RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LA TRANSITION VERS LA CRYPTOGRAPHIE POST-QUANTIQUE (PQC)

SAMIH SOUISSI

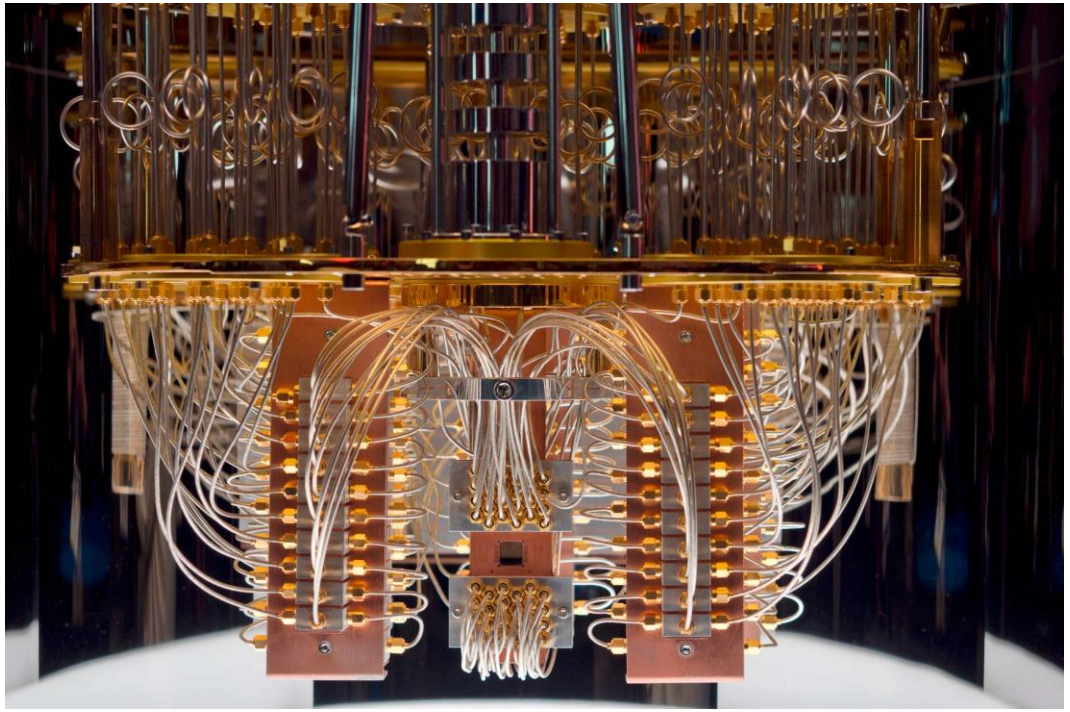
FORUM DES COMPÉTENCES – 11 DÉCEMBRE 2025

La PQC : Pourquoi c’est important ?

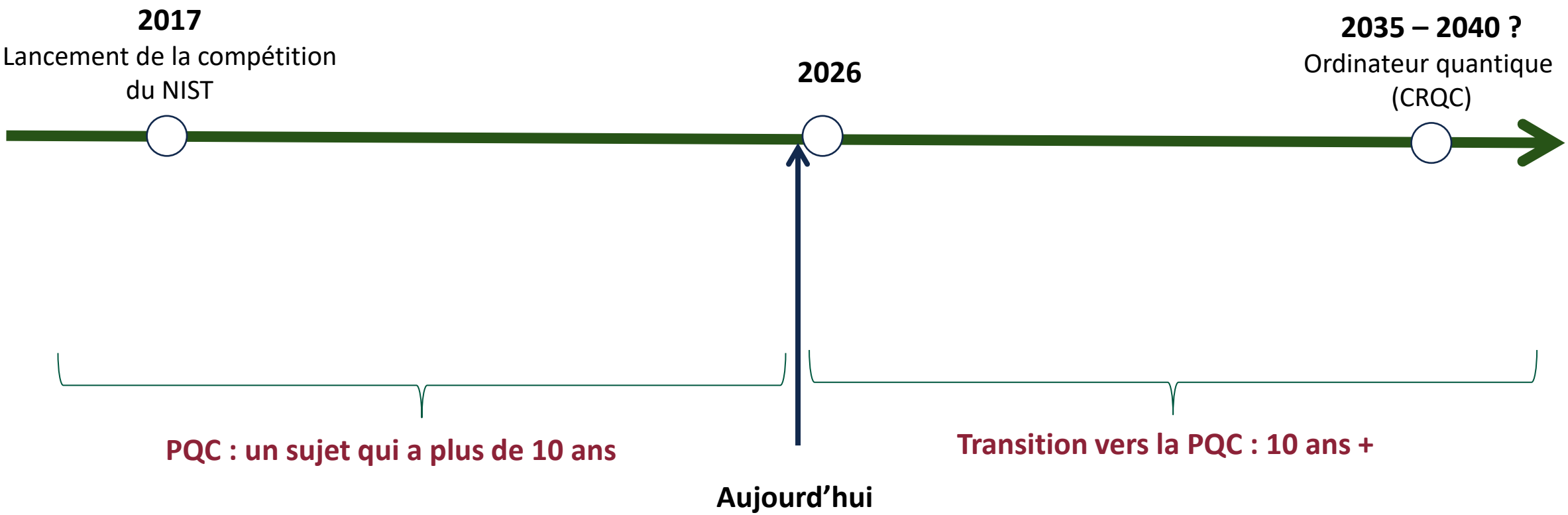
- La possibilité de l’émergence future d’un ordinateur quantique suffisamment puissant pour **compromettre la sécurité d’une grande partie de la cryptographie à clé publique** utilisée aujourd’hui.

