# 3 avancées technologiques en cybersécurité qui devraient intéresser les CISO et CTO

Les derniers progrès en matière de gestion des clés et de sécurité cryptographique

# PAIEMENT CONNECTIVITÉ CYBERSÉCURITÉ

POSTÉ LE 10.23.25

Face à l'essor et à la sophistication des cybermenaces et dans un contexte où les tensions géopolitiques alimentent les risques numériques, les besoins en cybersécurité augmentent dans tous les secteurs. La perspective du *« Q-Day »*, le moment où des ordinateurs quantiques cryptographiquement pertinents (CRQC) pourraient casser les systèmes de chiffrement actuels, rend d'autant plus important, pour les CISO, les équipes de sécurité informatique et les développeurs de logiciels, le fait de continuer à renforcer les défenses cryptographiques et d'en assurer la résilience. Explorons certaines des solutions qui peuvent donner un temps d'avance aux entreprises en leur offrant la protection des données évolutive et pérenne dont elles ont besoin.

## 1/ Repenser la gestion des clés cryptographiques grâce à un HSM composé d'une matrice d'éléments sécurisés

Qu'ils soient déployés dans des data centers privés ou hébergés dans le cloud, les HSM traditionnels reposent généralement sur **un processeur unique et puissant**. Dans ce modèle, la sécurisation du processeur et de la mémoire du HSM passe par la protection de la carte électronique dans un boîtier sécurisé contre les intrusions. Cette architecture classique peut générer certaines contraintes d'un point de vue matériel, en particulier en termes de coûts de déploiement, d'exploitation et de maintenance. Qui plus est, le recours à un processeur unique, qui implique une **ségrégation *logicielle*** des clés et des opérations cryptographiques, peut conduire à des conflits entre processus concurrents.

Repenser l'architecture du HSM autour d'une **matrice d'éléments sécurisés** permet d'intégrer la sécurité matérielle dès la conception et de renforcer l'isolation des environnements clients. Cette approche rend possible une **ségrégation *physique* des opérations cryptographiques**, avec des ressources matérielles et des enclaves sécurisées dédiées.

Un autre intérêt majeur à utiliser des éléments sécurisés basse consommation**,** outre le fait de réduire la consommation d'énergie[1], est de permettre le **stockage à froid**. L'utilisation d'éléments sécurisés dispense d'un système de protection alimenté par une batterie et évite ainsi les désagréments d'une reconfiguration en cas de défaillance de celle-ci. Ce modèle innovant de HSM, conçu par IDEMIA Secure Transactions (IST) et d'ores et déjà certifié FIPS 140-3, ouvre de nouvelles perspectives pour optimiser ou accélérer le déploiement de services de chiffrement, d'authentification et de signature digitale.

## 2/ Des librairies cryptographiques prêtes pour l'ère quantique : réduction des risques, économie de temps et conformité assurée

À l'approche de l'ère quantique, le temps presse pour déployer de nouveaux algorithmes et protocoles. Aujourd'hui, les développeurs peuvent s'appuyer sur des librairies cryptographiques open source avec un degré de confiance raisonnable. Mais contrairement aux standards cryptographiques éprouvés et fiables sur lesquels nous comptons depuis des décennies, la cryptographie post-quantique n'en est qu'à ses débuts**. Peu de personnes maîtrisent réellement toutes les subtilités de la migration vers le post-quantique**, et les normes devraient continuer à évoluer.

Pour s'assurer que leurs librairies cryptographiques seront maintenues dans la durée, et au rythme nécessaire, les organisations ont tout intérêt à se tourner vers des **librairies cryptographiques sous licence**. Adossées à des **contrats de maintenance**, celles-ci offrent également des **garanties** telles que la **signature du code**, ce qui permet de s'assurer de la provenance de celui-ci et d'éviter l'introduction involontaire de vulnérabilités dans les systèmes. **Le support pour intégrer la cryptographie post-quantique** sera également un élément déterminant pour les organisations qui ne disposent pas de l'expertise interne, notamment lorsqu'il s'agira de déployer des librairies dans des environnements matériels ou logiciels non standard.

Remplacer les librairies cryptographiques de tous les appareils, logiciels et services que nous utilisons chaque jour représente un défi considérable. **Il ne s'agit pas seulement de bien faire les choses, une bonne fois pour toutes, et de ne plus y penser.** Une mise en œuvre rigoureuse dans chaque environnement, un suivi continu, des tests rigoureux, des mises à jour régulières et des méthodes fiables de mise en conformité seront **la clé de la résilience post-quantique**. C'est là que des librairies cryptographiques conçues par des spécialistes aguerris dans des secteurs hautement réglementés, ainsi que l'accompagnement que ces experts sont en mesure d'apporter, feront toute la différence  En choisissant des librairies sous licence, les organisations s'assurent de **respecter le niveau d'engagement requis** par les nouvelles réglementations sur la cybersécurité, tant en termes de qualité et de fiabilité du code source que de rapidité de correction en cas de vulnérabilité.

