La migration cryptographique post-quantique et la crypto-agilité

Où est la cryptographie ?

Crypto utile pour

Authentifi-
cation

Crypto-
monnaie

Échange de
clés secrètes

Intégrité des
messages

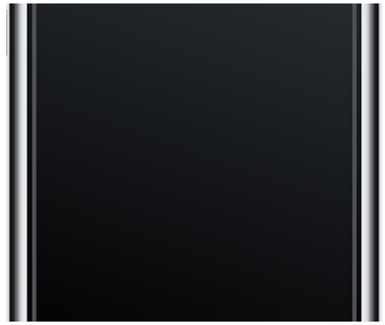
Sécuriser les
comms

Sécuriser le
stockage

Signature
électronique

À la maison, c’est présent dans

Achats en ligne



Cellulaires

Lecteurs DVD / BlueRay

Messagerie

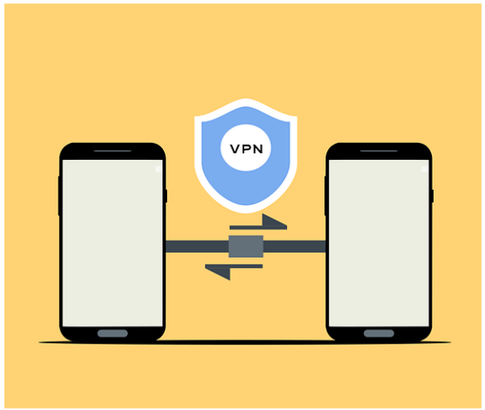
Navigation Web

Sécurité

WiFi

Au travail, c’est présent dans

Cartes à puce



RPV / VPN

Mots de passe

Transactions

Qu’est-ce que la cryptographie ?

Historique

- Principe de Kerckhoffs (1883)
  - Cryptosystème sécurisé même si l'attaquant connaît tous les détails de conception du système, à l'exception de la clé secrète.
  - Tous les détails : algorithmes de chiffrement et déchiffrement
- Clé secrète ne doit pas être compromise
  - Compromission : calculée – devinée – volée

