

Sécurité de l' IoT : DigiCert s'allie à Gemalto et Isara

DigiCert, Gemalto et Isara ont annoncé un partenariat d'ampleur. Il porte sur le développement de certificats numériques quantiques et la gestion sécurisée des clés pour objets connectés (IoT). Deepika Chauhan, vice-présidente 'marchés émergents' du fournisseur de solutions d'infrastructure à clés publiques (PKI) DigiCert, s'est exprimée.

Le partenariat vise à « protéger appareils connectés et réseaux contre les nouvelles menaces que l'implémentation d'[ordinateurs quantiques](#) fera peser sur la sécurité », a-t-elle expliqué. Et d'ajouter : l'alliance consiste donc « à garantir que les systèmes connectés de véhicules, de systèmes de contrôle industriel, de dispositifs médicaux, de centrales nucléaires et d'autres infrastructures critiques seront à l'abri de ces menaces dans cinq, dix et vingt ans ». Voeu pieux de la firme américaine ?

Cybersécurité post-quantique

Aujourd'hui, de nombreux dispositifs connectés s'appuient sur le chiffrement RSA (un acronyme qui reprend les initiales de Rivest-Shamir-Adleman) et ECC (Elliptic Curve Cryptography) pour protéger l'intégrité des communications électroniques.

Or, des « experts estiment que l'aube de l'[informatique quantique](#) à grande échelle arrivera dans les huit à dix ans », a déclaré Scott Totzke, directeur général de la société canadienne Isara (sécurité quantique). « Il ne sera alors plus possible de se fier au chiffrement à clé publique tel que nous le connaissons aujourd'hui », a-t-il ajouté.

Mieux vaut s'y préparer dès maintenant.

Pour rester dans la course face à d'autres prestataires, Isara, Gemalto et DigiCert veulent « garantir la sécurité d'un élément fondamental de la pile de sécurité – les certificats racines – en intégrant le chiffrement quantique », a-t-il insisté par voie de communiqué.

Et ce que les clients (fabricants d'objets connectés, grandes entreprises...) et partenaires (fournisseurs de services de sécurité managés...) privilégient un hébergement sur site, dans le cloud public ou en environnement hybride.

Todd Moore, vice-président produits de chiffrement du franco-néerlandais Gemalto (sécurité numérique), veut croire que l'alliance ainsi formée « aidera les entreprises à développer des opérations cryptographiques sécurisées et à l'épreuve du temps ».

(crédit photo : fumi via VisualHunt / CC BY-NC-SA)