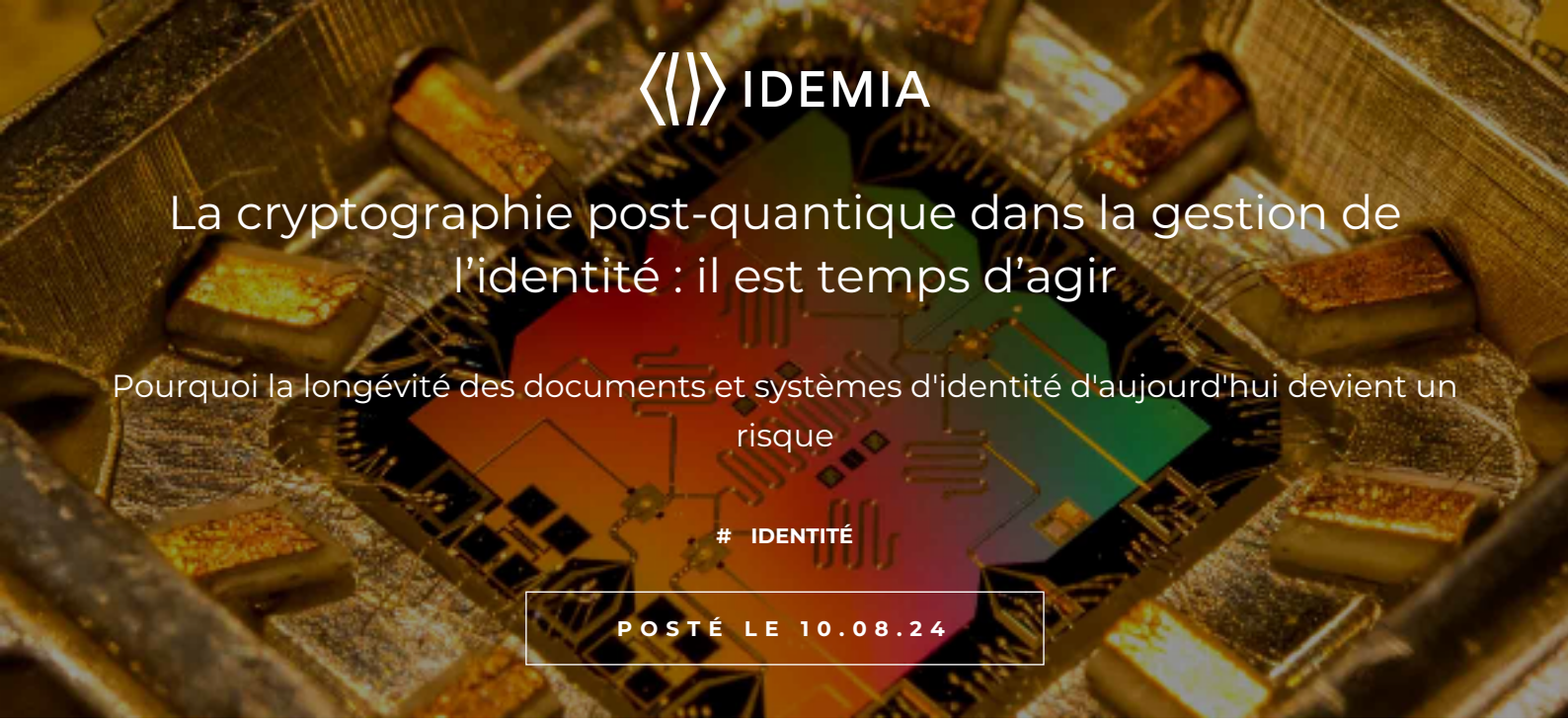

La cryptographie post-quantique dans la gestion de l'identité : il est temps d'agir

Pourquoi la longévité des documents et systèmes d'identité d'aujourd'hui devient un risque

 # IDENTITÉ

POSTÉ LE 10.08.24

La plupart des gens ont entendu parler des ordinateurs quantiques d'une manière ou d'une autre et comprennent qu'ils impliquent un risque élevé pour la sécurité de nos données. D'après une étude de McKinsey[1], les secteurs de l'assurance, de la banque et le secteur public risquent d'être les premiers ciblés en raison de la longue durée de validité des données traitées et de la durée de vie prolongée des systèmes concernés. Toutefois, sans une compréhension claire de la manière dont les futures attaques pourraient se présenter, de nombreux professionnels de la sécurité ne savent pas comment s'y préparer.

