IDEMIA Secure Transactions Announces its First Hardware Accelerator Designed for Post-Quantum Cryptography

Reaffirming its leadership in post-quantum cryptography, this cutting-edge accelerator significantly boosts data protection against quantum computing risks. The technology ensures top-notch security, high performance, and a seamless user experience, essential for transitioning to quantum-resistant standards.

PAYMENT CONNECTIVITY

POSTED ON 03.18.25

IDEMIA Secure Transactions (IST) is announcing today an advanced post-quantum accelerator based on Keccak[1], a core function widely used in new cryptographic algorithms.

Post-quantum algorithms are highly demanding on computational resources to ensure robust security. By utilizing hardware accelerators, intensive tasks can be offloaded from the main processor, significantly boosting both speed and efficiency. This approach is essential for ensuring secure, seamless and efficient data protection against the rising threats posted by quantum computing.

Leveraging IST's integrated design expertise and its deep knowledge in post-quantum cryptography, this latest hardware accelerator permits a more rapid execution of the quantum-resistant algorithms standardized by the National Institute of Standards and Technology (NIST)[2]. This advanced module optimizes cryptographic performance, enabling a smooth transition to post-quantum solutions without compromising speed or ease of use. It will be embedded in all future quantum-safe chips from IDEMIA Secure Transactions.

Innovation at the heart of digital resilience

This advancement comes at a critical juncture, as organizations across the banking, automotive, IoT, Industry 4.0 and healthcare sectors are seeking robust solutions to safeguard their long-term data security. It offers several benefits for service providers as well as end-users:

- **For businesses:** by adapting the design to new cryptography standards, IST offers an agile solution, capable of effortlessly supporting service providers in their post-quantum migrations.
- **For end-users:** this innovation ensures enhanced security against next-generation cyberattacks while maintaining the current user experience. Card payments, crypto wallets and communications via SIM cards or NFC products will remain seamless while benefiting from state-of-the-art security.

A holistic approach to security

As a global leader in secure solutions, IDEMIA Secure Transactions is committed to accompanying its customers in their post-quantum migration. This technological advancement exemplifies our holistic approach to securing the future, offering robust protection and seamless user experiences amid the quantum challenges.

Marc BERTIN, Chief Technology Officer at IDEMIA Secure Transactions

---

[1] Keccak is a cryptographic hash function, which was selected as the winner of the NIST (National Institute of Standards and Technology) SHA-3 (Secure Hash Algorithm) competition.
[2] ML-KEM (FIPS 203), ML-DSA (FIPS 204) and SLH-DSA (FIPS 205)

About IDEMIA Group - IDEMIA Group unlocks simpler and safer ways to pay, connect, access, identify, travel and protect public places. With its long-standing expertise in biometrics and cryptography, IDEMIA develops technologies of excellence with an impactful, ethical, and socially responsible approach. Every day, IDEMIA secures billions of interactions in the physical and digital worlds.

IDEMIA Group brings together three market-leading businesses that enable mission-critical solutions:
· **IDEMIA Secure Transactions** is the leading technology provider who unlocks safer and easier ways to pay and connect.
· **IDEMIA Public Security** is a leading global provider of biometric solutions that unlock convenient and secure travel, access, and protection.
· **IDEMIA Smart Identity** leverages the power of cryptographic and biometric technologies to unlock a single trusted identity for all.
With a global team of nearly 15,000 employees, IDEMIA Group is trusted by over 600 governmental organizations and more than 2,400 enterprises in over 180 countries. For more information, visit www.idemia.com and follow @IDEMIAGroup on X.

your press contact(s).

IDEMIA

contact.press@idemia.com

HAVAS

idemia@havas.com