Case study PQC - Infineon

to accompany the publication of ***Decrypting the Future: Global Timelines for Post-Quantum Cryptography and why they matter***

1. **Your company is an active member of the Charter of Trust's Post Quantum Cryptography (PQC) Working Group. What makes collaboration in the domain of PQC so important?**

No single company can make a system quantum-safe on its own. A secure product is a chain: silicon, firmware, software stacks, protocols such as Transport Layer Security (TLS) and X.509 (public cryptographic key for digital certificates), certification schemes, and the manufacturer (OEM) that puts it all together. If one link is not ready for PQC transition, the whole chain stays exposed.

Collaboration also protects against fragmentation. Standards bodies and national agencies are moving at different speeds and do not always recommend the same algorithms. A forum like the Charter of Trust lets partners from different sectors compare notes early, agree on what "ready" means, and send a consistent signal to the supply chain. This shortens the migration for everyone.

2. **Why is the topic of PQC particularly relevant for your company?**

Because Infineon sits at the very start of the product lifecycle. A semiconductor we design today may still be in the field in 20 or 30 years: a car with our chips has an average service life of around 15 years; industrial components often run for 20 to 30 years. The German Federal Office for Information Security (BSI) takes the view that it cannot be ruled out that **quantum computers capable of breaking today's main encryption methods appear in the early 2030s. Many products we ship now will still be operating** when it happens.

"Harvest now, decrypt later" adds a second reason to act early: data and design assets copied today can be decrypted later, a serious risk for sectors with long research and development cycles. **This is why Infineon started early.** We implemented a post-quantum key exchange on a commercially available contactless smart card chip as early as 2017 and contributed to the SPHINCS+ digital signature scheme now standardized by the US National Institute of Standards and Technology (NIST). In December 2024 we received what we believe to be the world's first Common Criteria Certificate covering post-quantum cryptography key exchange (ML-KEM) on a security controller.

3. **What is a key takeaway from your company's work on PQC in the past year and what are you focusing on for next year?**

In our experience, **PQC has moved from a research topic to a purchasing requirement**: customers increasingly ask for compliance against named standards rather than general reassurance.

Two products show how we answer that. The OPTIGA™ TPM SLB 9672, launched in 2022, is a Trusted Platform Module with a **firmware update mechanism protected by post-quantum signatures**. **With that, a device already in the field can still be updated if today's algorithms stop being trusted.** In August 2025 we announced the PSOC™ Control C3 Performance Line, our first MCU family with accelerated PQC options. It offers hardware-accelerated secure boot and firmware update verification, meets the post-quantum firmware-protection requirements set out in the US Commercial National Security Algorithm Suite (CNSA) 2.0, and is designed to withstand advanced hardware and software attacks (PSA Certified Level 3 requirements). Our Edge Protect Tools and ModusToolbox™ allow hybrid signing with both traditional and post-quantum key exchange and have moved from to samples in 2025 to dedicated power conversion and motor control parts in production during 2026.

Crypto-agility and a trusted quantum-resistant update path matter as much as the choice of algorithm. Infineon has demonstrated successful PQC pilots for the German National eID card with hybrid PQC implementation. Hybrid implementations and crypto agility for post quantum cyber resilience are important aspects for most implementers as the **security targets in a post-quantum era involving AI will be shifting frequently.**

For the coming year, Infineon focuses on extending PQC across more of the portfolio, preparing for ML-KEM and ML-DSA (for digital signatures) in hardware and firmware use cases. The goal is also **making the tooling simple enough so that customers do not need to be cryptography specialists** to adopt it.

4. **What is one challenge in applying PQC roadmaps across the world that you would like to see solved?**

Divergence between national frameworks. Approved algorithm lists, certification routes and deadlines differ across the US, the EU, the UK and the Asia-Pacific region, and they are not simply stricter or weaker versions of each other. **A semiconductor is designed once and sold everywhere, so it must satisfy several regimes at once.** This drives cost and slows delivery. What would help most is convergence on a common core of algorithms, faster protocol-level standardization, and mutual recognition of post-quantum specific evaluation results between certification schemes. Regional differences will remain, but they should sit at the edges, not in the foundations.

5. **Do you have any recommendations for peers working on applying PQC into the industry, in particular when working globally?**

Here are a few recommendations for our peers:

- Start with an inventory and include your suppliers. You cannot migrate cryptography you cannot see, and much of it sits in third-party components.
- Buy crypto-agile hardware now. Devices being designed today should already have the performance and memory headroom for post-quantum algorithms, plus a secure field-update path.
- Use hybrid during the transition. Running classical and post-quantum algorithms together protects interoperability while standards settle.
- Put PQC into procurement. Ask vendors for roadmaps and contractual commitments rather than statements of intent.
- Where regional requirements overlap, design to the superset; where they conflict, rely on crypto-agility rather than building separate product variants.
- Do not wait for perfect standards. The infrastructure change takes years; the quantum timeline will not wait for it.