RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

État de l'offre des solutions de cryptographie post-quantique en France en 2023

SOMMAIRE

SOMMAIRE

1. ENJEUX DE LA TRANSITION POST QUANTIQUE D'UN SYTEME D'INFORMATION — 4

2. SYNTHESE DE L'ENQUÊTE — 5-6

3. PRINCIPAUX FREINS IDENTIFIÉS PAR LES ÉDITEURS INTERROGÉS DANS LE CADRE DE CETTE ENQUÊTE — 7-9

→ **Principaux freins techniques** — 7-8

→ **Principaux freins organisationnels** — 9

Étude de l'ANSSI sur la transition post-quantique

Dans le cadre d'une étude visant à identifier des mesures qui pourront faciliter la transition des organisations vers la cryptographie post-quantique (PQC [1]), l'ANSSI a mené une enquête entre mai et juillet 2023 auprès d'une sélection d'entreprises qui conçoivent des briques cryptographiques pour des solutions numériques.

Après un exposé des enjeux de la transition vers la cryptographie post-quantique, le document présente la synthèse de l'analyse des réponses et les freins majeurs à la transition tels qu'indiqués par les répondants.

Cette enquête s'inscrit dans un travail de long terme de l'ANSSI pour accompagner les acteurs publics et économiques à se préparer à l'arrivée de la menace quantique et notamment faciliter l'émergence de solutions technologies innovantes pour se prémunir contre cette menace.

[1] L'acronyme PQC pour Post-Quantum Cryptography est le plus largement adopté dans la communauté scientifique, y compris francophone.

1. Enjeux de la transition post-quantique d'un système d'information

La transition post-quantique concerne en premier lieu la **cryptographie asymétrique[2],** notamment pour les usages en confidentialité et échanges de clé pour se prémunir contre des attaques rétroactives.

Les primitives cryptographiques actuellement déployées (« pré-quantiques ») sont bien maîtrisées par les développeurs en cybersécurité et il en existe de nombreuses implémentations efficaces et robustes, sous forme de bibliothèques commerciales ou libres.

La situation des futurs standards post-quantiques est différente. En effet, seuls quelques spécialistes du domaine maîtrisent complètement ces primitives. Des implémentations efficaces et durcies – qu'elles soient logicielles ou sur plateforme matérielle – vont demander beaucoup de temps et d'efforts. De même, les mécanismes et protocoles qui mettent en œuvre ces nouvelles primitives sont récents et ne jouissent pas du même niveau d'assurance et de confiance dans leur niveau de sécurité.

Ce constat global s'applique autant aux algorithmes d'établissement de clé qu'aux signatures numériques.

[2] Se référer à l'avis scientifique de l'ANSSI sur la migration vers la cryptographie post-quantique publié en décembre 2023 : https://cyber.gouv.fr/publications/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique-0.

2. Synthèse de l'enquête

Sur la petite cinquantaine d'éditeurs français initialement identifiés par l'ANSSI comme ayant une offre de solutions intégrant de manière significative de la cryptographie, 18 ont été retenus comme particulièrement pertinents pour répondre au questionnaire.

Pour cette première phase, l'objectif était de s'adresser uniquement aux éditeurs français les plus experts en matière de cryptographie, susceptibles d'apporter un éclairage à cet état des lieux. Le taux de réponse est proche de 100%.

L'enquête fait ressortir différents niveaux de maturité. Ces 18 éditeurs experts peuvent être eux-mêmes subdivisés en plusieurs groupes, du plus au moins expert :

- Les plus avancés sont **les spécialistes** : ceux qui développent des bibliothèques ad hoc qu'ils commercialisent avec, parfois, un accompagnement prenant la forme d'une offre de conseil ; ainsi que ceux qui développent des bibliothèques pour leurs propres solutions. Ces acteurs attendent des positions plus fermes de l'ANSSI : choix de protocoles plus détaillés, accès à une norme, recommandations, réglementation. Parmi eux, un petit nombre d'éditeurs se détachent, qui peuvent être considérés comme moteurs, voire même incontournables pour la transition post-quantique. Ces éditeurs ont une idée très claire des points bloquants[3] et développent des bibliothèques cryptographiques dont dépendent les non-spécialistes pour migrer leurs propres produits.

[3] Se référer à la section « Principaux freins identifiés par les éditeurs interrogés dans le cadre de cette enquête» ci-après.