- La menace quantique doit être prise en compte dès aujourd’hui.

- **Cryptographie post-quantique (PQC) :** la voie la plus prometteuse pour répondre à la menace quantique.



La PQC, un enjeux pour la prochaine décennie



Actions passées (2017-2025)

Actions passées (2017-2025)

Lancement de la compétition du NIST

Doctrine technique:
Recommandations technique de l'ANSSI :
Algorithmes PQC/hybridation

Normalisation de 3 algorithmes PQC par le NIST

Actions passées (2017-2025)

Lancement de la compétition du NIST

Doctrine technique:
Recommandations technique de l'ANSSI : Algorithmes PQC/hybridation

Normalisation de 3 algorithmes PQC par le NIST

Connaissance de l'écosystème :
3 études de marché ANSSI (offreurs, utilisateurs et prestataires de conseil)

Actions passées (2017-2025)

Lancement de la compétition du NIST

Doctrine technique:
Recommandations technique de l'ANSSI :
Algorithmes PQC/hybridation

Normalisation de 3 algorithmes PQC par le NIST

Connaissance de l'écosystème :
3 études de marché ANSSI (offreurs, utilisateurs et prestataires de conseil)

Certification :
Création d'une portée PQC à l'agrément des CESTI
Lancement des évaluation pilotes
Premier CESTI agréé et premiers visas de sécurité
Mise à jour des recommandations pour la certification européenne

Actions passées (2017-2025)

Lancement de la compétition du NIST

Doctrine technique:
Recommandations technique de l'ANSSI :
Algorithmes PQC/hybridation

Normalisation de 3 algorithmes PQC par le NIST

Connaissance de l'écosystème :
3 études de marché ANSSI (offreurs, utilisateurs et prestataires de conseil)

Certification :
Création d'une portée PQC à l'agrément des CESTI
Lancement des évaluation pilotes
Premier CESTI agréé et premiers visas de sécurité
Mise à jour des recommandations pour la certification européenne

Formation :
Initiation technique à la PQC au CFSSI

Actions passées (2017-2025)

Lancement de la compétition du NIST

Doctrine technique:
Recommandations technique de l'ANSSI : Algorithmes PQC/hybridation

Normalisation de 3 algorithmes PQC par le NIST

Connaissance de l'écosystème :
3 études de marché ANSSI (offreurs, utilisateurs et prestataires de conseil)

Certification :
Création d'une portée PQC à l'agrément des CESTI
Lancement des évaluation pilotes
Premier CESTI agréé et premiers visas de sécurité
Mise à jour des recommandations pour la certification européenne

Formation :
Initiation technique à la PQC au CFSSI

Coordination UE :
Feuille de route européenne PQC

Actions passées (2017-2025)

Lancement de la compétition du NIST

Doctrine technique:
Recommandations technique de l'ANSSI : Algorithmes PQC/hybridation

Normalisation de 3 algorithmes PQC par le NIST

Connaissance de l'écosystème :
3 études de marché ANSSI (offreurs, utilisateurs et prestataires de conseil)

