Strengthening Trust: Thales Approach to Post-Quantum Cryptography in Digital Identity and Security

THALES
Building a future we can all trust

Strengthening Trust: Thales Approach to Post-Quantum Cryptography in Digital Identity and Security

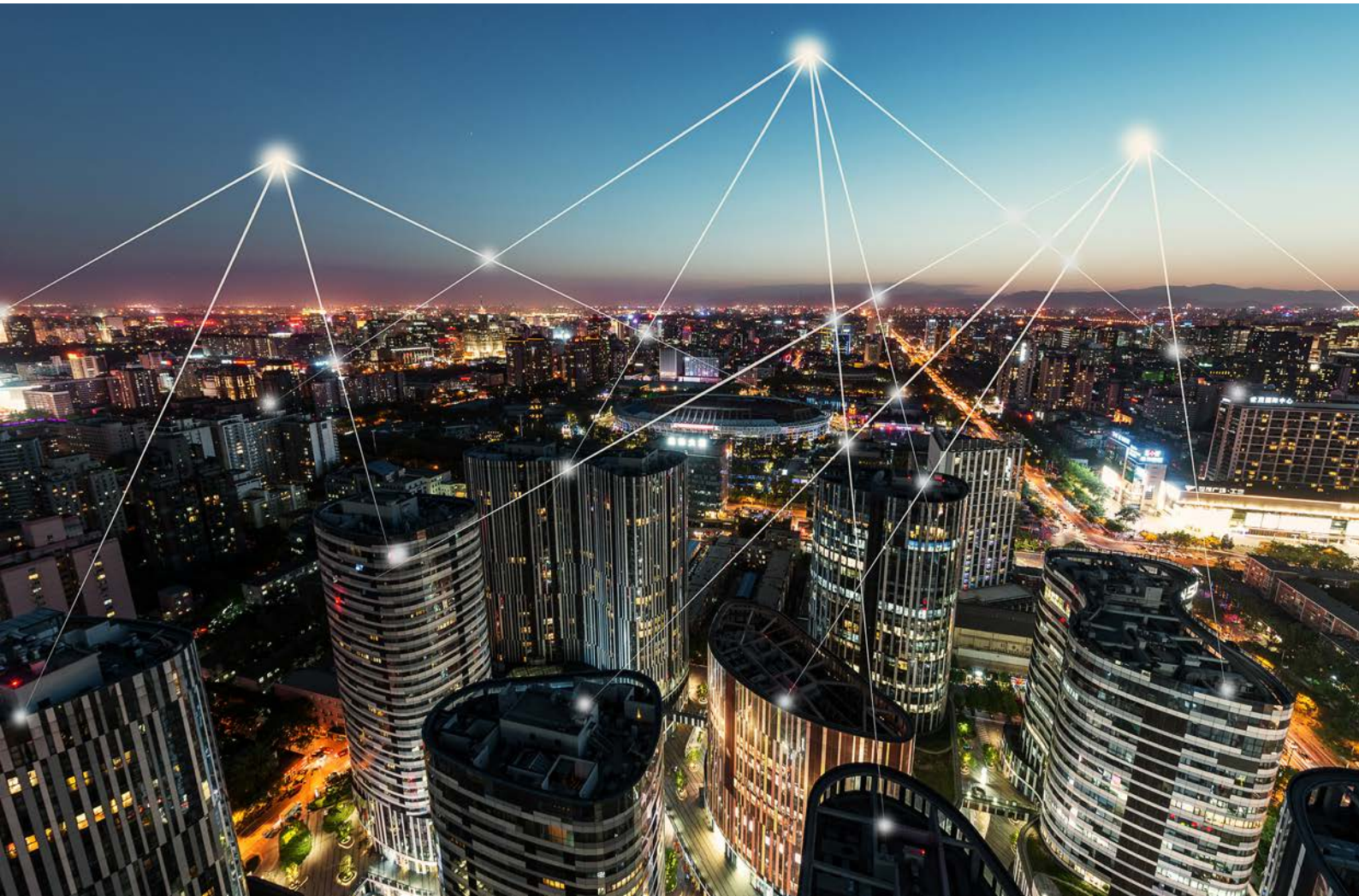
Mobile Connectivity Solutions | Identity and Biometric Solutions | Cloud Protection and Licensing

Thales Digital Identity and Security

Thales is a worldwide leader in data security, providing the tools an organisation needs to protect and manage its data, identities, and intellectual property – through encryption, advanced key management, tokenization, and authentication and access management. Whether it's securing the cloud, digital payments, blockchain or the Internet of Things, security professionals around the globe rely on Thales to confidently accelerate their organisation's digital transformation.