- Viennent ensuite les **non-spécialistes** qui se disent prêts mais qui ne maîtrisent pas (encore) véritablement les primitives post-quantiques. Ils sont conscients de la problématique et se tiennent informés des évolutions techniques ainsi que des avis de l'ANSSI. Ils pensent, à plus long terme, développer du code – ou intégrer du code provenant des spécialistes ou des solutions open source – dans leurs produits. Certains mènent d'ores et déjà des expérimentations ou participent à des projets de recherche et développement[4] avec les spécialistes. Ils attendent que les standards et recommandations soient plus stables. Avec les mêmes préoccupations que les spécialistes, ces acteurs sont encore davantage en attente de conseils et d'orientation venant de l'ANSSI.

  L'ensemble de ces acteurs (spécialistes et non spécialistes) suit de très près « l'actualité post-quantique ». Ils sont tous sensibilisés à la problématique de la transition post-quantique et connaissent les recommandations techniques de l'ANSSI. Malgré des niveaux de maturité différents, ils constatent les mêmes freins à la transition et formulent globalement les mêmes attentes auprès de l'ANSSI pour lever certains de ces freins. Cependant, les réponses démontrent une dépendance des éditeurs « non-spécialistes » à ceux en capacité de fournir des bibliothèques cryptographiques post-quantiques.

- Viennent enfin ceux qui n'ont pas réellement pris la mesure du sujet et qui n'ont pas encore engagé de plan d'actions visant à traiter la menace quantique. A ce stade, il est préoccupant que cette menace et l'impact de la transition post-quantique (sur les produits, systèmes, performances, etc.) puissent encore être minimisés. Cette dernière catégorie ne concerne qu'un seul répondant dans l'échantillon consulté par l'ANSSI, mais d'autres entretiens menés précédemment par l'agence laissent à penser que cette position est représentative de la quasi-totalité des éditeurs et fabricants de produits numériques en France.

[4] Pour illustration : les projets HYPERFORM et RESQUE regroupent des chercheurs académiques, des industriels, parfois des centres d'évaluation (CESTI), ainsi que l'ANSSI. Certains éditeurs de solutions de cybersécurité, bien représentatifs des « non-spécialistes », dépendent des résultats de ce type de projets pour véritablement entamer la transition post-quantique de leurs produits.

3. Principaux freins identifiés par les éditeurs interrogés dans le cadre de cette enquête :

Les répondants ont partagé librement les difficultés qu'ils rencontrent dans la mise en œuvre du post-quantique dans leurs solutions. Ces constats sont listés ci-dessous, par ordre croissant de fréquence d'occurrence.

→ Principaux freins techniques identifiés

A. Le manque de normes ou de standards décrivant précisément les algorithmes.
Certains brouillons de standards ont été publiés en août 2023 par le NIST[5] puis validés à l'été 2024 , mais la standardisation d'autres algorithmes (par exemple FrodoKEM, un des algorithmes recommandés par l'ANSSI et par certaines agences homologues européennes comme solution conservatrice) est plus lente.

B. Le manque de normes ou de standards décrivant la façon de mettre en œuvre l'hybridation.
Contrairement à leurs homologues américains, les agences européennes de cybersécurité recommandent fortement le recours à l'hybridation. La prise en compte de l'hybridation dans les protocoles de tunnel (tels qu'IPSec ou TLS) ainsi que dans les certificats (tels que x.509) n'est pas mature.

C. Le manque de briques logicielles (libres ou non) de référence ou d'un guide de bonnes pratiques pour les implémenter.
Avec le manque de recul sur les implémentations qu'ils pourraient être contraints d'intégrer dans leurs produits, certains éditeurs craignent d'en abaisser le niveau de sécurité ou d'y introduire de nouvelles vulnérabilités.

D. Le besoin de faire évoluer certains référentiels pour y intégrer la PQC.
Les produits devant assurer la sécurité de données très sensibles (marqués Diffusion Restreinte par exemple) doivent nécessairement être conformes à certains référentiels, de par la réglementation en vigueur. Ces produits nécessitent des cycles de développement particulièrement longs; les éditeurs concernés ressentent donc l'urgence d'une mise à jour de ce type de référentiels.

