions such as central banks and market infrastructures face systemic risks where a single cryptographic weakness can cascade across the financial ecosystem. Thales plays a pivotal role here, providing quantum-resistant hardware security modules (HSMs), secure key management frameworks, and expertise in regulated environments to enable a trusted post-quantum transition at the core of financial operations. By partnering with financial authorities and technology providers, Thales contributes to building quantum-safe communication channels and transaction validation flows—ensuring continuity, interoperability, and resilience from commercial banks to central banks in a future-proof cryptographic foundation.

Resilient Security at the Edge

Embed crypto-agility and PQC readiness at scale across eSIM and large automotive and IoT fleets with repeatable rollout patterns.

Thales provides secure solutions for a connected world, focusing on hardware, embedded software, and cloud-based platforms that protect identities, credentials and network access in billions of devices. As the SIM, eSIM and embedded Secure Element (eSE) form the root of trust in mobile networks and IoT ecosystems including automotive, their security must evolve to withstand the emerging capabilities of quantum computing.

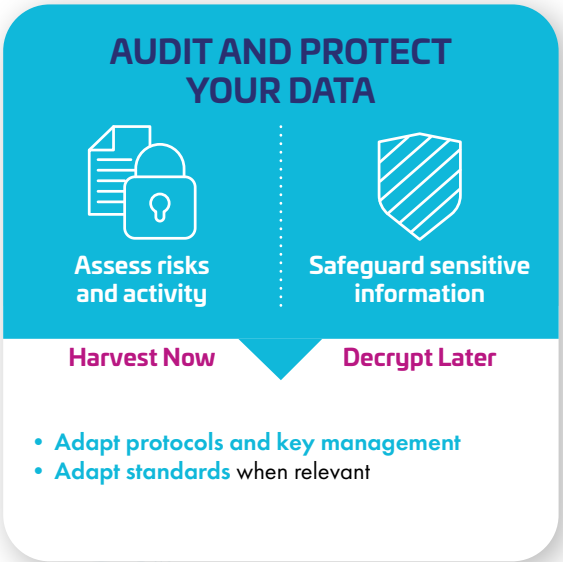
Quantum threats such as Harvest Now, Decrypt Later attacks require mobile ecosystem actors to adopt crypto-agile, quantum-resistant foundations. Thales is therefore implementing a comprehensive strategy to ensure long-term resilience across SIM and eSIM technologies, mobile devices, IoT modules, automotive IoT, and the broader connectivity ecosystem to reach full PQC deployment including digital signature algorithms.

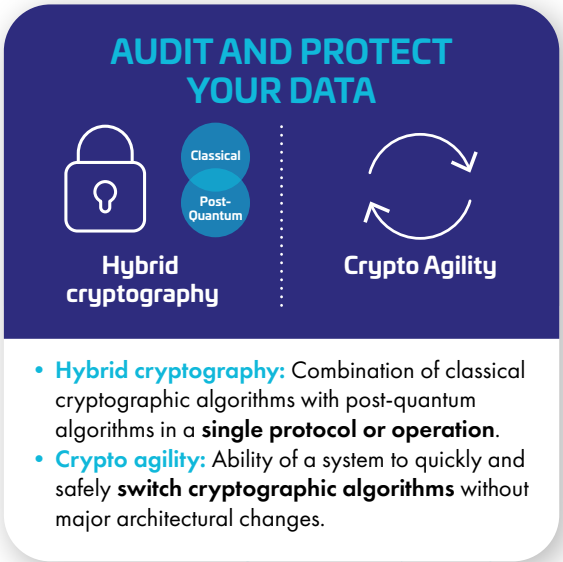
Towards Quantum Resistant Mobile Connectivity

Securing mobile connectivity against quantum threats requires coordinated upgrades across multiple layers:

- **Crypto-agility** built into SIM, eSIM and eSE operating systems, enabling algorithm updates even after deployment.
- **Integration of NIST-approved PQC algorithms**, including CRYSTALS-Kyber (ML-KEM) and ML-DSA, into authentication, key exchange and identity concealment mechanisms.
- **Enhanced hardware capabilities** to support the computational demands of PQC.
- **Collaboration across the ecosystem**—including MNOs, NEPs, OEMs and government agencies—to ensure end-to-end protection.
- **Security upgrades for the entire data exchange chain:** between the SIM/eSIM, the device, the core network, subscription management platforms and service providers.