Thales is a leading provider of digital security solutions, specialising in safeguarding critical assets, identities and data in an increasingly interconnected world. With a focus on innovation and reliability, DIS offers a comprehensive range of products and services encompassing cybersecurity, encryption, authentication, biometrics, and secure communication technologies addressed by business lines targeting specific markets.

For a future we can all trust, Thales must anticipate threats and the subsequent evolutions of our products and services. Quantum computing holds the potential to revolutionise technology, but also poses a significant threat to current encryption methods. This makes the development of Post-Quantum Cryptography (PQC) essential, ensuring that we proactively safeguard our data against future quantum-based attacks. Organisations must think strategically and begin preparations immediately to minimise disruptions and expenditures caused by change. Thales recommends that organisations start preparing now for the upcoming Post-Quantum Cryptography transformation to maintain the critical trust they and their customers rely on into a Quantum-Safe future.



Thales's Quantum Commitments

Thales's quantum endeavours gained momentum in response to France's ambitious National Quantum Computing Plan, unveiled in 2021. With a keen eye on the future, the company navigated the uncharted terrain of quantum mechanics, focusing on three areas: quantum sensors, communications, and Post-Quantum Cryptography. Through pioneering research, Thales harnessed the latent potential of matter, exploring sophisticated technologies such as superconducting quantum interference devices[1], solid-state sensors[2], and cold atom technology[3]. These endeavours promised applications in medical diagnostics and military intelligence. Concurrently, Thales embarked on a quest to establish impregnable quantum communication networks, collaborating within the EuroQCI consortium to safeguard sensitive data transmission across Europe. Anticipating the rise of quantum computing, Thales fortified existing systems with Post-Quantum Cryptography, ensuring resilience in an era of digital interconnection. Guided by France's strategic vision, Thales remains committed to excellence, forging ahead in sovereign quantum technologies.

Thales has actively engaged in Post-Quantum Cryptography (PQC) research and development for over a decade and has contributed to various standardisation efforts by industry regulatory bodies. The company is engaged in multiple research projects in the United States, France (RISQ) and across Europe, and funds numerous doctoral theses on the subject. Thales also co-authored the Falcon digital signature algorithm, which NIST selected in 2022 as a candidate for PQC standardisation.

Thales coordinates the RESQUE (*RÉSilience QUantiquE* (Quantum Resilience)) consortium comprising six French companies and organisations. RESQUE recently announced a three-year project to develop a Post-Quantum Cryptography solution capable of protecting the communications, infrastructure and networks of businesses and local governments against future quantum-based attacks.

Additionally, Thales participates in several PQC Consortiums in North America and Europe, including the Post-Quantum Cryptography Alliance, PKI Consortium, and the CFDIR Quantum-Readiness Working Group. Thales Digital Identity and Security and Thales Trusted Cyber Technologies (TCT) (a U.S.-based entity exclusively serving the U.S. Federal Government) are both participants in NIST's National Cybersecurity Center of Excellence (NCCoE)'s Migration to PQC Project. With the crypto-agility to shift between quantum vulnerable classical public key algorithms and the new PQC algorithms, Thales products contributed to the NCCoE project; these products are uniquely capable of assisting with the discovery of any vulnerabilities while also providing platforms for PQC interoperability testing.

Thales Trusted Cyber Technologies (TCT) and the National Security Agency (NSA) signed a Cooperative Research and Development Agreement (CRADA) for evaluating the National Institute of Standards and Technology (NIST) selected Post-Quantum Cryptography (PQC) algorithms when operating on a hardware security module (HSM).