[5] Three Draft FIPS for Post-Quantum Cryptography | CSRC (nist.gov) : https://csrc.nist.gov/news/2023/three-draft-fips-for-post-quantum-cryptography
[6] Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography : https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved
[7] L'hybridation consiste à combiner des algorithmes asymétriques post-quantiques avec une cryptographie asymétrique pré-quantique bien connue et bien étudiée, fondée sur la factorisation ou le logarithme discret.
[8] Concernant IPSec, Strongswan (https://docs.strongswan.org/docs/6.0/news/whatsNew.html) intègre depuis peu de la PQC en mode hybride, mais concernant TLS il n'y a toujours pas de version officielle.
[9] Malgré de premiers travaux réalisés à l'IETF, par exemple la RFC 9370 et draft-ietf-tls-hybrid-design-10.

E. Le manque de maturité des implémentations sur du matériel.
Seuls quelques développeurs sont en mesure d'offrir des briques de code pour des solutions matérielles. Les standards et les clients ne sont pas encore prêts pour qu'ils puissent proposer une offre plus complète.

F. Des inquiétudes concernant les pertes de performance des signatures post-quantiques.
En utilisant les temps de référence indiqués dans les soumissions faites au NIST, les développeurs n'ont pas d'inquiétude quant aux performances des protocoles d'échange de clés. En revanche, pour les signatures, certains d'entre eux craignent des difficultés à prendre en compte plusieurs algorithmes et l'hybridation en plus, notamment pour les implémentations sur du matériel.

[10] La certification de sécurité repose en général sur un produit fini qui permet d'en connaitre son contexte d'usage et limite sa surface d'exposition, ce qui n'est pas le cas d'une bibliothèque. Pour savoir si un certificat permettrait d'apporter la confiance nécessaire dans ces composants génériques, il est nécessaire, pour l'ANSSI, de réaliser une étude préalable sur le contour et la portée d'un tel certificat et de définir une méthodologie satisfaisante pour son évaluation.

→ Principaux freins organisationnels identifiés

G. L'absence d'un plan de transition. Certains industriels réclament des contraintes plus fermes en termes de calendrier et d'obligations sur la transition post-quantique. Ils espèrent des contraintes réglementaires pour les utilisateurs ainsi que des recommandations de l'ANSSI précisant l'usage de la PQC (en lien avec la définition du risque quantique). Ces recommandations pourraient être formulées à partir d'une grille d'auto-évaluation mise à disposition des utilisateurs afin qu'ils puissent mesurer « le risque quantique » auquel sont exposés leurs systèmes d'information et faciliter l'organisation de leur transition

H. L'incertitude sur la certification des bibliothèques cryptographiques . Sans certification, les développeurs d'implémentations robustes et efficaces des primitives post-quantiques ne peuvent pas valoriser la qualité de leurs solutions. Les développeurs de solutions numériques (cyber ou non cyber) sont également pénalisés[11] .

L'absence de bibliothèques cryptographiques post-quantiques de référence entraîne un retard des actions de transition de l'ensemble des acteurs et un faux sentiment de sécurité vis-à-vis des solutions intégrant des implémentations non évaluées et comportant des vulnérabilités.

I. Le manque de sensibilisation concernant les utilisateurs. Le marché, à de rares exceptions près, n'est pas sensibilisé au risque quantique et n'a pas de projet de migration.

J. Le coût pour mettre à jour ses compétences sur le sujet (recrutement de spécialistes, formation des experts d'autres domaines à ce sujet).

Cette liste ne constitue pas nécessairement un plan d'actions que l'ANSSI mènera au profit des éditeurs. Certains constats pourront conduire l'ANSSI à prendre des mesures, tandis que d'autres seront plutôt de la responsabilité des offreurs eux-mêmes. L'état des lieux consolidé par d'autres investigations – notamment auprès des utilisateurs et des prestataires de services – et par les résultats d'analyses de risque quantique permettra de déterminer un plan d'actions.