Menace cryptographique

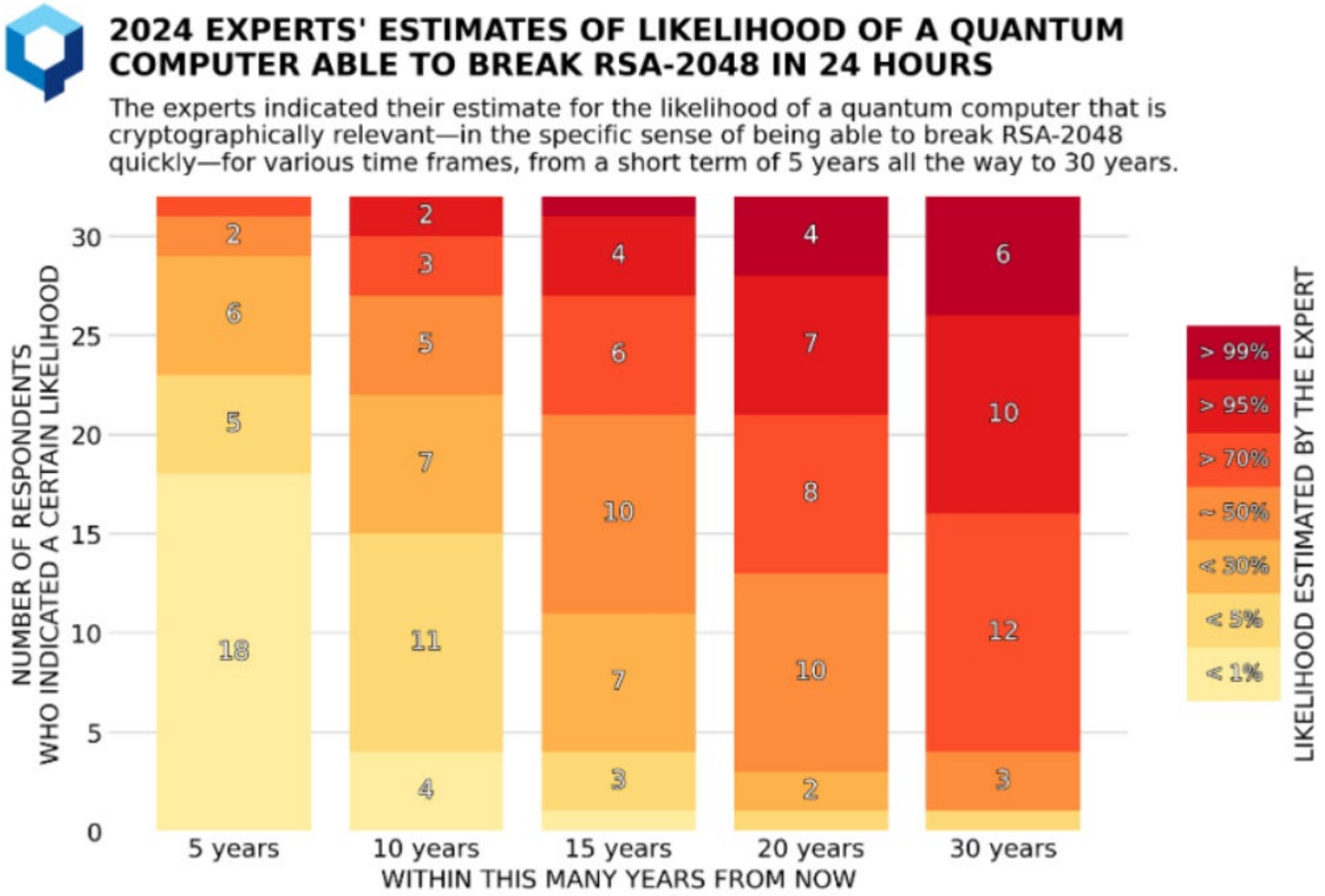
La vitesse de l’innovation

- L’innovation disruptive
  - Évolue rapidement, car l’innovation s’auto-alimente
  - Bouleverse les façons de faire actuelles
  - Résistance des acteurs en place
  - Cause un changement radical (disruptif)