Stratégie PQC :
Publication des orientations de l'ANSSI sur la PQC

Certification :
Création d'une portée PQC à l'agrément des CESTI
Lancement des évaluation pilotes
Premier CESTI agréé et premiers visas de sécurité
Mise à jour des recommandations pour la certification européenne

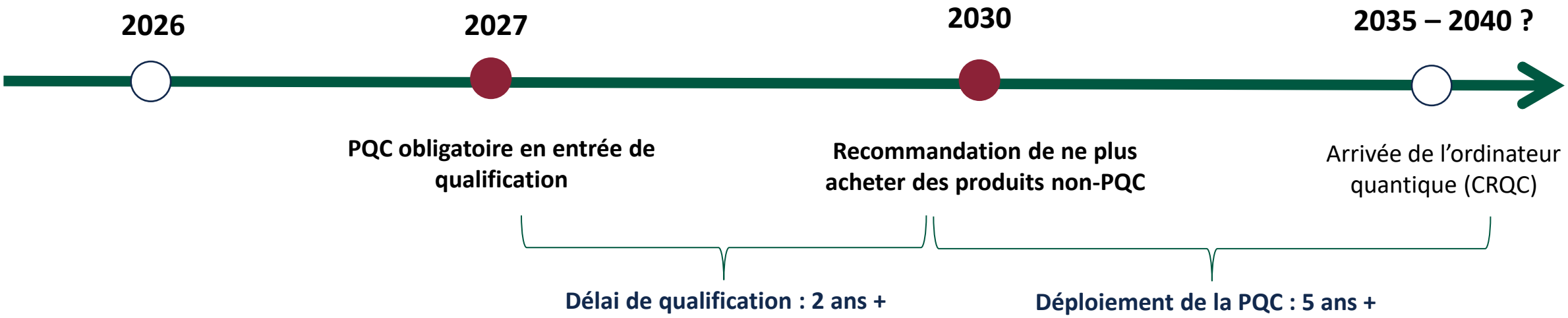
Formation :
Initiation technique à la PQC au CFSSI

Coordination UE :
Feuille de route européenne PQC

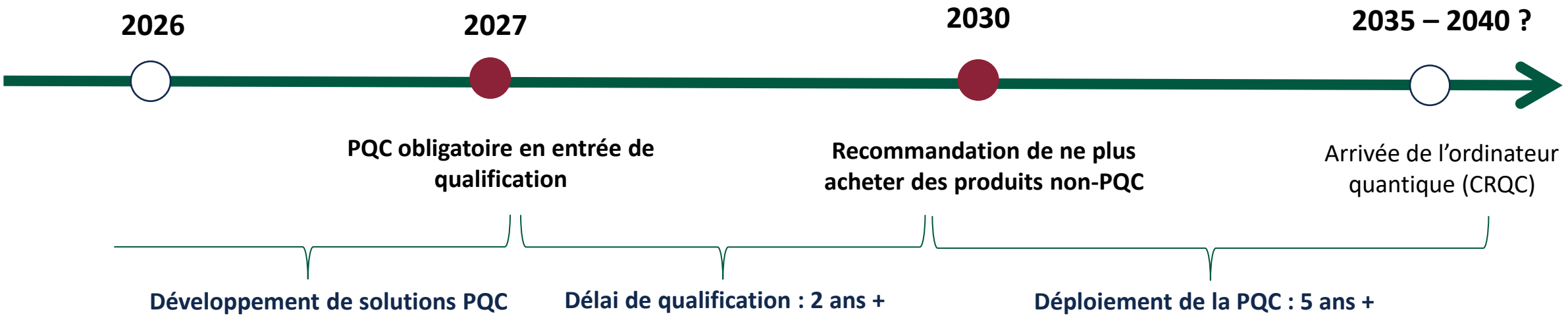
Actions futures (2026+)

Actions futures (2026+)