Thales has adopted crypto-agility across its product lines by actively prototyping NIST PQC algorithm finalists within its products and is now focusing on these selected PQC algorithms. Thales is also accelerating towards practical Proof of Concepts (PoCs) with customers, notably for hybrid algorithms in digital signatures and key exchange mechanisms. At Thales, we recognise organisations must adopt a strong Post Quantum crypto-agile strategy. In preparation for the transition, Thales encourages organisations to practice crypto-agility now, to help them evolve and avoid expensive security retrofitting in the future as quantum computing becomes more established. This design principle facilitates changes to the cryptography even after deployment and enables preparation for the transition to quantum-safe solutions once the NIST standardisation process is completed. Finally, Thales has recently contributed in the writing of GSMA's Post-Quantum Cryptography Guidelines for Telecom use cases, emphasizing governance, risk analysis, and cryptographic agility.

[1] ***Superconducting quantum interference devices:*** *Highly sensitive instruments that can measure magnetic flux with exceptional precision.*

[2] ***Solid state sensors:*** *Electronic sensors that detect and measure physical phenomena, such as temperature, pressure, force, or acceleration, and provide a corresponding output, usually in the form of an electronic signal.*

[3] ***Cold atom technology:*** *Scientific approach that involves cooling atoms that allows the exploration of new quantum phenomena and the discovery of novel states of matter, conduct research and gain insights into various quantum phenomena.*

Quantum-safe Solutions for Digital Identity and Security

Preparing Customers for a Quantum-Safe Future

CLOUD PROTECTION & LICENSING

- Network Encryption (HSE)
- Hardware Security Modules
- CipherTrust Data Security Platform

IDENTITY & BIOMETRIC SOLUTIONS

- Secure ID
- Secure Passports
- Identity Services

MOBILE CONNECTIVITY SOLUTIONS

- Embedded SIM
- Embedded Secure Element
- OTA Platform
- Removable SIM

Code Signing | **Networks** | **Communications** | **Certificate Authority** | **TLS** | **PKI** | **Identities**

Thales PQC focus in Digital Identity and Security

Identity and Biometric Solutions

On governmental markets, Thales is on a mission to "Protect people's identity and citizens' rights with Secure, Sustainable and User Centric Solutions". Thales designs, builds and delivers identity and biometrics solutions and services with an holistic approach of security, combining all the effects of physical and electronic security. Crypotography is part of it.

Quantum computers threaten to break the asymmetric cryptography deployed today in electronic ID, health cards, and travel documents such as passports, which will severely impact on security and privacy if not mitigated in advance. The following are some of the ways this might play out:

- PKI based authentication or authorisation to any online or offline system or device could be faked and become insecure.
  - any rogue inspection or verification terminal could authenticate to an ID card or passport and access secret data stored in the chip.
  - an attacker could steal the identity of any citizen and log-in to any public eGovernment service or private eServices such as banking or eHealth and access user data.
- Digital signature on any data would lose its capability to prove that it was performed by a certain party or that the information has not been modified.
  - The identity data stored in an ID card or passport and signed by the issuing country could be altered or created from scratch which would remain undetected as the document signing (DS) key of the Country-Signing CA (CSCA) used for Passive Authentication could be broken.
  - Any electronic document (PDF, web form, etc.) with a qualified signature would lose its legal equivalence with a hand-written signature because the private signing key could be identified from the PKI certificate with the public key.
- Any encrypted communication between two parties would be deprived of its confidentiality as an attacker could eavesdrop on the preceding key exchange to find out the secret key used.
  - The key exchange used in the EAC and SAC protocol for ICAO (International Civil Aviation Organization) travel documents could lose its strength in preventing chip cloning, protecting access to confidential data, and avoiding decrypting the contactless communication between the document and the inspection terminal.
  - The security of encrypted communication between an ID card and an online service or the use of an ID card for encrypted emails, web sessions or to set up a VPN would be broken.