Menace : deux algorithmes quantiques

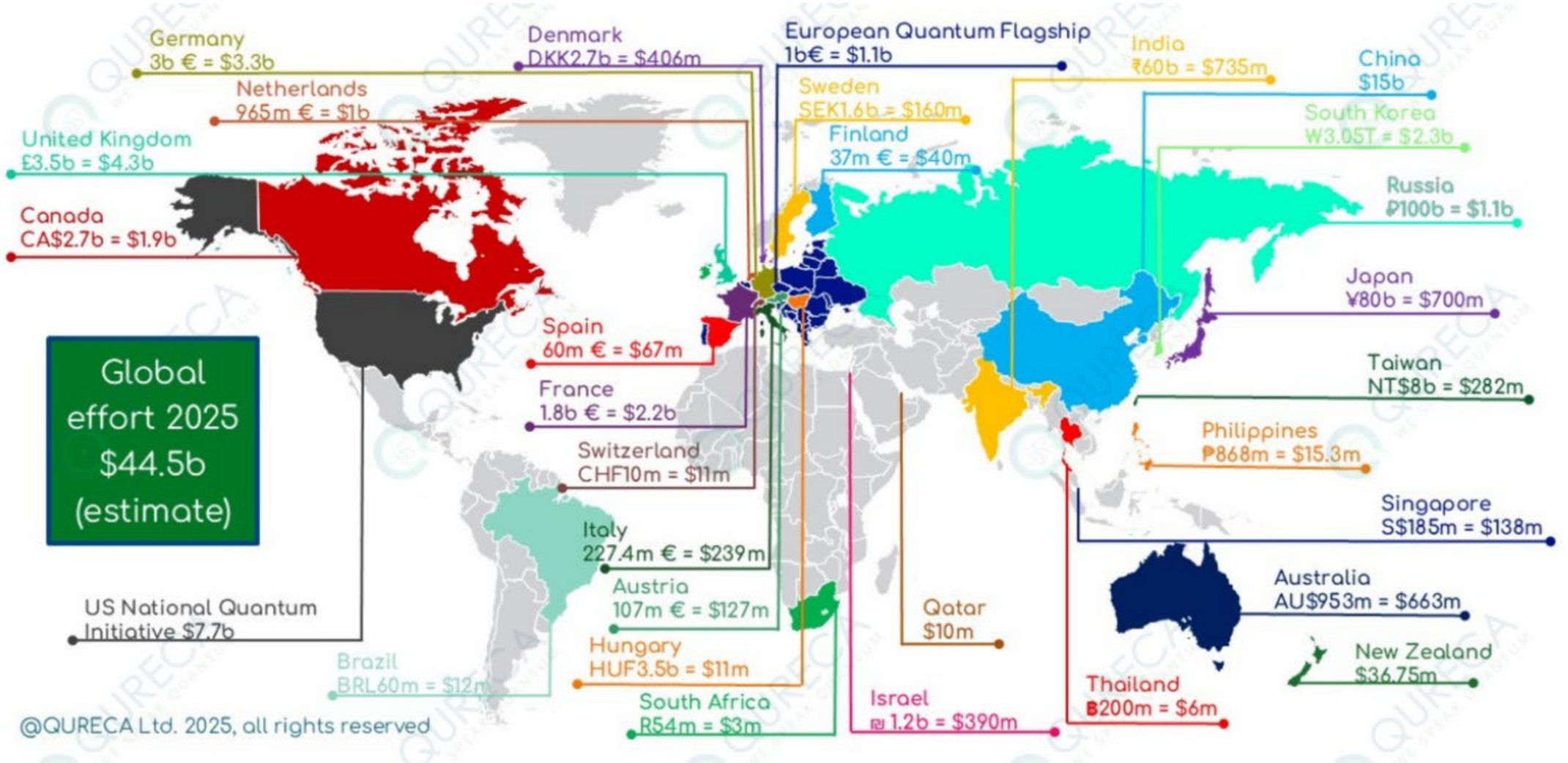
- 1994 : Algorithme de Shor
  - factoriser en temps polynomial un nombre ou de calculer un logarithme discret
  - casse la crypto asymétrique comme RSA et Diffie-Hellman
  - ex : RSA-2048 « cassable » en quelques heures (ou jours), au lieu de 2112 opérations ~ 1016 années
- 1996 : Algorithme de Grover
  - Permet d'inverser une fonction de hachage
  - Temps de calcul $\sqrt{n}$

Et c’est pour bientôt ?



SOURCE : https://globalriskinstitute.org/mp-files/quantum-threat-timeline-report-2024.pdf/

La course aux technologies quantiques



Crypto-apocalypse ?

- Pire cas
  - Sans aucune préparation de notre part
  - Effondrement des approches actuelles
- N’arrivera pas, car
  - Nos gouvernements se préparent déjà
  - Les problèmes technologiques sont encore complexes

La cryptographie symétrique

- Algorithmes résistants au quantique
- On double la taille des clés
- AES-128 → AES-256

La cryptographie asymétrique

- Les algorithmes actuels sont vulnérables et non réparables
- Factorisation de grands nombres (RSA)
- Logarithmes discrets (Diffie–Hellman, El Gamal)
- Courbes elliptiques (ECC)

La signature électronique

- La plupart des algorithmes reposent sur l'asymétrique…
- Les certificats (petit cadenas du navigateur) sont attestés par signature électronique…

Le hachage

- Algorithmes résistants au quantique
- On augmente de 50 % la longueur des condensats pour maintenir le même niveau de sécurité
- Ex. SHA-256 → SHA-384 et SHA-512