This approach ensures mobile networks remain secure, standard-aligned and compliant as quantum computing advances.





PQC-Ready Secure Elements for Consumer, IoT and Automotive Devices

Thales is advancing quantum-safe connectivity through four core pillars:

Crypto-Agile Operating Systems

Thales embeds crypto-agility into SIM, eSIM and eSE OS designs, allowing:

- Remote loading of new PQC algorithms (via OTA)
- Transition from classical to hybrid and PQC-only methods
- Alignment with GSMA, ETSI and NIST recommendations
- Reduced lifecycle and retrofitting costs for operators and OEMs
- Enable immediate corrective security actions for embedded products already on the field.

Post-Quantum Algorithms on the SIM and eSIM

PQC is progressively being integrated into the SIM and eSIM stack, enabling:

- PQC-based SUCI identity concealment
- Hybrid key exchanges merging classical (RSA/ECC) and quantum-safe (ML-KEM) schemes
- PQC resistant mutual authentication with 5G networks
- Future ML-DSA-based digital signatures (per NIST FIPS 204)

PQC-Ready Secure Elements for Consumer, IoT and Automotive Devices

The next generation eSE integrates:

- PQC libraries optimized for low power and compact design
- Crypto-agile OS capable of upgrading algorithms post - deployment
- Hardware acceleration to support large PQC key sizes

This ensures long-lasting confidentiality, integrity, and authenticity for sensitive applications across consumer devices and industrial systems.

PQC-Ready Subscription Management Platform

- **Securing the eSIM Profile Package Download (PPD)** by protecting highly sensitive cryptographic material whose compromise would enable future decryption of user communications
- **Hybrid post-quantum cryptography at the transport layer,** combining established classical algorithms with quantum-resistant algorithms to secure SM-DP+ communications over untrusted networks
- Mitigation of HNDL attacks, ensuring that intercepted **profile downloads remain cryptographically protected** against future quantum adversaries
- **Compatibility with existing deployed eUICCs,** allowing quantum-resistant protection to be activated through **LPA updates** without requiring immediate hardware replacement
- **Progressive extension toward end-to-end PQC protection,** targeting the full eSIM profile download protocol through industry alignment and upcoming SGP.22 evolutions
- Foundation for **next-generation quantum-resistant SM-DP+** and eUICCs, enabling true end-to-end post-quantum security across the eSIM ecosystem

Flagship Achievements — Advancing Quantum-Safe Mobile Connectivity

Samsung Systems LSI and Thales — Establishing a New Baseline for Embedded Post-Quantum Security

Samsung System LSI and Thales jointly launched the **world's first embedded Secure Element (eSE)** integrating **hardware-based Post-Quantum Cryptography**, powered by a Thales operating system and PQC library.

This solution delivers:

- Hardware accelerated PQC up to **18× faster** than software-based approaches
- Ultra-efficient architecture suitable for large-scale consumer and IoT deployments
- Native protection against classical and quantum threats, including HNDL
- Compliance with **CC EAL6+** and NIST PQC standards

This achievement demonstrates that PQC is no longer limited to critical infrastructures - **it can now be embedded directly into mass-market connected devices**, ensuring long-term resilience.

Thales x SK Telecom — First PQC-Protected Subscriber Identity in a Commercial 5G SA Network

Thales and SK Telecom were the first to demonstrate PQC-protected SUCI generation on a commercial 5G standalone network using a Thales PQC-enabled SIM.

The trial confirmed:

- Hybrid ML-KEM/classical key exchanges
- Quantum resistant identity concealment
- Operational performance under real and end-to-end authentication flows
- Enhanced long-term user privacy

This pioneering result validated the feasibility of PQC deployment in live operator environments.

Cryptosmart Mobile — Post-Quantum Protection for High Sensitivity Communications

Thales' secure mobility solution, Cryptosmart Mobile, demonstrated the first PQC-secured mobile voice calls, integrating CRYSTALS-Kyber into end-to-end encrypted communication channels.

This solution provides:

- Quantum-resistant protection for calls, messages and mobile data
- Device-level security certified for NATO use
- Deployability today for government and high security missions

Cryptosmart demonstrates that PQC-secured communications are no longer conceptual - they are operational.

