IDEMIA empowering years of research to be ready for the post-quantum era

The transition to post-quantum cryptography has already begun, and IDEMIA has long been a pioneer in innovating to protect critical data.

CONNECTIVITY

POSTED ON 06.28.23

Quantum computers have the potential to revolutionize our world by speeding up the performance of certain tasks much faster than today's computers are capable of on a large scale. However, their arrival also raises concerns about security that could affect our daily lives. Even while traditional key cryptography is not at risk today, it is crucial to anticipate and be at the forefront of this new technological evolution.

The transition to post-quantum cryptography has already begun, and IDEMIA has long been a pioneer in innovating to protect critical data. IDEMIA's Research & Development department is actively engaged in creating quantum-resistant solutions that safeguard society in the post-quantum world for every verticals we address with our cryptography solutions such as identity documents, payment or SIM/eSIM connectivity solutions. In the Telecom market, our longstanding expertise in security and cryptography makes us a natural technology leader; driving industry contribution to standards bodies, moving into practice through pilot projects, and supporting our customers in the transition to post-quantum cryptography (PQC) solutions.

IDEMIA participates in the GSMA "Post Quantum Telco Networks" taskforce with industry groups, governments, and the vendor ecosystem on roadmaps to implement post-quantum cryptography. At the same time, the telecom industry is mobilizing to define guidelines, processes, and standards for the PQC transition.[1]

Members of the GSMA have specified the importance of:

- Impact assessment for the transition to Post-Quantum Cryptography in telecom networks
- Updates to existing security architecture as existing algorithms become vulnerable
- Understanding how to treat legacy systems, services, and products that may not be updated
- Reducing the creation of technical cryptographic debt*
- Considering impacts to key management systems

The technological features implemented in our solutions are already evolving in-line with the PQC transition, particularly in the area of 5G. IDEMIA's Quantum-Safe 5G SIM technology uses a cryptographic algorithm resistant to quantum computing that has been selected and recommended by the National Institute of Standards and Technology (NIST). These state-of-the-art algorithms have been proactively integrated in anticipation of new ETSI and GSMA standards, ensuring privacy protection for the subscriber identity, represented by the IMSI (International Mobile Subscriber Identifier). By preventing its transfer in plaintext over the cellular network, IDEMIA's Quantum-Safe 5G SIM

technology eliminates the risk of personal data breaches and safeguards user confidentiality

In 2022, IDEMIA pioneered post-quantum cryptography initiatives with a successful pilot project tested to be resilient in the post-quantum era.[2]

During the 2023 Mobile World Congress, IDEMIA was recognized by the industry with a GLOMO award in the “Best Mobile Security Solution” category for our 5G technologies. The award highlights IDEMIA’s commitment to providing mobile operators with a secure and reliable connectivity solution for their customers with the best use of technology to safeguard customers’ personal data and help network operators and service providers combat fraudulent access to networks.

Our technologies (biometrics, cryptography, systems, analytics, and smart devices) enable a world of novel experiences and are built on decades of research and ongoing investments. With significant investments in cryptography, IDEMIA is spearheading advancement of the technological building blocks within the industry and serving our enterprises and governments customers around the world. This proactive approach ensures that we serve the needs of today while preparing the “technological vaccines” of tomorrow.

Contact your IDEMIA representative to visit our Innovation Hub at the Experience Center based in Paris-La Defense Headquarters for an in-private demonstration and envisioning workshop.

* accumulation of legacy systems and applications that are difficult to maintain and support

---

1. https://www.gsma.com/newsroom/resources/post-quantum-telco-network-impact-assessment-whitepaper/
2. https://www.idemia.com/press-release/idemia-and-telefonica-espana-boost-security-5g-sim-technology-pioneering-solutions-protect-users-communications-2022-05-03
