RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

État de l'offre des prestations d'accompagnement et de conseil en sécurité en France en 2023

SOMMAIRE

SOMMAIRE

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 auprès d'un échantillon de 34 prestataires de services ayant une offre d'accompagnement et de conseil en cybersécurité (essentiellement des PASSI [2] disposant d'activités de conseil et potentiellement candidats à PACS [3]) entre décembre 2023 et janvier 2024.

Après un rappel 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.
[2] PASSI : prestataire d'audit de la sécurité des systèmes d'information
[3] PACS : prestataire d'accompagnement et conseil en sécurité

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

La transition post-quantique concerne en premier lieu la **cryptographie asymétrique** [4], 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.

[4] 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 auprès des prestataires d'accompagnement et de conseil en sécurité

Cette consultation fait ressortir en premier lieu que la demande de conseil et d'accompagnement pour la problématique de la menace quantique est, à ce jour, très faible. **Le marché est quasi inexistant**, à tel point que la majorité des prestataires (70 %) n'a réalisé aucune prestation de ce type.

Pour ceux qui en ont déjà réalisé, les prestations de sensibilisation des décideurs à la menace quantique représentent près de 40% du total. Si on ne tient pas compte de ces prestations de sensibilisation, les prestataires qui ont réalisé au moins une prestation «post-quantique» n'en ont réalisé à ce jour que 4 en moyenne, pour un maximum de 14 prestations réalisées par l'un d'entre eux.

De ce fait, **l'offre commerciale est très immature** et peu de prestataires ont une offre structurée pour accompagner leurs (futurs) clients. **70% des prestataires n'ont aucune offre structurée**. Cependant, la quasi-totalité des prestataires déclarent qu'ils comptent développer une offre commerciale de conseil et d'accompagnement à la transition post-quantique (80 %). Ils pensent être à même de proposer une telle offre en **deux ans au plus**.

Par ailleurs, les prestataires déclarent avoir une connaissance théorique plutôt satisfaisante de la menace que représente la cryptanalyse quantique.

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

A. Le manque de recommandations techniques et d'actions de sensibilisation à destination de l'ensemble des acteurs économiques ou du secteur public.

B. Le manque de cadre règlementaire contraignant.
Environ 60 % des prestataires souhaiteraient que l'ANSSI instaure un cadre réglementaire qui impose à ces mêmes acteurs privés ou publics de prendre en compte la menace quantique. Sur ce point, 26% sont contre et 13% n'ont pas d'avis.

C. Une communauté de prestataires encore trop peu structurée.
Tous les prestataires qui ont un avis sur la question pensent que l'ANSSI devrait créer et animer une nouvelle communauté de prestataires sur le sujet du post-quantique (70 % se prononcent favorablement, 30 % n'ont pas d'avis).

Concernant la question d'ajouter ce qui pourrait ressembler à une « portée technique post-quantique » dans les référentiels d'exigences de l'ANSSI pour la qualification des prestataires d'accompagnement et de conseil en sécurité (PACS), les avis sont plus mitigés : entre 30% et 60% y seraient favorables, suivant la façon dont la question est posée. Autrement exprimé, les prestataires veulent bien être accompagnés dans leur montée en compétences sur le sujet du post-quantique mais ne souhaitent pas nécessairement que leurs compétences soient évaluées.

CONCLUSION

CONCLUSION

Cette enquête auprès des prestataires confirme les constats de l'enquête auprès des bénéficiaires [5] : nous observons une quasi **absence de demande** pour le moment et une quasi **absence d'offre** commerciale.

