IDEMIA Secure Transactions Advances Post-Quantum Authentication with New KEM-Based Technology

Replacing traditional digital signatures with KEM, IST becomes the first to demonstrate efficient post-quantum authentication on PIV cards.

CYBERSECURITY

POSTED ON 06.16.26

IDEMIA Secure Transactions (IST) announces an advance in post-quantum cryptography (PQC) through the design of a new authentication technology that replaces traditional digital signatures with Key Encapsulation Mechanisms (KEM) to enable more efficient, scalable quantum-resistant security.

As quantum threats accelerate, many post-quantum cryptography migration strategies rely on the direct replacement of classical signatures with Post-Quantum signature schemes—introducing substantial overhead in constrained environments. IST investigated a different approach by redesigning the authentication flow itself to leverage KEM, enabling equivalent security objectives with improved performance.

This approach enables:

- Reduced data exchange and faster execution
- Lower computational and memory requirements
- More efficient deployment on embedded and resource-constrained devices

To validate this innovation in a real-world environment, IST has successfully applied it to the NIST PIV framework, becoming the first company to demonstrate a complete Personal Identity Verification (PIV)[1] application running on a smartcard using post-quantum cryptography.

This demonstration confirms that post-quantum authentication can be both secure and practical, preserving existing system architectures while preparing them for the quantum era.

> *Moving to post-quantum security requires more than replacing algorithms, it also calls for rethinking protocols. Our KEM-based approach delivers strong security with significantly improved efficiency, paving the way for practical, scalable PQC deployment.*
>
> Marc Bertin, CTO, IDEMIA Secure Transactions

IDEMIA Secure Transactions brings a strong track record of leadership in post-quantum cryptography, demonstrated through a series of industry firsts: introducing the first quantum-safe 5G SIM in 2021, launching the first crypto-agility solution for a smart card in 2024, delivering the first offline CBDC solution in 2024, and earning recognition as a top-ranked player in Juniper Research's 2025 post-quantum cryptography matrix.

This milestone further demonstrates the company's ability to turn post-quantum innovation into real-world, scalable deployments.

---

[1] A secure smartcard used to verify identity and control access to systems and physical locations, widely used in government and enterprise environments.