Examinons de plus près la situation dans laquelle nous nous trouvons.

Les ordinateurs quantiques ne seront pas largement disponibles de sitôt. En réalité, la première menace tangible ne devrait pas apparaître avant environ dix ans. Plusieurs défis subsistent à leur apparition :

- **La taille :** La plupart des ordinateurs quantiques actuels sont extrêmement volumineux, occupant plusieurs mètres carrés, ce qui les rend accessibles uniquement aux grandes organisations.
- **Les conditions de fonctionnement :** ils nécessitent souvent des températures extrêmement basses pour fonctionner, proches du zéro absolu (-273 °C).
- **La correction d'erreurs :** pour chaque qubit effectif, de multiples qubits supplémentaires sont requis pour corriger les erreurs de calcul, ce qui nécessite des ordinateurs quantiques très volumineux. La réduction de ces erreurs de calcul est une priorité.

Les documents d'identité physiques modernes délivrés aujourd'hui ont une durée de validité moyenne de 10 ans à compter de leur émission. La durabilité du polycarbonate et les éléments de sécurité remarquables utilisés actuellement font que les citoyens ne ressentent pas le besoin de renouveler volontairement leur carte d'identité ou passeport avant la date d'expiration. Les systèmes de gestion de l'identité à travers le monde présentent des situations très variées. Les incidents de sécurité et les attaques augmentent rapidement et deviennent de plus en plus sophistiqués. Cela nécessite une adaptation constante pour développer des patches et mettre à jour les systèmes tout en assurant une cohérence globale.

Malheureusement, cette approche n'est pas toujours suivie. Si l'on ajoute à cela la sensibilité des données des citoyens qui y sont stockées (même en faisant abstraction des données biométriques), tout le monde comprendra qu'il n'est pas possible d'attendre la survenue de la première violation ou la mise en place de toutes les normes et règlementations pour se préparer à l'ère post-quantique.

> *L'important est d'entamer ce parcours dès aujourd'hui et de ne pas attendre la dernière minute.*
>
> Rob Joyce, Directeur de la cybersécurité de la NSA (Agence nationale américaine de sécurité)

Comment se préparer dès maintenant à une menace qui semble virtuelle ? La réponse réside dans la crypto-agilité et l'adoption d'une approche hybride.

L'agilité cryptographique

L'agilité cryptographique peut être définie comme la capacité à passer facilement d'un système cryptographique à un autre. Actuellement, nous manquons clairement d'une perspective à long terme sur les algorithmes de cryptographie post-quantiques, particulièrement en matière de sécurité. Même si les algorithmes sélectionnés ont été étudiés, de nouvelles améliorations peuvent amener à reconsidérer leur utilisation ou leur configuration, et même à effectuer des changements vers d'autres algorithmes.

Il y a donc un besoin évident de pouvoir remplacer facilement un algorithme post-quantique par un autre, ou du moins de pouvoir augmenter la taille des clés utilisées. Les systèmes de gestion de l'identité doivent être modulaires et adaptables, pour nous permettre de les mettre à jour après leur déploiement. Ce n'est qu'à ces conditions qu'ils seront adaptés aux évolutions futures.

