IDEMIA and Telefónica Showcase Post-Quantum eSIM Technology

Protecting smart utility networks and IoT devices from post-quantum cyber threats

CONNECTIVITY CYBERSECURITY

POSTED ON 07.18.25

IDEMIA Secure Transactions (IST) and **Telefónica** unveiled the innovative post-quantum proof-of-concept at Mobile World Congress (MWC) Barcelona 2025 which is now available for demonstration at their respective Experience Centers. The demo showcases post-quantum eSIM technology securing IoT devices in smart utility networks, with built-in crypto agility and quantum-resistant security.

Request a demo

Securing Smart Utility Networks Against Emerging Threats

Utility networks, such as those used by smart water, gas, and electricity meters, are expected to grow by 10% over the next decade*. These long-lifecycle devices often remain deployed in the field for 10 to 15 years, making them prime targets for emerging cybersecurity threats. This creates a critical need for quantum-safe solutions to protect both device technology infrastructure and data.

The IST and Telefónica demonstration features a smart meter in an IoT deployment, seamlessly transitioning from current security to post-quantum security—enabled by a post-quantum-ready eSIM with cryptographic agility capabilities. IST's solution, integrated by Telefónica, ensures the protection of mobile communications used for both the remote provisioning of eSIM cards and the transmission of meter readings. This approach preserves privacy and prevents tampering, ensuring the security and integrity of transmitted data.

Quantum-Safe Algorithms and Crypto Agility

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.

This setup ensures that even powerful future attacks can be mitigated—for example, using quantum computing to impersonate a mobile operator, alter eSIM profiles, or intercept transmitted data. And if further adaptations become necessary, the cryptography can be updated remotely through the same secure eSIM channel.

In industrial IoT environments, where long lifespans and large-scale deployments make equipment upgrades costly and complex, this level of crypto-agility is a game changer. It allows utilities to stay ahead of emerging security threats without replacing devices or sending technicians into the field, helping ensure resilience, compliance, and operational continuity over time.

---

*Source: Transforma Insights IoT Forecast Database, 2024
