Obstacles majeurs à l'adoption de la Cryptographie Post-Quantique

Le manque de réglementations claires, d'éducation et d'expertise freinant la mise en œuvre de la PQC.

IDENTITÉ

POSTÉ LE 02.26.25

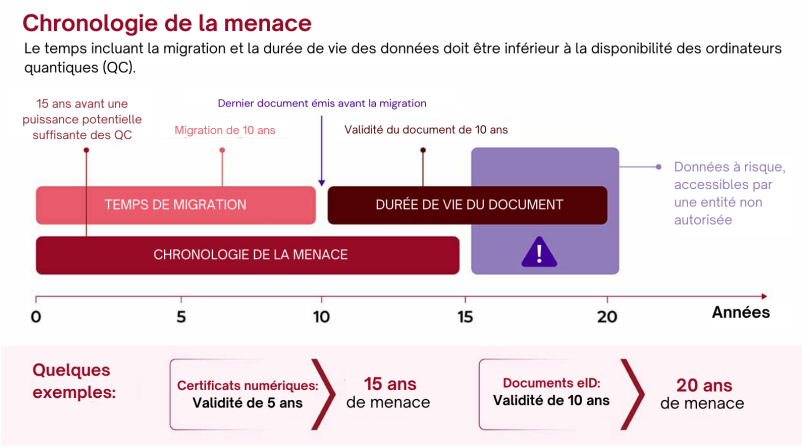
Avec l'annonce ce mois-ci par Microsoft * de la fabrication réussie de son premier processeur quantique basé sur un matériau novateur connu sous le nom de « conducteur topologique », le marché de l'identité et des documents sécurisés est confronté à un défi crucial : garantir la sécurité des systèmes cryptographiques face aux menaces potentielles des ordinateurs quantiques. Une récente enquête sur la cryptographie post-quantique (PQC) révèle des perspectives éclairantes de la part des professionnels du secteur, mettant en évidence à la fois leur niveau de préparation et les obstacles à l'adoption des solutions PQC.

L'enquête, organisée par Reconnaissance en collaboration avec IDEMIA Smart Identity, s'est déroulée entre septembre et novembre 2024. Un nombre restreint de professionnels sélectionnés dans le domaine de la PQC et de la cybersécurité ont partagé leur point de vue sur le niveau de préparation des organisations privées et publiques à l'ère des ordinateurs quantiques.

Les résultats de l'enquête montrent une forte sensibilisation des répondants quant à l'impact potentiel de l'informatique quantique (QC) sur les systèmes cryptographiques actuels. Sur 35 participants, 29 ont évalué leur compréhension comme « Bonne », « Très bonne » ou « Excellente », tandis que seulement 6 l'ont jugée « Moyenne » ou « Faible ». Ce niveau de conscience élevé est essentiel, car il souligne la reconnaissance par l'industrie de la menace imminente des ordinateurs quantiques.

La conviction quant à l'émergence des ordinateurs quantiques est quasi unanime parmi les participants à l'enquête. Seuls quatre répondants ont exprimé du scepticisme, estimant que la QC est « Peu probable » ou déclarant « Je ne pense pas que cela arrivera ». Cette vision majoritaire met en évidence l'urgence de se préparer à un avenir sécurisé face aux menaces quantiques, la plupart des professionnels anticipant l'avènement de la QC d'ici la prochaine décennie.

L'enquête met en évidence un consensus fort sur l'importance d'implémenter la PQC au sein des organisations. 15 répondants l'ont jugée « Très importante », 9 l'ont qualifiée de « Moyennement » ou « Légèrement importante » et 1 seul participant a estimé qu'elle n'était 'Pas du tout importante'. Cette prise de conscience est un indicateur positif que l'industrie reconnaît la nécessité de passer à des solutions cryptographiques résistantes aux menaces quantiques pour protéger les données sensibles et les informations personnelles identifiables. Le graphique « Threat timeline » ou « Chronologie de la menace» illustre l'urgence de la transition vers ces systèmes, soulignant le risque de « stocker maintenant, décrypter plus tard », qui met en danger les documents d'identité électroniques sensibles en raison de leur durée de vie de 10 ans.