## 3/ La crypto-agilité au service d'une cybersécurité pérenne et en profondeur

Étroitement liée aux défis de la résilience post-quantique, l'agilité cryptographique (ou crypto-agilité), offrira aux CISO et aux équipes de sécurité IT des capacités inédites pour effectuer des **mises à jour de sécurité en profondeur** des appareils et systèmes sur le terrain**. L'époque des mises à jour ponctuelles est révolue.** Le secteur bancaire, par exemple, a connu plusieurs changements cryptographiques au cours des dernières décennies.[2] À mesure que les systèmes deviennent plus complexes et que les acteurs sont davantage interconnectés, **ces mises à jour demandent toujours plus de temps et de ressources**, un luxe que le secteur ne pourra plus se permettre à l'ère post-quantique. Cela vaut également pour les réseaux mobiles, les infrastructures énergétiques, les systèmes de santé, les véhicules connectés et tout autre système utilisant des technologies de chiffrement.

Indépendamment du défi quantique, la crypto-agilité constitue **un investissement à long terme dans la cyber-résilience**. Plutôt que de planifier et d'exécuter à répétition des migrations massives de systèmes et d'appareils, les professionnels de la sécurité pourront réagir rapidement dès qu'une mise à jour d'algorithme ou de protocole sera nécessaire. **L'évolution cryptographique deviendra alors partie intégrante des opérations courantes**, plutôt qu'une succession de mises à niveau d'ampleur.

La crypto-agilité est en phase avec les **référentiels et standards actuels** dont les objectifs sont d'aider les organisations à gérer les risques liés à la cybersécurité et à renforcer les protections cryptographiques dans les secteurs critiques, qu'il s'agisse des standards techniques tels que le FIPS 140-3 ou les standards cryptographiques ISO/IEC, des référentiels sectoriels comme le PCI DSS, ou des recommandations en matière de gestion des risques telles que celles du

Cybersecurity Framework du NIST (CSF).

Elle devient également **un atout en matière de conformité** à l'heure où de nouvelles réglementations, telles que le *Cybersecurity Resilience Act* (CRA), la directive NIS2 *(Network and Information Security Directive 2)* et le *Digital Operational Resilience Act* (DORA) en Europe, ou encore les règles de déclaration en matière de cybersécurité définies par la SEC aux États-Unis, exigent des mesures renforcées. Il s'agit d'une part de **garantir la cybersécurité des produits et logiciels dès la conception** et d'autre part de **gérer l'évolution des risques de cybersécurité**, en termes de prévention, de reporting transparent et de réponse aux incidents.

## Préparez votre stack technologique pour le compte à rebours quantique

Avec l'approche du Q-day et la complexité croissante des cybermenaces, il devient crucial de faire les bons choix pour préparer infrastructures, systèmes et appareils aux défis de demain. Dans la boîte à outils de la cybersécurité, **ces trois avancées technologiques** offrent aux organisations les moyens de répondre avec confiance aux exigences réglementaires en constante évolution, tout en garantissant la protection de leurs données et de leurs actifs bien au-delà des standards actuels.

- **Un HSM souverain et sécurisé dès la conception**, pensé pour une mise en œuvre simple, une évolutivité optimale et une meilleure maîtrise des coûts
- **Une librairie cryptographique prête pour l'ère quantique**, couplée à l'expertise nécessaire pour garantir une implémentation optimisée, la conformité aux standards et des mises à jour régulières
- **Des capacités de crypto-agilité**, des terminaux aux cœurs des systèmes et jusqu'au Cloud

Envie d'explorer plus en détail ces 3 avancées et d'en savoir plus sur les technologies cryptographiques de pointe qui peuvent vous accompagner dans votre transition post-quantique et au-delà ?

Contactez-nous

---

[1] Avec une consommation électrique typique de 50 W par appareil, IDEMIA Sphere HSM consomme jusqu'à 50% d'énergie en moins qu'un HSM traditionnel.

[2] Le secteur bancaire a dû faire face à plusieurs évolutions cryptographiques au cours des dernières décennies : la norme DES, utilisée depuis les années 1970, a été remplacée dans les années 1990 par 3DES, suivie de la norme AES au début des années 2000, dont le déploiement est encore en cours. Dans le même temps, la longueur des clés RSA a été augmentée, et les fonctions de hachage associées ont été mises à jour à plusieurs reprises depuis les années 2000.
Source: https://www.fsisac.com/pqc-crypto-agility

---