PQC Solutions for Identity and Biometric

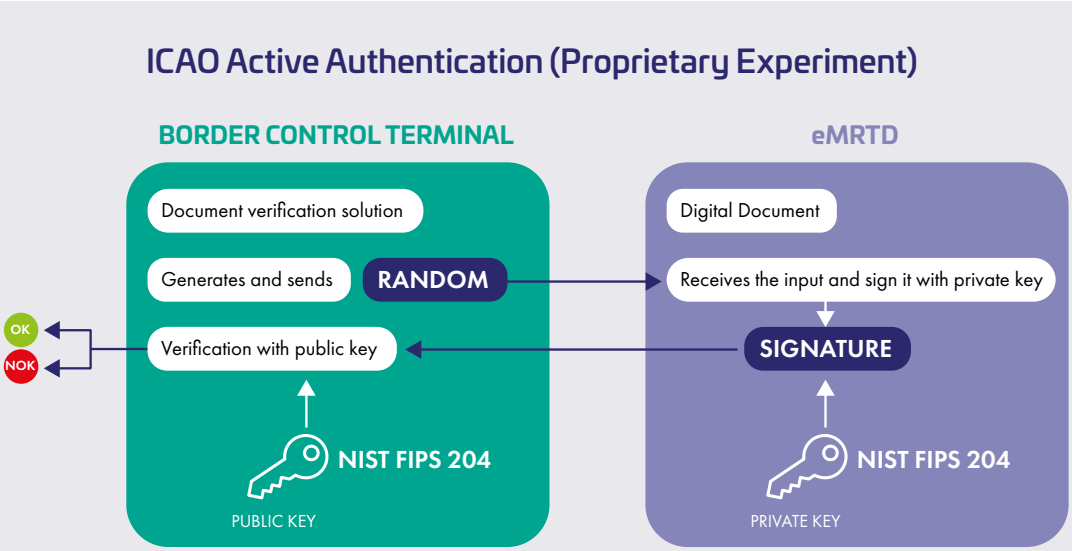
To address the concerns outlined above, Thales is introducing MultiApp v5.2, the first post-quantum-ready operating system for electronic documents premium PQC. Thales built this open and agile platform on a new high-performance chip with enough free memory for extended user data. It complies with the latest JavaCard and GlobalPlatform standards and offers a full suite of JavaCard applets for diverse government use cases. This brand new product adopts a hybrid cryptographic approach and supports:

- Legacy cryptographic features (RSA, ECC, 3DES, AES)
- Hybrid quantum safe signature (RSA (up to 4K)) and NIST FIPS 204 (ML-DSA) – imbricated or concatenated
- Asymmetric on-board key generation (RSA, ECC & NIST FIPS 204)
- Crystals Kyber JavaCard API services for future key exchange applications

In line with the latest cybersecurity recommendations, issued by European Security Agencies (ANSSI & BSI), the hybrid approach offered by our new products ensures the capitalisation of the well demonstrated properties already deemed guaranteed by the traditional RSA algorithm while at the same time enhancing it with the much newer quantum safe technologies.

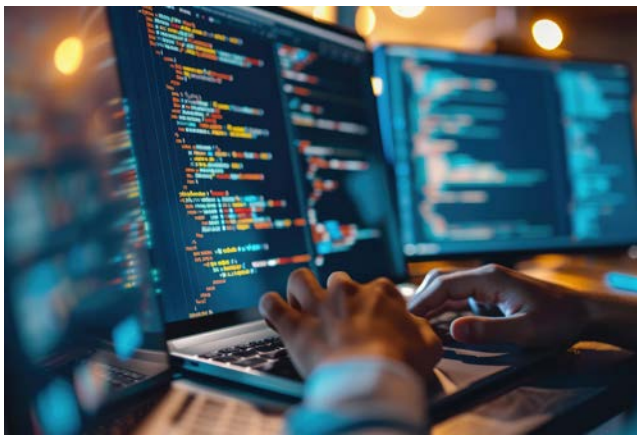
Our engineering teams are also involved in several initiatives (European Research Projects, Technology RFIs) related to the evolution of the Machine Readable Travel Documents (eMRTD) in order to make them Quantum Safe in a near future.

The figure below illustrates ones of the concepts that has been worked out.



eMRTD testing for Quantum Safe specifications

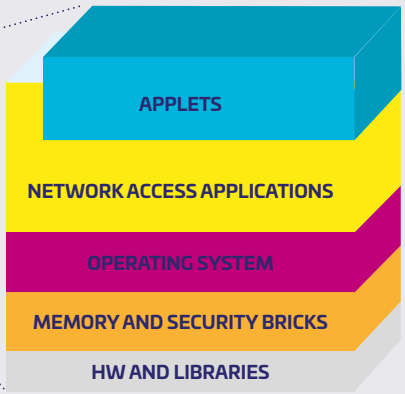
Thales contributes to eMRTD standardisation (ICAO DOC 9303 New Technology Working group) in order to release a quantum safe specification of eMRTD documents. More information is publicly accessible in this Eurosmart document: Eurosmart | The voice of the Digital Security Industry | Quantum computers will compromise the security of identity documents



Mobile Connectivity Solutions

Thales provides secure solutions for a connected world, focusing its efforts primarily on hardware (HW), embedded software (SW), and solutions that facilitate, manage, and provide security for cellular connectivity. MCS specialises in products such as the SIM card, eSIM, and eSE (embedded Secure Element) which are integral to a wide variety of consumer and industrial devices, including Automotive and IoT.

