COMMUNIQUÉ DE PRESSE
24 février 2023
Paris La Défense

Des appels téléphoniques sécurisés par Cryptographie Post-Quantique – un premier pilote mondial réussi par Thales

- Thales, leader en hautes technologies, a expérimenté avec succès des appels téléphoniques cryptés de bout en bout, testés pour être résilients à l'ère post-quantique.
- Le pilote a été réalisé avec l'application mobile sécurisée « Cryptosmart » de Thales et ses cartes SIM 5G, testant ainsi un appel chiffré de 'mobile à mobile' sur smartphones traditionnels.
- Toutes les données échangées lors de l'appel sont chiffrées pour résister aux attaques post-quantiques grâce à une approche de cryptographie hybride, combinant des mécanismes de défense pré et post-quantiques.

Thales, leader mondial en cybersécurité, a créé la première application intégrant de la Cryptographie Post-Quantique (PQC) dans son application mobile sécurisée « Cryptosmart », utilisant sa SIM 5G comme un coffre-fort à PQC. Pour ce pilote, la cryptographie hybride (crypto pré et post-quantique) a été utilisée lors d'un appel téléphonique entre deux appareils pour protéger les informations échangées pendant l'appel. Thales investit et teste des technologies en cybersécurité post-quantique depuis plus d'une décennie afin de se préparer aux nouvelles menaces.

Même si les prototypes actuels de l'ordinateur quantique[1] sont encore loin de constituer une menace pour la cryptographie à clé publique (Public Key Cryptography 'PKC'), il est essentiel de commencer à chercher et trouver des solutions. Cette recherche est d'autant plus nécessaire qu'il existe par exemple une attaque qui consiste à « stocker maintenant, décrypter plus tard » des données et messages qui seraient échangés et enregistrés de nos jours mais déchiffrés une fois l'arrivée d'ordinateurs

quantiques. Cela signifie que la sécurité des infrastructures numériques actuelles basée sur la cryptographie à clé publique (PKC) peut déjà être vulnérable à une attaque quantique à venir.

Ces menaces sont particulièrement critiques lors de scénarios impliquant des informations hautement sensibles, telles que des informations classifiées, qui seraient échangées via un appel téléphonique. Pour adresser ce type de scénarios, Thales s'est lancé le défi de cette expérimentation pour tester la fiabilité et la qualité de ses solutions, de ses cartes SIM 5G à ses logiciels de communication sécurisés.

En effet cette première solution mobile résistante à l'ère post-quantique - *qui combine l'application "Cryptosmart " de Thales à sa carte SIM 5G* - utilise la cryptographie hybride, telle qu'elle est recommandée par le NIST (National Institute of Standards and Technology). Ainsi 'CRYSTALS- Kyber', l'un des quatre algorithmes retenus par le NIST[2], est l'algorithme PQC intégré nativement à la SIM 5G de Thales, et que l'application 'Cryptosmart' utilise pour chiffrer la communication.

« Construire des protections contre des menaces qui n'existent pas encore peut sembler particulièrement ardu. Mais avec l'arrivée imminente de l'informatique quantique c'est exactement à cela que la communauté mondiale en cybersécurité se confronte aujourd'hui. L'ère post-quantique est encore à venir, mais à mesure que l'informatique quantique se développe, c'est précisément la pratique de l'agilité cryptographique via ce type de pilotes, qui aide Thales et ses clients à se préparer », a déclaré **Philippe KERYER, Directeur général adjoint Stratégie, Recherche et Technologie chez Thales.**

[1] des ordinateurs capables d'effectuer certaines tâches beaucoup plus rapidement que les ordinateurs actuels à grande échelle.

[2] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

À propos de Thales

Thales (Euronext Paris: HO) est un leader mondial des hautes technologies qui investit dans les innovations du numérique et de la « deep tech » – connectivité, big data, intelligence artificielle, cybersécurité et quantique – pour construire un avenir de confiance, essentiel au développement de nos sociétés. Le Groupe propose des solutions, services et produits qui aident ses clients – entreprises, organisations, Etats - dans les domaines de la défense, de l'aéronautique, de l'espace, du transport et de l'identité et sécurité numériques, à remplir leurs missions critiques en plaçant l'humain au cœur des décisions.

Thales compte 81 000 collaborateurs dans 68 pays. En 2021, le Groupe a réalisé un chiffre d'affaires de 16,2 milliards d'euros.

CONTACT PRESSE

Thales, Relations Presse
Identité et sécurité numériques
Vanessa Viala
+33 (0)6 07 34 00 34
vanessa.viala@thalesgroup.com

PLEASE VISIT

Thales Digital Identity & Security
Thales unveils three quantum technologies set to revolutionise the world of tomorrow | Thales Group
Business Data Protection and Cybersecurity | Ercom