Building End-to-End Quantum-Safe Connectivity

Thales' **post-quantum cryptography (PQC) patent portfolio** enables efficient optimisation and high performance across a broad range of chipsets. Through Samsung's S3SSE2A-class platform capabilities—including clock frequency, memory resources, and dedicated hardware accelerators such as SHA-3 and CRYSTALS co-processors—Thales delivers best-in-class PQC software implementations, combining minimal footprint with high cryptographic performance.

These achievements underscore Thales' unique ability to deliver **quantum-resilient security at scale** across the entire mobile ecosystem, from embedded hardware and SIM technologies to 5G network infrastructure and secure digital applications—laying a solid foundation for the post-quantum future of trusted connectivity.

Managed Resilience: Assessment and Integration across the ecosystem

Your Expert Path to PQC

Execute PQC as a controlled program with discovery, validation, integration support, and operational runbooks.

As quantum computing advances, today's public-key cryptography is becoming fundamentally vulnerable, exposing long-lived data (such as state secrets, intellectual property, and personal records), critical infrastructures, and high-value transactions to future decryption through Harvest Now, Decrypt Later attacks. To address this strategic threat, Thales offers a comprehensive Post-Quantum Cryptography (PQC) Migration service that bridges cyber consulting and cyber integration, enabling organisations to move from risk assessment to the deployment of quantum-resilient architectures.

- Thales' approach begins with a detailed cryptographic and data inventory across IT, OT, cloud, and applications, mapping all cryptographic algorithms, protocols, libraries, keys, and certificates to data sensitivity, regulatory constraints, and business criticality. This allows us to identify "crypto technical debt" and prioritize systems and data at highest risk.
- The company then performs a quantum impact and risk analysis per asset, assessing the threat horizon, data shelf-life, and potential operational, financial, and regulatory impact of a future quantum break, while also evaluating the performance and architectural implications of PQC adoption (larger keys, ciphertext sizes, and hybrid crypto patterns).
- Based on this analysis, Thales delivers a tailored, multi-year PQC migration roadmap and crypto-agility strategy that prioritises high-risk systems, high-value data and critical applications. We define crypto-agile policies, governance and standards to avoid fragmented, ad-hoc changes and ensure a sustainable, future-proof adoption of PQC.

Thales Quantum-Safe Migration Services

Quantum Readiness Strategy Offer

Quantum Risk Awareness

Cryptographic Algorithm Inventory
Tool : Crypto Inventory

Quantum Impact Analysis
Methodology: Risk Analysis

Quantum Risk Reduction Roadmap

Cyber Integration Services

Quantum-resistant security architecture advisory

Quantum-resistant cyber solution integration

On the integration side, Thales cyber services teams support the design and deployment of quantum-resistant security architectures through the management of solutions covering key management, identity, network security, data-at-rest, and data-in-motion protection, with architecture patterns for hybrid deployments (classical and PQC) to manage transition risk and maintain interoperability.

- Thales quantum-ready solutions are integrated — including Luna HSMs, CipherTrust Data Security Platform key management , High Speed Encryptors network encryption, IAM, and secure gateways — into the customer's existing IT/OT environment, and we also integrate PQC-compliant and hybrid solutions from leading technology partners (PQC libraries, crypto-agile gateways, application stacks), including performance validation and regression testing.
- For products and systems requiring advanced cryptographic mechanisms, we provide post-quantum architecture expertise to design secure, future-ready solutions. Our approach covers embedded components, infrastructure, and administrative environments to ensure cyber resilience today and tomorrow through crypto-hybridisation, re-encryption, and crypto-agility techniques. We also offer advanced evaluation services for software and hardware cryptographic implementations to validate the robustness of security products prior to certification and/or deployment.
- Finally, we support the operationalisation of the new cryptographic environment, defining and implementing new procedures for key lifecycle, certificate management, and crypto policy enforcement in a PQC context, and we accompany customers through pilots, staged rollouts, and coexistence phases to minimize disruption while ensuring compliance and auditability.

With deep expertise in cyber consulting, cryptography, and integration for high-security sectors (defence, finance, transport, critical infrastructure), Thales' proven portfolio of quantum-ready and crypto-agile security products, and co-development of the NIST-standard Falcon PQC algorithm, we enable operators of essential services to build a crypto-agile, quantum-resilient security architecture that protects long-term confidentiality, integrity, and compliance in the post-quantum era.

Crypto Agile Strategy for Protecting Data Against the Quantum Threat

THALES

Building a future we can all trust

Thalesgroup.com