The Futurist: Invisible Innovation, Real-World Impact

In the first episode of The Futurist: Innovation Stories, IST discusses its latest advances in post-quantum cryptography and digital security.

PAYMENT CONNECTIVITY CYBERSECURITY

POSTED ON 06.24.25

The future of digital security is being written today—quietly, but decisively. In the first episode of **The Futurist: Innovation Stories**, IDEMIA Secure Transactions (IST) discusses its latest advances in post-quantum cryptography (PQC). As quantum computing edges closer to reality, the entire ecosystem—from industry to government and academia—must act. IST is already building the foundations of a secure, quantum-resilient world, empowering customers to safeguard their infrastructure, extend product lifecycles, and stay confidently ahead of tomorrow's threats.

Why Post-Quantum Matters Now

Quantum computing is no longer a distant threat. Its ability to break today's cryptography standards could compromise everything from financial transactions to national infrastructure. Recognizing the shift early, IST's R&D teams have been preparing since 2016 for a future where quantum resilience isn't optional; it's essential.

> *Quantum computers will revolutionize the way computing works... but they will also be good at one thing: breaking traditional cryptography.*
>
> Amaanie Hakim, Vice President of Innovation and IP, IDEMIA Secure Transactions

But post-quantum cryptography isn't just about algorithms. It's about agility, adaptability, and trust. IST's innovation journey has focused on building crypto agile solutions that can evolve as threats evolve—ensuring that security isn't just strong today, but resilient tomorrow.

From Vision to Validation: A Quantum-Ready Breakthrough

The journey from concept to real-world impact is rarely linear. IDEMIA Secure Transactions' collaboration with Telefónica marked a pivotal moment in the partners' post-quantum cryptography journey. What began as a shared vision for crypto-agile, future-proof security culminated in a live demonstration that drew industry-wide attention.

> *This wasn't innovation for innovation's sake. We worked closely with Telefónica to define a use case that was both technically advanced and commercially relevant.*
>
> Dario Suarez, Telefonica Global Account Manager, IDEMIA Secure Transactions

Unveiled at Mobile World Congress 2025, the demonstration showcased how quantum-safe technologies can secure both the remote provisioning of eSIM profiles and the transmission of smart meter data. Using post-quantum algorithms for digital certificates and profile signing, the solution prevents impersonation and tampering—even in the face of future quantum threats.

The solution is built on two key pillars. First, all cryptographic operations in the smart meter are handled within the eSIM, leveraging the standardized IoT SAFE applet. This applet can be accessed by the meter's operating system, allowing cryptographic processes to be offloaded to a secure, tamper-resistant environment. Second, the solution takes advantage of the existing end-to-end eSIM infrastructure—including the Subscription Manager (SMDP+) and eSIM IoT Remote Manager (eIM)—to enable remote cryptographic updates with no need for physical access or field intervention.

By embedding cryptographic libraries directly into the eSIM profile, the meter can be easily upgraded to support post-quantum versions of protocols such as TLS (Transport Layer Security), which secures data exchanges with the utility. These updates are performed remotely, demonstrating a strong level of crypto-agility (the ability to adapt cryptographic mechanisms over time without hardware replacement) making it possible to maintain a high level of protection for deployed devices even as threats evolve.

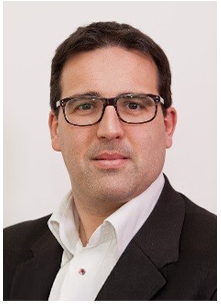
> *The idea of this project was to demonstrate that we could update cryptography over the air on already deployed chips, thus transitioning from classic to post-quantum cryptography, and even replacing one PQ algorithm with another, all while maintaining security.*
>
> Antton Bodin, Embedded Software Engineer, IDEMIA Secure Transactions

The demonstration validated not just the technical feasibility of PQC in constrained IoT environments, but also its practical value to help customers secure their systems today and adapt for tomorrow.

The Bigger Picture: Future-Proofing Trust

What makes this story powerful isn't just the technology; it's the mindset. IDEMIA Secure Transactions is proving that some of the most transformative innovations happen behind the scenes.

> *Post-quantum is a very technical and almost invisible innovation. (..) It must be a joint effort—a real collaboration with all stakeholders.*
>
> Benoit Collier, VP Product Business Line, IDEMIA Secure Transactions



By strengthening the cryptographic foundations of our digital world, IST is helping customers prepare for what's next—without disruption, without compromise. It's a reminder that true innovation isn't always visible, but its effects are lasting: trust that endures, systems that adapt, and security that scales with the future.