# The Futurist: Innovation invisible. Réel impact.

Dans ce premier épisode du podcast « *The Futurist: Innovation Stories* », nos intervenants échangent sur les dernières avancées d'IST dans le domaine de la cryptographie post-quantique et de la sécurité digitale.

**# PAIEMENT CONNECTIVITÉ CYBERSÉCURITÉ**

**POSTÉ LE 06.24.25**

The Futurist

Le futur de la sécurité digitale s'écrit aujourd'hui, en silence, mais de façon déterminante. Dans le premier épisode du podcast vidéo « ***The Futurist: Innovation Stories*** », nos intervenants échangent sur les dernières avancées d'IDEMIA Secure Transactions (IST) dans le domaine de la cryptographie post-quantique (PQC). A l'heure où l'informatique quantique devient une réalité tangible, tous les acteurs au sein de l'industrie, des pouvoirs publics et de la recherche doivent se mobiliser. IST n'a pas attendu pour le faire et pose d'ores et déjà les fondations d'un monde sécurisé et résilient face à l'ordinateur quantique, en apportant à ses clients les moyens de protéger leurs infrastructures, de prolonger la durée de vie de leurs produits et de garder une longueur d'avance sur les menaces de demain.

## Cryptographie post-quantique : pourquoi il est urgent d'agir

L'informatique quantique n'a plus rien d'une menace lointaine. Sa capacité à casser les systèmes cryptographiques actuels pourrait tout remettre en question, des transactions financières aux infrastructures nationales. Les équipes R&D d'IST ont identifié très tôt ce tournant majeur et se sont préparées dès 2016 à un avenir où la résilience quantique ne sera pas un choix, mais une nécessité absolue.

> *Les ordinateurs quantiques vont révolutionner l'informatique… mais excelleront aussi dans un domaine : casser la cryptographie actuelle.*
>
> Amaanie Hakim, Vice President of Innovation and IP, IDEMIA Secure Transactions

La cryptographie post-quantique n'est pas qu'une question d'algorithmes, c'est aussi une question d'agilité, d'adaptabilité et de confiance. La démarche d'innovation d'IST s'est concentrée sur des solutions crypto-agiles, prêtes à s'adapter à l'évolution des menaces, de sorte que la sécurité soit non seulement robuste aujourd'hui, mais aussi résiliente à l'avenir.

## Du concept à la preuve : une avancée majeure dans la résistance à l'ordinateur quantique

Passer du concept à l'impact réel est souvent un chemin semé d'embûches. La collaboration entre IDEMIA Secure Transactions et Telefónica a été un moment charnière pour les deux partenaires dans leur cheminement pour faire de la cryptographie post-quantique une réalité. D'une vision partagée d'une sécurité crypto-agile à l'épreuve des évolutions à venir, est née une démonstration concrète qui a marqué les esprits dans tout le secteur.

> *Il ne s'agissait pas d'innover dans le simple but d'innover. Nous avons travaillé main dans la main avec Telefónica pour définir un cas d'usage techniquement avancé et qui aura aussi un réel impact commercial.*
>
> Dario Suarez, Telefonica Global Account Manager, IDEMIA Secure Transactions

Présentée au Mobile World Congress 2025, la démonstration a montré comment les technologies post-quantiques peuvent sécuriser à la fois la gestion à distance des profils eSIM et la transmission des données des compteurs intelligents. En utilisant des algorithmes post-quantiques pour les certificats digitaux et la signature des profils, la solution prévient l'usurpation et l'altération, y compris face aux menaces futures de l'ère quantique.

La solution repose sur deux principes clés. Premièrement, toutes les opérations cryptographiques du compteur intelligent sont gérées au sein de l'eSIM, en utilisant l'applet standardisée IoT SAFE. Le système d'exploitation du compteur fait appel à cette applet pour traiter les processus cryptographiques, ce qui permet de réaliser ceux-ci dans un environnement sécurisé et protégé contre les altérations. Deuxièmement, la solution utilise l'infrastructure eSIM complète déjà disponible qui comprend le gestionnaire d'abonnement (*Subscription Manager*, ou SMDP+) et le gestionnaire à distance eSIM IoT (*eSIM IoT Remote Manager*, ou eIM) afin de permettre des mises à jour cryptographiques à distance, sans nécessiter d'accès physique à l'appareil ni d'intervention sur site.

Grâce à l'intégration des bibliothèques cryptographiques directement dans le profil eSIM, le compteur peut facilement être mis à niveau pour prendre en charge les versions post-quantiques de protocoles de sécurité, tels que le TLS ( *Transport Layer Security*) qui protège les échanges de données avec l'entreprise qui gère le service. Ces mises à jour sont effectuées à distance, ce qui démontre un niveau élevé de crypto-agilité, c'est-à-dire la capacité d'adapter les mécanismes cryptographiques au fil du temps sans remplacement de matériel. Cela permet de maintenir une forte protection des appareils sur le terrain, même lorsque les menaces évoluent.

> *L'objectif de ce projet était de démontrer que nous pouvions mettre à jour la cryptographie à distance dans des puces déjà déployées. Il s'agissait de passer de la cryptographie classique à la cryptographie post-quantique, et même de remplacer un algorithme post-quantique par un autre, tout en maintenant la sécurité.*
>
> Antton Bodin, Embedded Software Engineer, IDEMIA Secure Transactions

La démonstration a validé non seulement la faisabilité technique du passage à la cryptographie post-quantique dans des environnements IoT contraints mais aussi l'intérêt concret que cela représente pour aider les clients à sécuriser leurs systèmes dès maintenant et assurer l'adaptabilité de ceux-ci face aux enjeux à venir.

## Voir plus loin : pérenniser la confiance

La force de cette histoire ne tient pas seulement à la technologie employée, mais aussi à l'état d'esprit qui l'anime. A travers cette démonstration, IDEMIA Secure Transactions prouve que certaines des innovations les plus transformatrices se déroulent parfois en coulisses.

> *Le post-quantique est une innovation très technique et quasi-invisible. (...) Cela nécessite un effort conjoint, une collaboration réelle entre toutes les parties prenantes.*
>
> Benoît Collier, VP Product Business Line, IDEMIA Secure Transactions

En consolidant les fondations cryptographiques du monde digital, IST aide ses clients à préparer l'avenir, sans perturbation, ni compromis. C'est une preuve que la véritable innovation n'est pas toujours visible, mais que ses effets sont durables : une confiance qui persiste, des systèmes résilients et une sécurité capable d'évoluer avec le temps.