**Thales et Senetas ont collaboré pour le lancement de la première solution au monde à permettre le chiffrement de réseau résistant à l'informatique quantique, protégeant ainsi les données des clients (à des vitesses atteignant 100 Gb/s) contre les attaques de demain, décuplées par la révolution quantique. Considérée comme l'une des menaces les plus importantes pour la cybersécurité, l'informatique quantique devrait rendre obsolètes de nombreuses méthodes de sécurité actuelles, notamment la cryptographie.**

Dans la mesure où l'on estime qu'un ordinateur quantique opérationnel et hors laboratoire sera une réalité d'ici cinq à dix ans, des standards minimums de sécurité sont en cours d'élaboration pour protéger les données dans un monde quantique. Le *National Institute of Standards and Technology* (NIST) américain procède actuellement à la sélection d'un algorithme de cryptographie quantique qui deviendra d'ici fin 2022 la référence en la matière. Dans l'attente de cette sélection, la collaboration entre Thales et Senetas soutient les finalistes actuels (parmi lesquels, l'algorithme Falcon de Thales), assurant ainsi une transition fluide vers la formule gagnante qui devrait être choisie par le NIST en 2022. La solution fournie par les deux entreprises supporte également les dernières normes de l'Institut européen des normes de télécommunication relatives aux modes de création, de protection et de distribution des clés quantiques — une importante fonctionnalité de sécurité émergente qui peut être utilisée dans les réseaux 5G.

**La protection de demain**

En permettant aux clients de combiner le chiffrement conventionnel et la résistance quantique au sein d'une même et unique plateforme de sécurité réseau, la solution assure également une protection durable des données dans un monde quantique. Les données aujourd'hui subtilisées par les hackers sont rendues inexploitables grâce à des clés de chiffrement de plus en plus répandues au sein des organisations. La puissance des superordinateurs de demain permettra de casser ces clés de chiffrement classiques, libérant ainsi la voie aux hackers.

L'adoption des nouvelles normes associée à la solution de Thales protégera toutes les données critiques face aux ordinateurs de de demain et les rendra inutilisables sans la bonne clé, résistante au quantique.

> *« À mesure que l'informatique quantique devient une réalité, les entreprises du monde entier doivent élaborer une stratégie de sécurité quantique et entamer la planification de la mise en œuvre d'un chiffrement résistant à l'informatique quantique le plus tôt possible ». Cette plateforme de chiffrement de réseau à haut débit, la première à être commercialisée, assure un chiffrement résistant à la dimension quantique avec la technologie de chiffrement actuelle. Nos clients des secteurs gouvernementaux, de la défense et des affaires peuvent assurer une transition sûre vers un futur monde à sécurité quantique, avec la garantie que les données sont protégées à long terme, »*

a déclaré Andrew Wilson, PDG de Senetas.

> *« Il est essentiel que les entreprises comprennent que les standards de chiffrement actuels ne sont pas adaptés à un monde quantique. Les hackers ont conscience que le quantique est proche et s'emploient activement à subtiliser des données aujourd'hui pour pouvoir y accéder à l'avenir. Les grandes organisations et les multinationales sont particulièrement exposées en raison de leurs obligations en matière de conformité et de confidentialité. Les entreprises ne peuvent pas se permettre d'attendre, le moment est venu de revoir leur stratégie de sécurité quantique, »*

a déclaré Todd Moore, vice-président des solutions de cryptage chez Thales.