IDEMIA launches enhanced security smart cards resistant to quantum computers

PUBLIC SECURITY & IDENTITY

POSTED ON 04/11/19

- Asymmetric cryptography lies at the heart of digital security
- The asymmetric algorithms (e.g. RSA and ECC) are deemed not to be resistant to cryptanalysis methods that will be achievable with the new generation of quantum computers
- Post-quantum cryptography is the newest generation of cryptographic algorithms, which is resistant to the cryptanalysis methods that will be possible with quantum computers

Asymmetric cryptosystems are at the heart of digital security as they are the cornerstone for the Public Key Infrastructure (PKI), as well as – amongst other things - secure authentication, digital Identities and trusted services. In particular, they are widely deployed in secure elements to perform safe authentication of people and things (IoT).
Indeed, it is believed that quantum computers will be able to break various asymmetric cryptographic algorithms (such as RSA or ECC) within the next 20 years.

To make quantum-resistant smart cards, IDEMIA, the global leader in Augmented Identity, has implemented in a secure element/smart card, an asymmetric post-quantum algorithm creating an unforgeable signature when using a quantum computer for enhanced authentication. Documents can be signed in less than 2 seconds, ensuring a frictionless user experience. These IDEMIA smart cards are now resistant “by design”.

IDEMIA is one of the only companies which offer quantum-safe asymmetric cryptosystems, capitalizing on secure elements/smart cards, which offer portability and confidentiality of secret elements (keys and PIN/Biometric credentials).

This solution paves the way for the migration of digital security to quantum-safe implementation: public key infrastructure, secure authentication of people and things (IoT) and trusted services like electronic signatures.

With its brand-new smart card solution, IDEMIA will address business needs in authentication, logical access, tracking of actions, data encryption and protection, for customers such as security agencies or governmental organizations including ministries of defense.

IDEMIA is the trusted partner to help national security agencies, governments, and also the private sector to continuously guarantee security. With this innovation, IDEMIA has proven that a post-quantum algorithm can be implemented on a smart card. Indeed, our R&D teams are committed to always providing cutting-edge technologies, preparing our customers for the future, ahead of the curve.

Jean-Christophe Fondeur, Executive Vice-President for R&D activities at IDEMIA

About us - IDEMIA, the global leader in Augmented Identity, provides a trusted environment enabling citizens and consumers alike to perform their daily critical activities (such as pay, connect, travel and vote), in the physical as well as digital space.

Securing our identity has become mission critical in the world we live in today. By standing for Augmented Identity, an identity that ensures privacy and trust and guarantees secure, authenticated and verifiable transactions, we reinvent the way we think, produce, use and protect one of our greatest assets – our identity – whether for individuals or for objects, whenever and wherever security matters. We provide Augmented Identity for international clients from Financial, Telecom, Identity, Public Security and IoT sectors.
With 13,000 employees around the world, IDEMIA serves clients in 180 countries.

For more information, visit www.idemia.com / Follow @IdemiaGroup on Twitter

your press contact.

IDEMIA - HAVAS PARIS PR AGENCY

+ 33 6 63 73 30 30
idemia@havas.com