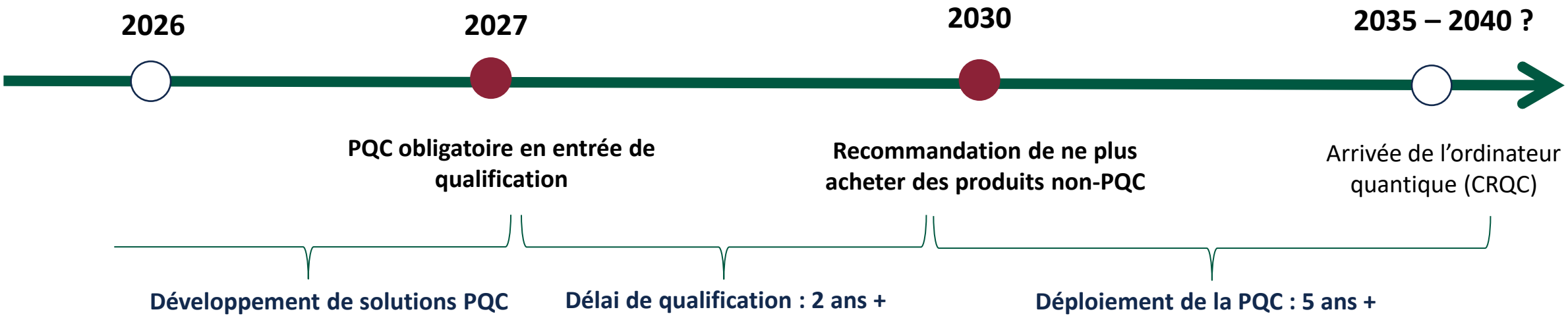
Actions futures (2026+)



Actions futures (2026+)



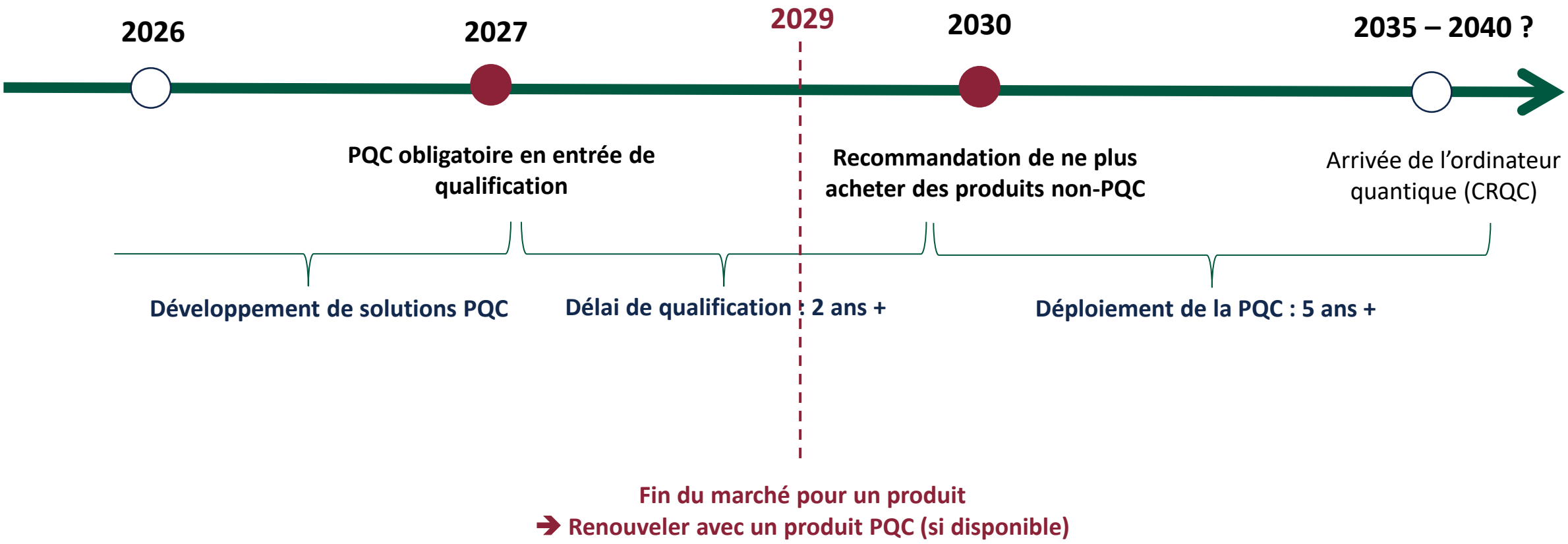
Actions futures (2026+)



Prérequis pour la transition

1. **Connaissance du SI et des délais de renouvellement des équipements**
2. **Migration planifiée dans le cycle de renouvellement du SI**

Actions futures (2026+) - Exemple



Que faire dès aujourd'hui ?