The SIM and eSIM are structured in logical layers; the HW (chip) and a SW stack including an operating system as well as applets, integral for managing subscriber credentials, subscription details, settings, and, significantly, the security aspects. Thales provides also platform services, predominantly cloud-based, for updating SIM cards and managing connectivity.

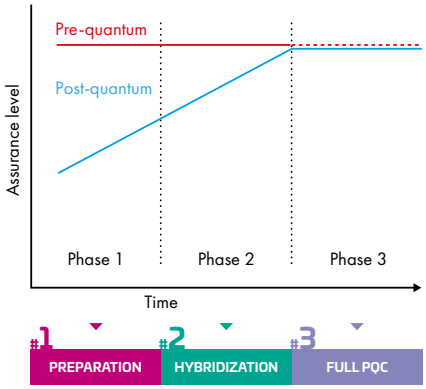


SIM CARD PHYSICAL AND LOGICAL LAYERS

The bottom grey layer is the SIM card hardware, in orange the memory layer and security bricks, the following layer is the operating system (Java card, virtual machine, native apps, etc.) and yellow layer is for specific applications like connectivity management to the network, and finally the applets for the SIM card's configuration.

SIM card technical stack

TOWARDS FULL PQC

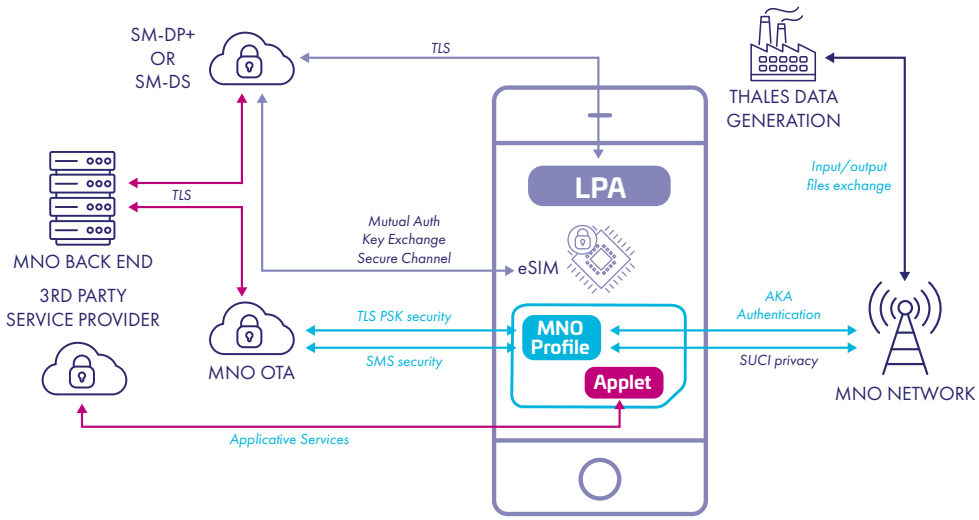


To make Mobile Connectivity Solutions quantum resistant, the following measures are being adopted:

1. Making the **OS upgradable** Over the Air post-issuance so that it can be updated with **new algorithms when a product is already in use on the field.** This is **crypto-agility.**
2. Integrating **PQC algorithms in existing cryptographic security mechanisms including hybrid cryptography to comply with latest recommendations from Security Agencies.**
3. Long term, designing new hardware and software layers to onboard new high demanding PQC algorithms by increasing the **processing power** needed for the cryptographic operations.

But it's not only what Thales delivers that must be quantum protected. In the mobile connectivity ecosystem data exchange happens at many points, between the core network, the end user, the service providers, the SIM/eSIM manufacturer and the SIM/eSIM management platforms. The whole ecosystem needs to be protected. To secure these data exchanges, cryptographic algorithms & protocols shall be upgraded.

