# IDEMIA s’appuie sur des années de recherches pour être prêt pour l’ère post-quantique

La transition vers la cryptographie post-quantique a déjà commencé et IDEMIA est un pionnier de longue date dans le domaine de l'innovation pour protéger les données critiques.

**# CONNECTIVITÉ**

**POSTÉ LE 28.06.23**

Les ordinateurs quantiques ont le potentiel de révolutionner notre monde en permettant d’exécuter certaines tâches beaucoup plus rapidement que ne le permettent les ordinateurs actuels, et à l’échelle de la mécanique quantique. Cependant, leur arrivée soulève également des inquiétudes quant à la sécurité qui pourrait affecter notre vie quotidienne. Même si la cryptographie à clé publique n’est pas menacée aujourd’hui, il est crucial d’anticiper et d’être à la pointe de cette nouvelle évolution technologique.

La transition vers la cryptographie post-quantique a déjà commencé, et IDEMIA est depuis longtemps un pionnier de l’innovation dans la protection les données critiques. Le département Recherche & Développement d’IDEMIA est activement engagé dans la création de solutions résistantes aux ordinateurs quantiques. Elles protègent la société dans le monde post-quantique, dans les différents marchés que nous adressons, avec des solutions basées sur la cryptographie, telles que les documents d’identité, les cartes bancaires, les solutions de connectivité SIMs/eSIMs. Pour le marché des Telecoms, notre expertise de longue date en matière de sécurité et de cryptographie nous positionne naturellement en leader technologique ; moteur dans la contribution de l’industrie aux organismes de normalisation/standardisation, mettant en pratique la recherche à travers des tests pilotes et apportant notre support aux clients dans leur transition vers des solutions de cryptographie post-quantique.

IDEMIA participe au groupe de travail « Post Quantum Telco Networks » de la GSMA avec des industriels, des institutionnels et l’écosystème de vente sur la roadmap d’implémentation de la cryptographie post-quantique. Dans le même temps, l’industrie des télécommunications se mobilise pour définir les lignes directrices, processus et normes de la transition PQC.[1]

Les membres de la GSMA ont précisé l’importance de :

- L’analyse d’impact pour la transition vers la cryptographie post-quantique dans les réseaux de télécommunications
- Les mises à jour de l’architecture de sécurité existante à mesure que les algorithmes existants deviennent vulnérables
- La compréhension des traitements des systèmes, services et produits existants qui peuvent ne pas être mis à jour
- La réduction de la création de dette technologique* en cryptographie
- Prise en compte des impacts sur les principaux systèmes de gestion

Les fonctionnalités technologiques mises en œuvre dans nos solutions évoluent déjà en ligne avec la transition PQC, en

particulier dans le domaine de la 5G. La technologie SIM 5G Quantum-Safe d'IDEMIA utilise un algorithme cryptographique résistant à l'informatique quantique qui a été sélectionné et recommandé par le National Institute of Standards and Technology (NIST). Ces algorithmes de pointe ont été intégrés de manière proactive en prévision des nouvelles normes ETSI et GSMA, assurant la protection de la vie privée de l'identité de l'abonné, représentée par l'IMSI (International Mobile Subscriber Identifier). En empêchant son transfert en clair sur le réseau cellulaire, la technologie SIM 5G Quantum-Safe d'IDEMIA élimine le risque de violation des données personnelles et préserve la confidentialité des utilisateurs.

En 2022, IDEMIA a lancé des initiatives de cryptographie post-quantique avec le succès d'un projet pilote testé pour être résilient à l'ère post-quantique.[2]

Lors du Mobile World Congress 2023, IDEMIA a été récompensé par l'industrie par un prix GLOMO dans la catégorie « Meilleure solution de sécurité mobile » pour nos technologies 5G. Ce prix souligne l'engagement d'IDEMIA à fournir aux opérateurs mobiles une solution de connectivité sécurisée et fiable pour leurs clients avec la meilleure utilisation de la technologie pour protéger les données personnelles des clients et aider les opérateurs de réseaux et les fournisseurs de services à lutter contre l'accès frauduleux aux réseaux.

Nos technologies (biométrie, cryptographie, systèmes, analyses et appareils intelligents) donnent accès à un monde d'expériences inédites et reposent sur des décennies de recherche et d'investissements continus. Grâce à d'importants investissements dans la cryptographie, IDEMIA est le fer de lance de l'avancement des briques technologiques au sein de l'industrie et sert ses clients entreprises et gouvernementaux du monde entier. Cette approche proactive nous permet de répondre aux besoins d'aujourd'hui tout en préparant les « vaccins technologiques » de demain.

*Contactez votre représentant IDEMIA pour visiter l'Innovation Hub situé au sein de notre Experience Center basé au siège de Paris-La Défense pour une démonstration privée et l'organisation d'un « atelier d'innovation-conception ».*

* retard accumulé dans la modernisation des infrastructure technologiques

---

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

---