ANSSI

- Finaliser la doctrine technique
- Faire évoluer les référentiels et guides existants
- Poursuivre l'accompagnement des CESTI
- Lancer des projets pilotes de définition de plan de transition vers la PQC
- Poursuivre la coordination UE

Que faire dès aujourd'hui ?

ANSSI

- Finaliser la doctrine technique
- Faire évoluer les référentiels et guides existants
- Poursuivre l'accompagnement des CESTI
- Lancer des projets pilotes de définition de plan de transition vers la PQC
- Poursuivre la coordination UE

Offreurs de solutions

- Initier les développent PQC (si ce n'est pas encore fait)
- Définir et communiquer les roadmaps produits
- **Se préparer pour l'entrée en qualification des produits PQC en 2027**, a minima pour :
  - les produits permettant de répondre aux attaques rétroactives
  - les produits qui sont déployés dans des environnements complexes
  - des usages impliquant des longs cycles de vie

Que faire dès aujourd'hui ?

ANSSI

- Finaliser la doctrine technique
- Faire évoluer les référentiels et guides existants
- Poursuivre l'accompagnement des CESTI
- Lancer des projets pilotes de définition de plan de transition vers la PQC
- Poursuivre la coordination UE

CESTI

- Monter en compétence dans :
  - L'évaluation des mécanismes hybrides
  - L'évaluation des algorithmes PQC connus
  - L'évaluation des attaques par canaux secondaires auxiliaires sur certains algorithmes PQC
- **Être capable d'évaluer des produits PQC d'ici 2027**

Offreurs de solutions

- Initier les développent PQC (si ce n'est pas encore fait)
- Définir et communiquer les roadmaps produits
- **Se préparer pour l'entrée en qualification des produits PQC en 2027**, a minima pour :
  - les produits permettant de répondre aux attaques rétroactives
  - les produits qui sont déployés dans des environnements complexes
  - des usages impliquant des longs cycles de vie

Que faire dès aujourd'hui ?

ANSSI

- Finaliser la doctrine technique
- Faire évoluer les référentiels et guides existants
- Poursuivre l'accompagnement des CESTI
- Lancer des projets pilotes de définition de plan de transition vers la PQC
- Poursuivre la coordination UE

CESTI

- Monter en compétence dans :
  - L'évaluation des mécanismes hybrides
  - L'évaluation des algorithmes PQC connus
  - L'évaluation des attaques par canaux secondaires auxiliaires sur certains algorithmes PQC
- **Être capable d'évaluer des produits PQC d'ici 2027**

Offreurs de solutions

- Initier les développent PQC (si ce n'est pas encore fait)
- Définir et communiquer les roadmaps produits
- **Se préparer pour l'entrée en qualification des produits PQC en 2027**, a minima pour :
  - les produits permettant de répondre aux attaques rétroactives
  - les produits qui sont déployés dans des environnements complexes
  - des usages impliquant des longs cycles de vie

Utilisateurs (ministères, OIV, etc.)

- **Anticiper** la transition vers la PQC :
  - Identifier les données et usages menacées
  - Identifier les équipements et contacter les fournisseurs
  - Identifier les délais de renouvellement des équipements
  - Renouveler avec des solutions PQC
  - Identifier les points de blocages
- **Ne plus acheter des produits non-PQC à partir de 2030**

Conclusion

- **La transition vers la PQC est un enjeu majeur de la prochaine décennie :**
  - Elle doit être planifiée le plus possible dans **le cycle de renouvellement des systèmes d'information** pour maîtriser les coûts**.**

- **Cadre réglementaire et référentiels :**
  - Les référentiels et guides concernés seront mis à jour pour intégrer la PQC courant 2026 ;
  - Le cadre réglementaire européen (CSA, CRA, etc.) pourrait imposer, sur le long terme, l'utilisation de la PQC.

- **La disponibilité d'une offre de produits PQC de confiance est nécessaire pour réussir la transition :**
  - Au-delà de de la dimension de sécurité nationale, la transition représente également une opportunité pour nos industriels de rester compétitifs et profiter d'un marché croissant de produits et de prestations PQC.

- **Dates à retenir :**
  - A partir de 2027 : obligation PQC en entrée de qualification ;
  - A partir de 2030 : recommandation de ne plus acheter de produits n'intégrant pas de PQC.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

MERCI !

FAQ PQC : CRYPTOGRAPHIE POST-QUANTIQUE - FAQ | ANSSI