IDEMIA

IDEMIA et Telefónica présentent une technologie eSIM post-quantique

Protéger les réseaux intelligents des services d'utilité publique et les objets connectés contre les cybermenaces post-quantiques

CONNECTIVITÉ CYBERSÉCURITÉ

POSTÉ LE 07.18.25

Lors du Mobile World Congress (MWC) 2025 à Barcelone, **IDEMIA Secure Transactions (IST)** et **Telefónica** ont dévoilé une preuve de concept innovante. La démonstration de celle-ci est désormais disponible dans leurs Experience Centers respectifs. Cette démonstration consiste à utiliser une technologie eSIM post-quantique (intégrant des capacités crypto-agiles et des mesures de sécurité résistantes aux attaques quantiques), pour la protection d'appareils IoT utilisés dans les réseaux intelligents des services d'utilité publique.

Demander une démo

Sécurisation des réseaux de services publics intelligents contre les menaces émergentes

Les réseaux de services d'utilité publique, tels que ceux dans lesquels sont utilisés des compteurs intelligents d'eau, de gaz et d'électricité, devraient connaître une croissance de 10% au cours de la prochaine décennie. * Ces appareils à longue durée de vie restent généralement sur le terrain pendant 10 à 15 ans, ce qui en fait des cibles privilégiées face aux menaces de cybersécurité qui émergent. Il en résulte le besoin critique de déployer des solutions post-quantiques pour protéger à la fois l'infrastructure technologique constituée par ces appareils et les données.

La démonstration d'IST et Telefónica porte sur un compteur intelligent tel qu'il serait déployé dans un environnement IoT. Elle consiste à faire passer celui-ci de façon transparente de la sécurité actuelle à une sécurité résistante à l'ordinateur quantique grâce à une eSIM post-quantique dotée de capacités crypto-agiles. La solution d'IST, intégrée par Telefónica, permet de protéger les communications mobiles utilisées d'une part pour charger à distance des profils eSIM et d'autre part pour transmettre des relevés de compteurs. Cette approche préserve la confidentialité et empêche toute falsification, garantissant ainsi la sécurité et l'intégrité des données transmises.

Algorithmes quantiques et crypto-agilité

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.

Cette configuration permet de s'assurer que même les attaques les plus puissantes à l'avenir, par exemple celles utilisant l'informatique quantique pour usurper l'identité d'un opérateur mobile, modifier des profils eSIM ou intercepter des données lors de leur transmission, pourront être enrayées. Et si d'autres adaptations s'avéraient nécessaires, la cryptographie pourra de nouveau être mise à jour à distance via le même canal eSIM sécurisé.

Dans les environnements IoT industriels, où la longue durée de vie et les déploiements à grande échelle rendent les mises à niveau des équipements coûteuses et complexes, ce niveau de crypto-agilité change la donne. Il permet aux entreprises qui gèrent les services d'utilité publique de garder une longueur d'avance sur les nouvelles menaces de sécurité sans avoir à remplacer les appareils ni à envoyer des techniciens sur le terrain. Cela contribue ainsi à la résilience, au respect des normes et à la continuité opérationnelle au fil du temps.

---

*Source : Transforma Insights IoT Forecast Database, 2024