Interopérabilité et cryptographie hybride pour une transition progressive

Aujourd'hui, la plupart des systèmes s'appuient sur la cryptographie pré-quantique et pourraient rester en opération pendant des décennies. Il est nécessaire d'effectuer une transition sans heurts vers la cryptographie post-quantique tout en garantissant que les systèmes actuels restent compatibles avec les nouveaux systèmes de cryptographie post-quantique (PQC). L'intégration simultanée des algorithmes pré-quantiques et post-quantiques dans un système permettra aux systèmes pré-quantiques de fonctionner aux côtés des systèmes post-quantiques et de maintenir l'interopérabilité pendant la transition vers la cryptographie post-quantique. Par exemple, un citoyen disposant d'un passeport électronique sécurisé contre les menaces quantiques devrait pouvoir franchir les frontières de pays qui n'ont pas encore mis en œuvre des systèmes de frontière post-quantiques, et vice versa.

De plus, étant donné que nous manquons d'expérience suffisante dans les algorithmes PQC, il est essentiel de concevoir des systèmes avec de la cryptographie hybride. Cette dernière implique deux couches de protection : une avec un algorithme pré-quantique et une autre avec un algorithme post-quantique, offrant ainsi une sécurité dans les deux mondes. Si une attaque classique contre l'algorithme post-quantique est découverte, l'algorithme pré-quantique au sein de la solution hybride continuera de fournir une protection.

En outre, tous les experts s'accordent à dire que cette phase de préparation à l'ère post-quantique sera longue et complexe. Par conséquent, il est essentiel de créer un plan détaillé d'atténuation des risques qui priorise d'abord les actifs les plus critiques, afin de garantir que les ressources limitées soient utilisées là où elles sont le plus nécessaires.

L'identification des actifs les plus critiques dans la gestion de l'identité

Comme dans tout plan d'atténuation des risques, la première étape critique est l'analyse des actifs les plus vulnérables. Dans la gestion de l'identité, nous devons d'abord protéger les éléments exposés à des tiers (points d'entrée du réseau) :

les jetons tels que les badges d'entreprise ou les cartes d'identité électroniques pour un usage numérique (par exemple, signatures, accès à des portails gouvernementaux), qui permettent aux utilisateurs de se connecter aux systèmes et les rendent vulnérables aux attaques.

Il est tout aussi important de veiller à ce que les données restent authentiques et confidentielles. Dans le cas d'un enrôlement impliquant la capture de données biométriques, le transfert des données vers une base de données centrale pourrait être vulnérable aux interceptions. Il est donc fondamental d'assurer en priorité la protection des données et de se préoccuper de la sécurité des canaux dans un deuxième temps.

Conclusion : soyez préparés, agiles et résilients

Face à toutes les incertitudes évoquées concernant les ordinateurs quantiques, notamment en ce qui concerne leur disponibilité, il est compréhensible que certains adoptent aujourd'hui une attitude de l'autruche. Se préparer à une situation aussi incertaine paraît difficile et semble être une perte potentielle de temps et d'argent. Cependant, comme nous l'avons expliqué, l'application de quelques principes clés permet déjà d'atteindre une première étape importante dans notre préparation post-quantique :

1. Assurez-vous que vos systèmes de gestion de l'identité sont agiles sur le plan cryptographique.
2. Commencez à actualiser votre système de gestion de l'identité avec la cryptographie post-quantique, tout en veillant à rester en conformité avec les systèmes pré-quantiques.
3. Mettez d'abord à jour les actifs les plus vulnérables

À propos de l'auteur :

Jérôme Boudineau, Responsable de produit et expert en cryptographie post-quantique chez IDEMIA Smart Identity. IDEMIA Smart Identity occupe une place de premier plan en matière de conseil auprès des États et des organisations dans la transition leurs systèmes de gestion de l'identité vers l'ère post-quantique.

Quelle est votre niveau de préparation au PQC ?

Nous vous invitons à répondre à cette courte enquête pour nous aider à comprendre la préparation de votre organisation, ainsi que les perceptions et l'état actuel du PQC dans le domaine de la gestion des identités.

Vos réponses nous sont extrêmement précieuses!

Répondez à l'enquête

---

[1] How to prepare for post quantum cryptography (Comment se préparer à la cryptographie post-quantique ?)| McKinsey

---