IDEMIA announces first in world Quantum-Safe 5G SIM technology

IDEMIA is proud to announce the implementation of a Quantum-Safe algorithm on a 5G SIM card that protects data and subscriber privacy from a quantum computer threat.

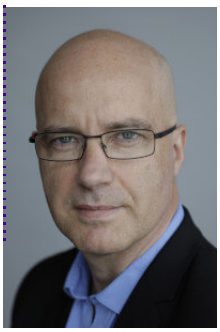
CONNECTIVITY

POSTED ON 12.17.21

IDEMIA is proud to announce the implementation of a **Quantum-Safe algorithm** on a **5G SIM card** that **protects data and subscriber privacy** from a quantum computer threat.

A world first in telecommunications, the Quantum-Safe 5G SIM card uses a quantum-resistant public-key cryptographic algorithm shortlisted by NIST* as a candidate for the first standard devised to protect against the threat of a quantum attack.

The quantum revolution, which first came to people's attention more than 20 years ago, will soon magnify this risk. Imagine a computer that can run quantum system-based algorithms so as to instantly find out secret codes that otherwise would be totally watertight. This will be inevitable in the next few years, and IDEMIA, as a security and cryptography leader, has been working diligently to remain ahead of quantum security breaches by developing the defenses needed for iron-clad security. Quantum computers are on the way to penetrating everything that we know now as practically impenetrable, including today's encryption.



The quantum revolution is a tremendous opportunity that will play a promising role in many industries on the condition of anticipating risks. We're preparing today the technological vaccines for tomorrow, in particular to maintain security of critical systems and data protected by cryptography.

Marc BERTIN, CTO SET at IDEMIA

As 5G technology is already the most secure in terms of subscriber privacy by encrypting the International Mobile Subscription Identifier (IMSI) in a 5G SIM card, IDEMIA is leveraging this technology with Quantum-Safe algorithms for **the ultimate privacy shield**.

Why now? Quantum computing is delivering huge leaps forward in processing power to solve complex challenges in seconds or minutes as opposed to a billion years in the case of asymmetric cryptography. With this type of computer also comes new dangers to data security, and threats to citizen privacy, as all data processed, stored, and secured with current cryptography can be hacked when the quantum era becomes a reality, which could be in 5 to 10 years. Therefore, it is important to be prepared now, especially for information sent across telecommunication networks that will still have a value in the next 10 years, more specifically in personal information.

IDEMIA is currently working with some the world's key mobile operators to continue exploring solutions, and research that protects the telecom industry from quantum attacks.

At the forefront of innovation to protect critical data, IDEMIA's Research & Development department has long been working to develop quantum-resistant solutions that protect society, and look forward to future technological breakthroughs that will help prepare the industry for tomorrow's future.

---

* National Institute of Standards and Technology