Allons vers les solutions

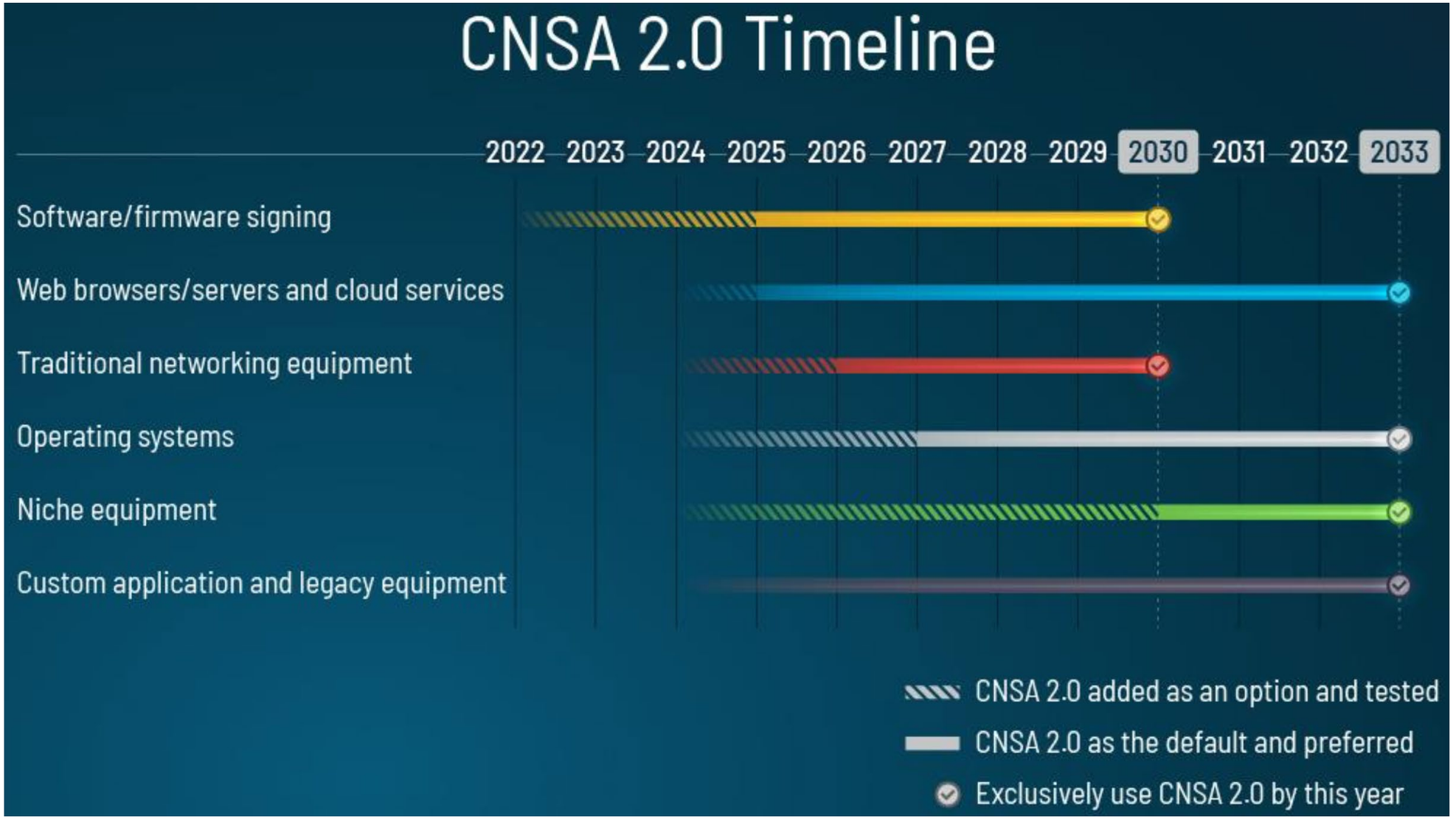
National Institute of Standards and Technology (NIST)

- Normalisation pour le gouvernement fédéral américain
- Standardise, entre autres, l'utilisation de la cryptographie
  - Federal Information Processing Standards (FIPS)
  - AES (symétrique) : FIPS PUB 197
  - DSA (signature électronique) : FIPS PUB 186-4
  - SHA (hachage sécuritaire) : FIPS PUB 180-4
  - Longueur des clés : Special Publication 800-57 Part 1 Rev. 5

NIST : crypto post-quantique

- 13 août 2024
- 3 standards publiés
  - FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard
  - FIPS 204 Module-Lattice-Based Digital Signature Standard
  - FIPS 205 Stateless Hash-Based Digital Signature Standard