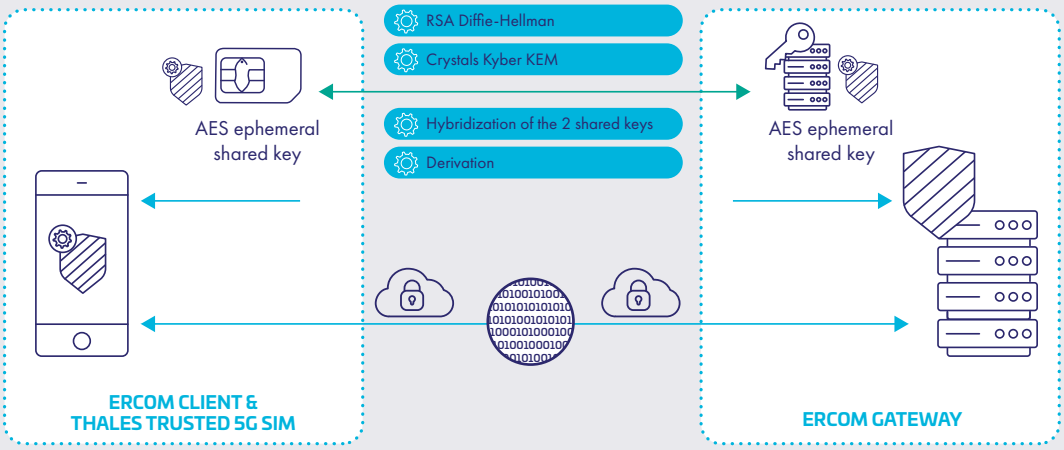
UICC /eUICC cryptography overview



PQC solutions for Mobile Connectivity

One example of this proactive response to quantum threats includes a Mobile-to-Mobile PQC encrypted communication solution that has already been developed:

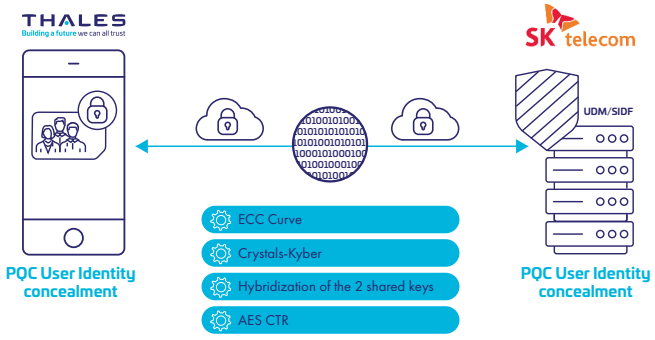
"Cryptosmart", a mobile application to secure calls created by ERCOM, a Thales company, was enhanced to provide protection against Post Quantum potential Harvest Now, Decrypt Later (HNDL) attacks through a hybrid cryptography approach. This evolution utilises CRYSTALS-Kyber, a key exchange management & algorithm approved by NIST (National Institute of Standards and Technology), implemented natively in the SIM operating system. Thales developed and implemented the CRYSTALS-Kyber algorithm exclusively, without involving any third-party development. Notably, the solution focuses on confidentiality, protecting all interfaces on a phone, independent of network security, and is certified by NATO for end-to-end mobile communication security.



Thanks to a hybrid cryptography approach combining pre-quantum and post-quantum defence mechanisms, any data exchanged during the call is resistant to Post-Quantum attacks

Here is another example, with a wider scope of collaboration:

In collaboration with SK Telecom, the largest mobile operator in Korea, Thales explored solutions to preserve SKT users' identities on a 5G network. Using a Thales 5G SIM with a PQC algorithm on a commercial smartphone within SK Telecom's commercial 5G standalone network for this purpose, protection of users' privacy from future quantum threats was achieved, insulating against potential Harvest Now, Decrypt Later (HNDL) attacks. This trial, conducted under realistic conditions of authentication and usage, is seen as a significant advancement as it applied post-quantum encryption algorithms combined with hybrid certificates to protect subscribers' identities, ensuring future proof GDPR compliance by safeguarding users from potential location tracking.