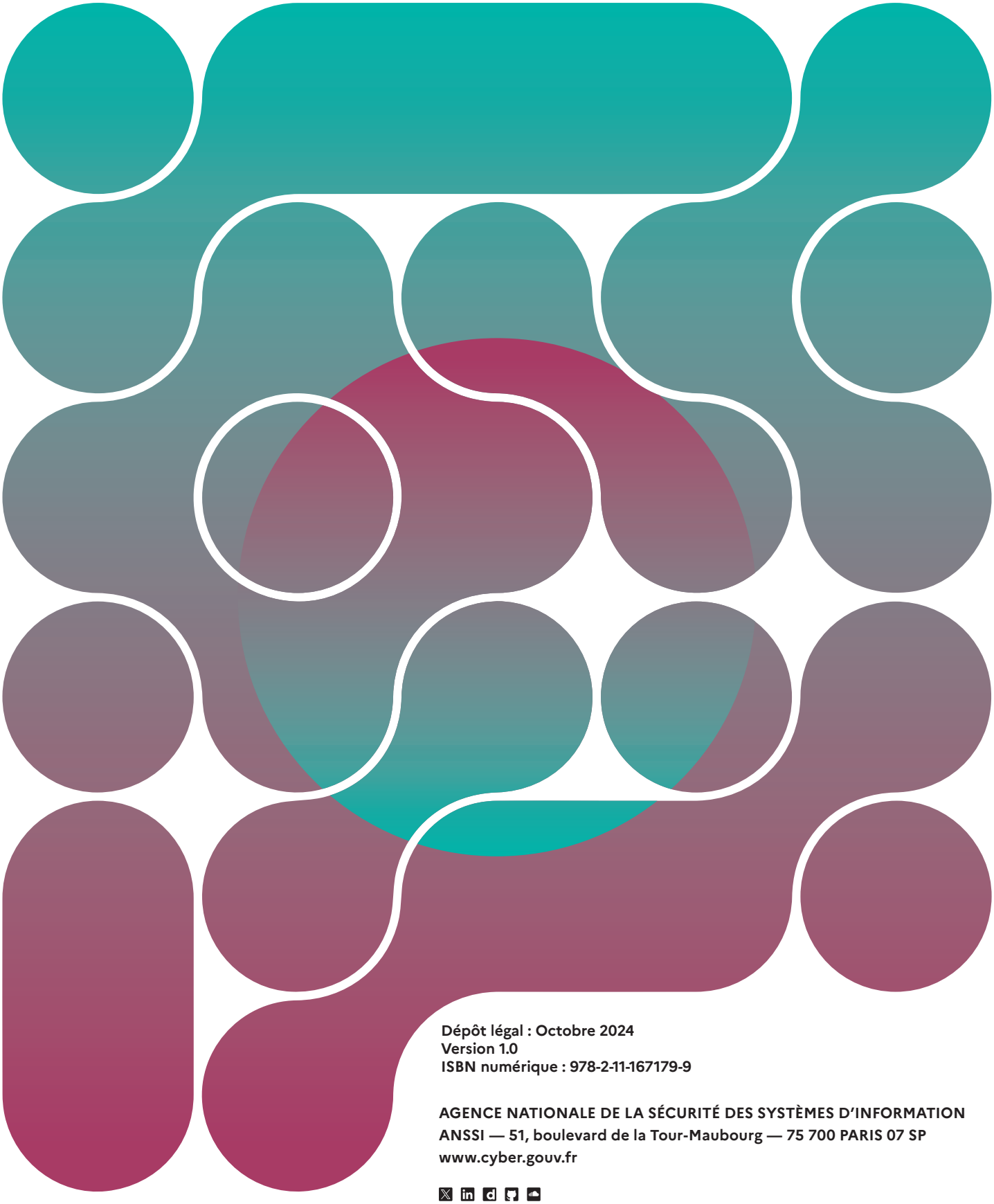
[11] La majorité des éditeurs n'auront pas les compétences pour développer eux-mêmes une implémentation robuste et performante des primitives post-quantiques et « attendront » des implémentations de référence validées ou recommandées pour migrer leurs produits.

CONCLUSION

CONCLUSION

A la lumière des résultats de cette enquête et de la criticité de la menace représentée par l'émergence future des ordinateurs quantiques, l'ANSSI souhaite rappeler **l'importance de démarrer sans tarder les actions préparatoires à la transition post-quantique**, et ce pour tout type d'organisation. Il est essentiel que chaque organisation évalue son niveau de risque réel vis-à-vis de la menace quantique et élabore un plan de transition dédié, afin d'assurer la sécurité de ses données sur le long terme. L'immaturité constatée des solutions n'est que transitoire et ne devrait pas servir de prétexte à l'inaction. Certaines actions devront être mises en œuvre sans délai et d'autres pourront être déployées progressivement, dans les années à venir.

Remerciements
L'ANSSI remercie les sociétés COSMIAN, CRYPTO EXPERTS, CRYPTONEXT SECURITY, CYFERALL, EVERTRUST, EVIDEN, LEANEAR, OLVID, OODRIVE, PRIM'X, SEALD, SECURE-IC, STORMSHIELD, THALES, THE GREEN BOW, TIXEO et WALLIX pour leur participation.



Dépôt légal : Octobre 2024
Version 1.0
ISBN numérique : 978-2-11-167179-9

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.cyber.gouv.fr