RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Enjeux et objectifs de la transition post-quantique : enjeux industriels

Olivier GUERIN – ANSSI / Division industrie & technologies – 25 juin 2024

QUELS SONT LES ENJEUX INDUSTRIELS ?

Les objectifs visés :

Côté client

- Réaliser la transition à temps (y compris attaques rétroactives)
- Réussir la transition (pas de perte de disponibilité ou d'intégrité)

Côté offre

- Disposer d'offres (produits & services) de confiance
- Conserver / acquérir une autonomie stratégique européenne
- Transformer le défi technologique en une opportunité économique

LES ÉTUDES MENÉES PAR L'ANSSI

✓ 3 études conduites entre juillet 2023 et janvier 2024.

Auprès de qui ?

- Éditeurs de cryptographie
- Bénéficiaires de l'ANSSI
- Prestataires d'accompagnement et de conseil

Questionnaire

Pour savoir quoi ?

- Connaissance du sujet
- Freins à la transition
- Besoins et attentes

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

1/3

LES ÉDITEURS DE CRYPTOGRAPHIE

LES ÉDITEURS DE CRYPTOGRAPHIE

L'ANSSI a interrogé les « **développeurs de produits de sécurité utilisant de la cryptographie** ».

- Ceux qui implémentent les algorithmes basés sur les primitives post-quantique : les « spécialistes en cryptographie »
- Ceux qui utilisent les algorithmes post-quantique pour les intégrer dans les protocoles de leurs produits

Consultés hors étude : les éditeurs de solutions de cybersécurité.

Non interrogés : tous les autres dont les éditeurs de produits numériques connectés.

LES ÉDITEURS DE CRYPTOGRAPHIE

Connaissance du sujet et maturité

…à l'exception des éditeurs de produits de cybersécurité.

Freins à la transition

- Manque de normes (algorithmes & hybridation)
- Manque de normalisation de certains protocoles
- Pas ou peu de demande client
- Flou sur les performances et sur l'impact sur les systèmes

Besoins et attentes

- Implémentations d'algorithmes post-quantiques de référence
- Plan de transition (et calendrier associé)
- Sensibilisation de l'écosystème (décideurs, clients)

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

2/3

LES BÉNÉFICIAIRES DE L'ANSSI

LES BÉNÉFICIAIRES DE L'ANSSI

Une quarantaine de **bénéficiaires de l'ANSSI** ont répondu à l'enquête.

- Institutions publiques
- Opérateurs régulés (public et privé) des secteurs d'activité suivants :
  - Enseignement supérieur & recherche
  - Défense
  - Industrie
  - Santé
  - Finance
  - Espace
  - Télécom

LES BÉNÉFICIAIRES DE L'ANSSI

Connaissance du sujet et maturité

- **> 50% des bénéficiaires à risque vs attaques rétroactives**
- Aucun plan de transition
- Fort besoin d'accompagnement et de conseil à la transition

Freins à la transition

- Mauvaise compréhension des enjeux
- Manque de moyens (financiers & humains)
- Absence d'offre de conseil à la transition
- Absence d'obligation réglementaire

Besoins et attentes

- Communication sur la menace quantique
- Visibilité sur l'agenda
- Analyse de risque quantique
- Sensibilisation des décideurs à la menace quantique

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

3/3

LES PRESTATAIRES D'ACCOMPAGNEMENT ET DE CONSEIL EN SÉCURITÉ

LES PRESTATAIRES D'ACCOMPAGNEMENT

Ceux qui **accompagneront les organisations** dans leur transition post-quantique.

- Prestataires d'accompagnement et de conseil en sécurité (« PACS ») en cours de qualification par l'ANSSI
- Prestataires d'audit de sécurité (« PASSI »)
- Les centres d'évaluation des produits/services cyber (« CESTI »)

LES PRESTATAIRES D'ACCOMPAGNEMENT

Connaissance du sujet et maturité

- Offre commerciale d'accompagnement et conseil très immature (70% n'ont aucune offre)
- Connaissance de la menace et des enjeux
- Prêts à mettre en place une offre de service en moins de 2 ans

Freins à la transition

- Pas de demande client, aucune mission réalisée
- Pas d'intérêt ni d'urgence perçus chez les clients
- Absence d'obligation réglementaire

Besoins et attentes

- Publication de recommandations techniques
- Actions de sensibilisation
- Cadre réglementaire contraignant
- Animation de la communauté

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

CONCLUSION

La route est encore longue !

Chacun a son rôle à jouer

- L’État / UE
- L’offre privée
- Les utilisateurs