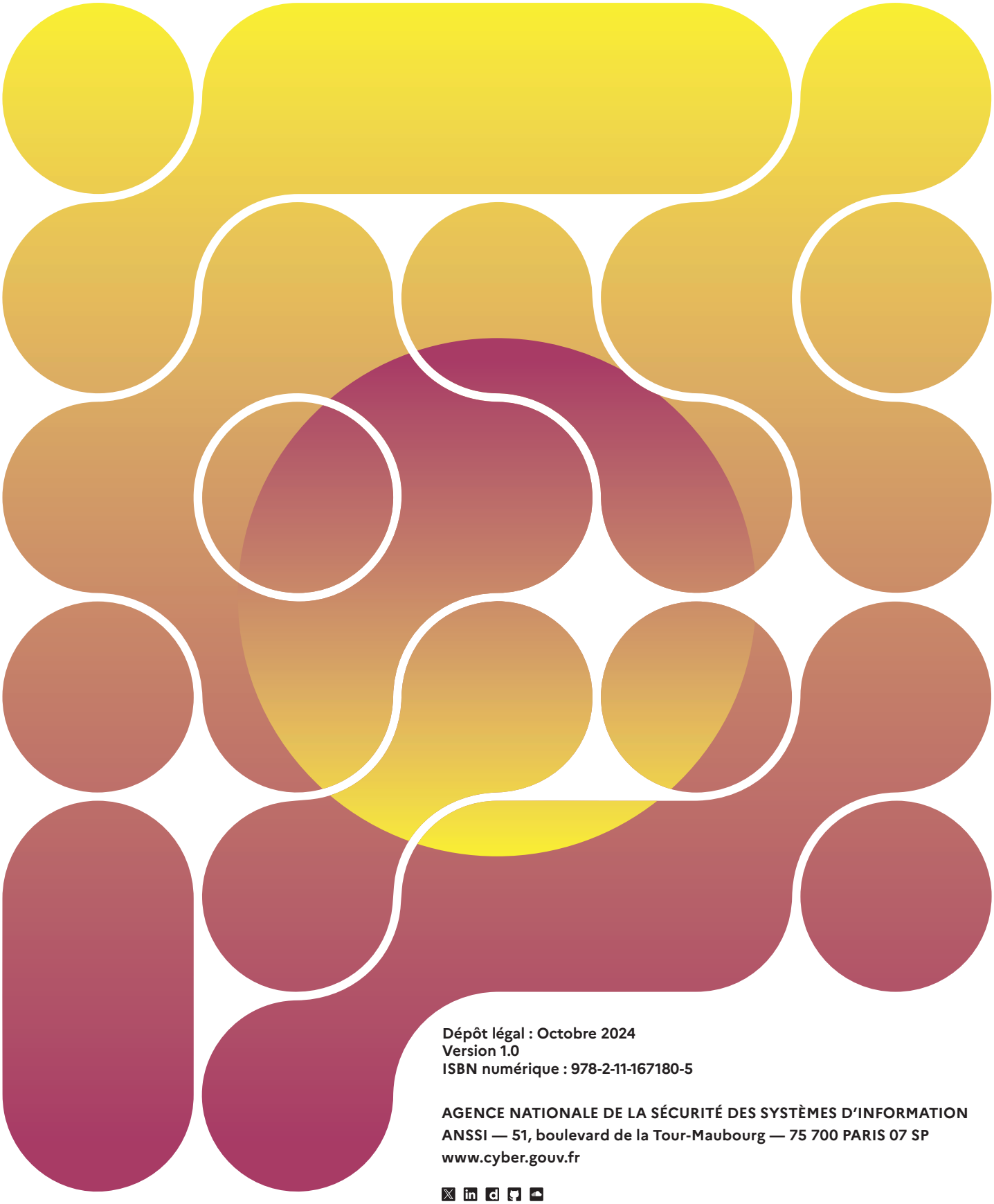
Les prestataires expliquent l'absence de demande par un sentiment, chez leurs clients, qu'il n'est pas urgent d'agir contre la menace quantique. Le fait qu'il n'y ait aucune obligation réglementaire conforte les clients dans leur posture d'attente.

Il convient de remarquer que la plupart des prestataires de services se tiennent toutefois prêts à répondre à la demande lorsque celle-ci se développera. Il est vrai que ce nouveau marché devrait représenter une **opportunité commerciale importante** pour le secteur du conseil.

Remerciements

L'ANSSI remercie les sociétés ACCENTURE, ADVENS, AIRBUS PROTECT, AKERVA, ALMOND, CAPGEMINI, CGI FRANCE, CRYPTOEXPERTS, CS GROUP, DELOITTE, EVIDEN, EY, FORMIND, INTRINSEC, KPMG, LEXFO, MAGELLAN CONSULTING, MAZARS, ON-X, OWN-SECURITY, QURISK, SERMA SAFETY & SECURITY, SQUAD, SYNACKTIV, WAVESTONE pour leur participation à cette étude.

[5] Enquête non publique à la date de publication de ce document.



Dépôt légal : Octobre 2024
Version 1.0
ISBN numérique : 978-2-11-167180-5

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