IDEMIA Secure Transactions fait progresser l'authentification post-quantique grâce à une nouvelle technologie basée sur un mécanisme d'encapsulation de clé (KEM).

En remplaçant les signatures numériques traditionnelles par un mécanisme d'encapsulation de clé (KEM), IST est la première entreprise à démontrer une authentification post-quantique efficace sur des cartes PIV.

 # CYBERSÉCURITÉ

POSTÉ LE 06.16.26

IDEMIA Secure Transactions (IST) annonce une avancée majeure en cryptographie post-quantique (PQC) grâce à la conception d'une nouvelle technologie d'authentification qui remplace les signatures numériques traditionnelles par des mécanismes d'encapsulation de clé *(Key Encapsulation Mechanisms ou KEM)*, afin d'offrir une sécurité résistante aux attaques quantiques plus performante et facilement déployable à grande échelle.

Face à l'accélération des menaces quantiques, de nombreuses stratégies de transition vers la cryptographie post-quantique consistent à substituer directement les signatures cryptographiques classiques par des schémas de signature post-quantiques, ce qui engendre une surcharge importante dans des environnements aux ressources limitées. IST a exploré une approche différente en repensant le flux d'authentification lui-même afin de s'appuyer sur des mécanismes d'encapsulation de clé (KEM). Cette approche permet d'obtenir un niveau de sécurité équivalent, tout en améliorant les performances.

Cette approche offre :

- une réduction des échanges de données et des temps d'exécution ;
- une diminution des besoins en puissance de calcul et en mémoire ;
- un déploiement plus efficace sur les systèmes embarqués et les appareils aux ressources limitées.

Pour valider cette innovation dans un environnement réel, IST l'a appliquée avec succès au cadre de vérification d'identité personnelle *(Personal Identity Verification, PIV)* du NIST, devenant ainsi la première entreprise à démontrer le fonctionnement d'une application PIV[1] complète utilisant la cryptographie post-quantique dans une carte à puce.

Cette démonstration prouve qu'il est possible de mettre en œuvre une authentification post-quantique à la fois sécurisée et opérationnelle en conservant les architectures systèmes existantes tout en les préparant à l'ère quantique.

> *La transition vers la sécurité post-quantique ne consiste pas seulement à remplacer les algorithmes ; elle implique également de repenser les protocoles. Notre approche fondée sur*

> *les mécanismes d'encapsulation de clé (KEM) apporte un niveau de sécurité élevé tout en améliorant considérablement l'efficacité. Elle ouvre la voie au déploiement concret et à grande échelle de la cryptographie post-quantique.*
>
> Marc Bertin, CTO d'IDEMIA Secure Transactions

IDEMIA Secure Transactions a déjà établi un solide leadership dans le domaine de la cryptographie post-quantique, à travers une série de premières mondiales : le lancement de la première carte SIM 5G résistante aux ordinateurs quantiques en 2021, la mise sur le marché de la première solution de crypto-agilité pour carte à puce en 2024, la première opération de paiement hors ligne avec une solution de monnaie numérique de banque centrale (CBDC) en 2024. IST a également été reconnue parmi les acteurs les mieux positionnés dans le classement 2025 de Juniper Research consacré à la cryptographie post-quantique.

Cette nouvelle étape confirme la capacité de l'entreprise à transformer les innovations post-quantiques en solutions opérationnelles, déployables à grande échelle et adaptées aux besoins du monde réel.

---

[1] Une carte à puce sécurisée utilisée pour vérifier l'identité et contrôler l'accès aux systèmes informatiques et aux sites physiques, largement utilisée dans les environnements gouvernementaux et les entreprises.