PQC SUCI on SK Telecom regular 5G SA thanks to Thales 5G PQC SIM

The successful implementation of this trial necessitated: an upgraded 5G Trusted SIM able to generate a quantum safe user identity concealment based on hybrid traditional asymmetric and PQC algorithm key exchanges; upgrade of SK Telecom's core network to handle PQC SUCI (user digital identity). This enabled the shielding of the user identity within the SIM, the exchange of PQC encrypted keys, and the deconcealment of the user identity on the core network side.

Thales continues its momentum in the development of quantum-resistant solutions also for Secure Elements (eSE), a strong-box to host applications in Consumer devices, Automotive and IoT. The new generation secure element will integrate a PQC algorithm, and the operating system will be capable of crypto agility, allowing the PQC algorithm to be updated on existing products.

The vision extends to identifying future impacts on SIM and eSIM management platforms and determining necessary upgrades for multiple solutions for subscription management such as Over the Air connectivity servers, Subscription Management Servers, and the entire Thales IoT Connectivity Suite, to keep them aligned with evolving security requirements.

Cloud Protection and Licensing

Thales provides cybersecurity solutions for a world powered by the cloud, data, and software. With products and services spanning hardware, software, and hybrid/cloud-based solutions, our mission is to simplify how organisations discover, protect, and control their sensitive data. Our products and services reduce risk and protect data, simplify, and streamline operations allowing companies to focus on their business.

The company is working on implementing PQC functionality within its HSM (Luna 7 and TCT Luna T-Series Hardware Security Modules) and HSE (High Speed Encryptor) network encryption products. It already has implementations of quantum-safe hash-based signatures (including LMSS and XMSS), Dilithium and Kyber, within the Functionality Module and QRNG and QKD using various partner integrations. The HSE product line has incorporated the pre-standard PQC algorithms using a FIPS compliant classic / PQC hybrid approach. It offers crypto-agile algorithm support, including the PQC candidates, across the range of its currently available hardware appliances.

In parallel with NIST's standardisation efforts and the NCCoE engagement, Thales is now aligning its PQC offerings with the NIST-selected algorithms and optimising PQC performance for upcoming firmware releases. Thales's early engagement with pre-standardised implementations demonstrates the value of crypto-agile architectures. It aligns with the US National Security Memorandum 10 (Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems). To assist customers in preparing for a PQC future by beta testing their PQC readiness today, Thales offers HSE network encryption and HSM starter kits.

Thales has already submitted the products below to the NIST NCCoE lab to help develop practices to ease migration from current algorithms to replacement post-quantum algorithms:

- Thales Luna 7 Hardware Security Module (HSM)
- Thales TCT Luna T-Series HSM (for the U.S. Government)
- Thales CipherTrust Manager for key management
- Thales High Speed Encryptors (HSE) for network encryption