Feuille de route CNSA



CNSA : Commercial National Security Algorithm Suite 2.0

Le train est en marche

- Initiative de UWaterloo : Open Quantum Safe
- IETF : Révision des protocoles Internet
- Grands fournisseurs
  - Participent à la standardisation et à la recherche
  - Ex. (non exhaustif) : AWS, Cloudfare, Entrust, Google, IBM, Intel, Microsoft, Thales, Apple

Les étapes

1. Se préparer
2. Identifier les systèmes cryptographiques
3. Analyser les risques
4. Prioriser les systèmes selon leur criticité
5. Planifier la migration
6. Obtenir les ressources nécessaires
7. Effectuer les migrations
8. Valider
9. Améliorer la feuille de route

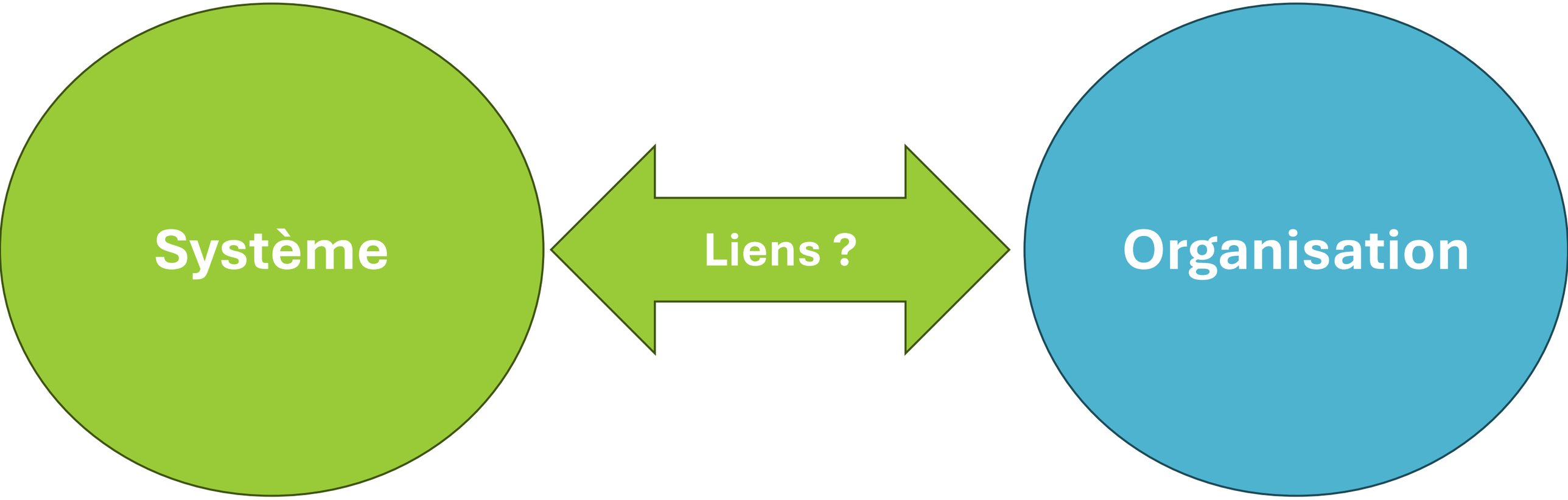
Les risques

- Sous-estimer les efforts et les coûts de remplacement
- Attendre trop longtemps (HNDL)
- Oublier un système
- Incertitude sur la robustesse des algorithmes PQC
- Complexité d’intégration
- Systèmes rigides
- Expertise insuffisante

Crypto-agilité

- Capacité à atteindre état final cryptographique souhaité en changeant UNIQUEMENT les algorithmes cryptographiques utilisés dans un système
- Deux niveaux
  - Systémique : comment concevoir le matériel, le logiciel, les protocoles et leur assemblage afin de la favoriser
  - Organisationnelle : quels sont les processus clés qui permettent de la favoriser

Crypto-agilité



Principes ?

Crypto-agilité

- Problématique
  - Quels sont les principes crypto-agiles clés qui permettent de concevoir le matériel, les logiciels et les protocoles tout en garantissant que les processus organisationnels puissent efficacement orchestrer ces changements au sein d'infrastructures complexes ?