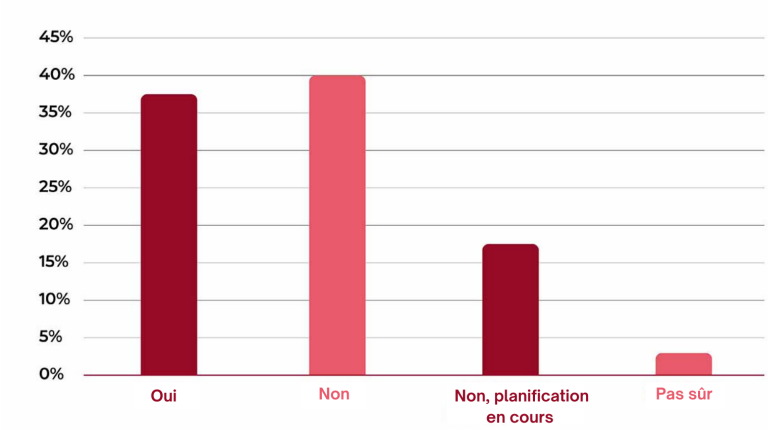
Principaux obstacles : Manque de connaissances, d'éducation et de réglementations & normes

Malgré la prise de conscience et la reconnaissance, d'importantes barrières à l'adoption de la PQC subsistent. Les principaux défis identifiés dans l'enquête sont le manque de connaissances et d'expertise ainsi que la complexité technique des technologies PQC. De nombreuses organisations ne disposent pas des compétences nécessaires pour mettre en œuvre ces solutions de manière efficace. Les professionnels de la cybersécurité, qui sont généralement chargés de cette mission, n'ont souvent pas de formation en cryptographie quantique. La complexité technique des technologies PQC représente un obstacle majeur, obligeant les organisations à naviguer dans un paysage technologique complexe pour développer et déployer des solutions résistantes aux ordinateurs quantiques.

L'industrie des documents d'identité et de sécurité n'est pas la seule à faire face à ces défis. Selon un article de Forbes**, des centaines d'entreprises recherchent activement des experts en informatique quantique. Cette demande souligne la tendance globale du secteur et le besoin croissant de talents spécialisés pour accélérer l'adoption de la PQC.

Favorablement, comme l'illustre le graphique ci-dessous, un peu plus de 50 % des répondants ont déjà commencé à mettre en œuvre des solutions PQC ou prévoient de le faire. Cette approche proactive démontre un engagement envers la sécurisation des systèmes cryptographiques contre les futures menaces quantiques. Cependant, ces organisations cherchent également un accompagnement et des conseils pour surmonter les complexités de l'adoption de la PQC.

Question : Votre organisation a-t-elle commencé à étudier ou à mettre en œuvre des solutions PQC ?



Les répondants à l'enquête ont identifié trois initiatives essentielles pour faciliter l'adoption de la PQC : une sensibilisation accrue, une meilleure éducation sur le sujet et une clarification des réglementations et des normes. Il est évident qu'il existe un besoin urgent de programmes éducatifs pour améliorer la compréhension des technologies PQC et de leur mise en œuvre. Des réglementations et des normes claires et cohérentes sont essentielles pour guider les organisations dans l'élaboration de leurs stratégies PQC. Au sein de chaque organisation, il reviendra au service de la sécurité de l'information de devenir le point de contact principal, en apportant l'expertise et les ressources nécessaires pour accompagner cette transition.

> *Lorsque nous discutons de la préparation à la PQC avec nos clients, il devient évident que, bien que le sujet figure en tête des priorités, les professionnels chargés de cette responsabilité ne savent tout simplement pas par où commencer. Nous constatons un respect pour la complexité du sujet, que nous ne pourrons résoudre qu'en unissant nos forces en tant qu'industrie. Nous ne doublerons pas le nombre d'experts en PQC du jour au lendemain, mais nous sommes suffisamment nombreux pour donner les conseils pertinents à ce moment précis.*
>
> Jerome Boudineau – Expert PQC chez IDEMIA Smart Identity

Le passage à la cryptographie post-quantique est complexe et semé d'embûches, mais les résultats de l'enquête montrent que le marché de l'identité et des documents sécurisés progresse de manière significative. Avec une compréhension approfondie des impacts potentiels de la QC, une conviction forte en son émergence et une reconnaissance de l'importance de la PQC, l'industrie est bien positionnée pour relever les défis à venir. En surmontant les obstacles liés aux connaissances et à la complexité technique, et en sollicitant le soutien des acteurs clés, les organisations peuvent réussir cette transition cruciale.

---

*https://news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/
**https://www.forbes.com/councils/forbestechcouncil/2024/12/12/beyond-quantum-where-to-look-for-quantum-ready-talent/