Preparing for Quantum today with Thales

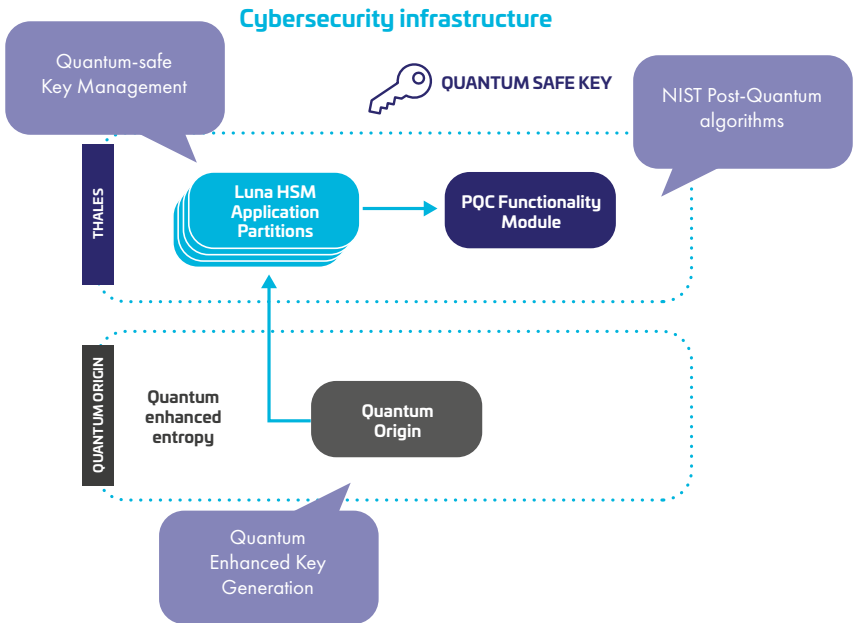
Case Study

A leading multinational financial services company sought to proactively formulate strategic and robust technical solutions so that the data, systems, and applications their customers rely upon could remain safe against future threats from Quantum risks such as Harvest Now, Decrypt Later, and its ability to break current cryptography. The customer wanted to establish PQC-ready security measures in their banking and innovation workflows using provably secure key generation and Post-Quantum Cryptography algorithms proposed by NIST to provide the safest protection for its keys.

Thinking proactively and strategically, knowing they had legacy hardware, system-wide applications, related certificates, and solutions from multiple vendors, any new solution they selected had to be easily integrated into their existing IT environment with minimal disruptions to daily operations. Their reputation as a leader in the financial industry meant ensuring the security of their customers' data and digital transactions and that the changeover to a new solution could have avoided downtime in their customers' online interactions.

Exploring their options, this team wanted to develop a scalable and agile PQC approach that could work across the entire enterprise. To solve this, the customer, Thales and its extensive PQC partner ecosystem worked together to develop a comprehensive quantum-safe commercial solution for secure key generation, management, and protection. This included a partner integration to provide the provably secure key generation within the Thales Luna HSM robust key storage solution paired with the PQC Functionality Module that provided the algorithms currently proposed by NIST for the customer to set up a lab environment to test the impacts of the new algorithms on their data and applications.

PQC HSM STARTER KIT: QUANTUM-SAFE ARCHITECTURE



Architecture of the Thales Luna PQC HSM Starter Kit

Thales, your trusted partner for a post-quantum world

Security is central to all Thales products and services. That's why governments, military, and organisations with extremely sensitive data needs have relied on the company for many decades. In a world increasingly dependent on digital transactions, where data has immense value, Thales has a vital role to play. Quantum cyberattacks could cripple large networks in minutes. In anticipation of this evolution, hackers have already begun a Harvest Now, Decrypt Later (HNDL) strategy of stealing longer life data they cannot yet access - but will soon be able to.

The SIM and eSIM represent the root of trust in connectivity. The Luna HSM, including the CipherTrust Manager, fulfills the same role for data. Thales High Speed Encryptors (HSE) are the solution of choice to enable secure transmission of data across networks. Thales has also built an open and agile first post-quantum-ready operating system for electronic documents. Building on these foundations, Thales is now focused on making all of the company's products and services quantum resistant and crypto-agile to ensure customers will be PQC ready. Crypto-agility is essential, enabling well-protected organisations to quickly change protocols, keys, and more besides, in the event of change. This facilitates greater resilience, even after Post-Quantum Cryptography is established, by ensuring organisations can react quickly to evolving threats.

Thales Digital Identity and Security shows robust positioning on Post-Quantum Cryptography, focusing on supporting the latest cryptographic algorithms including codeveloping the Falcon cryptographic signature algorithm, adopting new communications and key management protocols, and evolving certificates to increase quantum resistance. Attention is directed not only to the hardware and software but also the broader ecosystem that connects the various Thales organisations and beyond.
Notably, these proactive efforts represent significant opportunities for differentiation and the capacity to leverage Thales products, including the 5G PQC SIM card, PQC-ready Luna HSM and HSE network encryption solutions available today.

As with classical cryptography, Thales is augmenting the security level of its PQC implementations with specific in-house cybersecurity expertise (including physical security such as Side-channel attack protection) and is optimising them to fit within embedded device constraints.

Thales has developed solutions that are crypto-agile by design and can help defend against Harvest Now, Decrypt Later (HNDL) attacks today and into the future. Thales has an extensive and growing partner ecosystem, including PKI providers and PQC partners, to enable an optimum quantum transition that can begin immediately.

Thales's ongoing exploration and utilisation of PQC capabilities, offering the crypto-agility to evolve as quantum advances, paired with a focus on data and identity security, reinforce our commitment to ensuring trust across the expanding digital landscape and preparing for future quantum threats today.

THALES

Building a future we can all trust

Thalesgroup.com/Mobile

© Thales 2024. Photos credit: Shutterstock - September 2024 - Design: Jubeme