RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

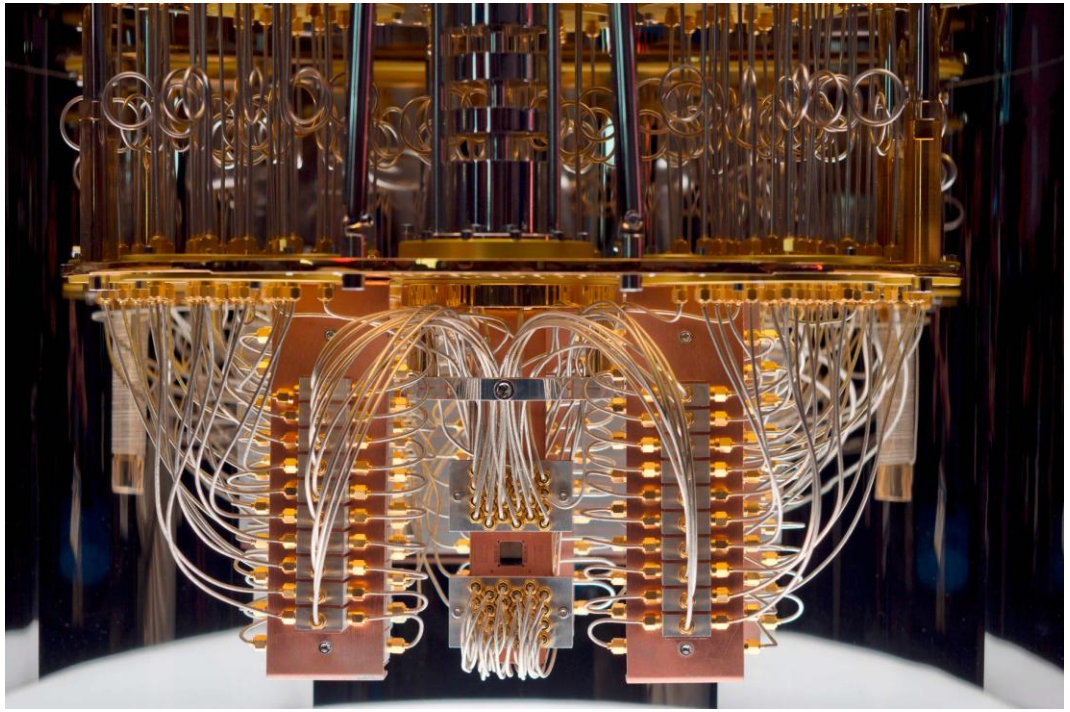
EMPOWERING THE POST-QUANTUM TRANSITION: BUILDING TRUST THROUGH PQC SOLUTIONS

SAMIH SOUISSI
CHIEF OF STAFF – EXPERTISE DEPARTMENT – ANSSI

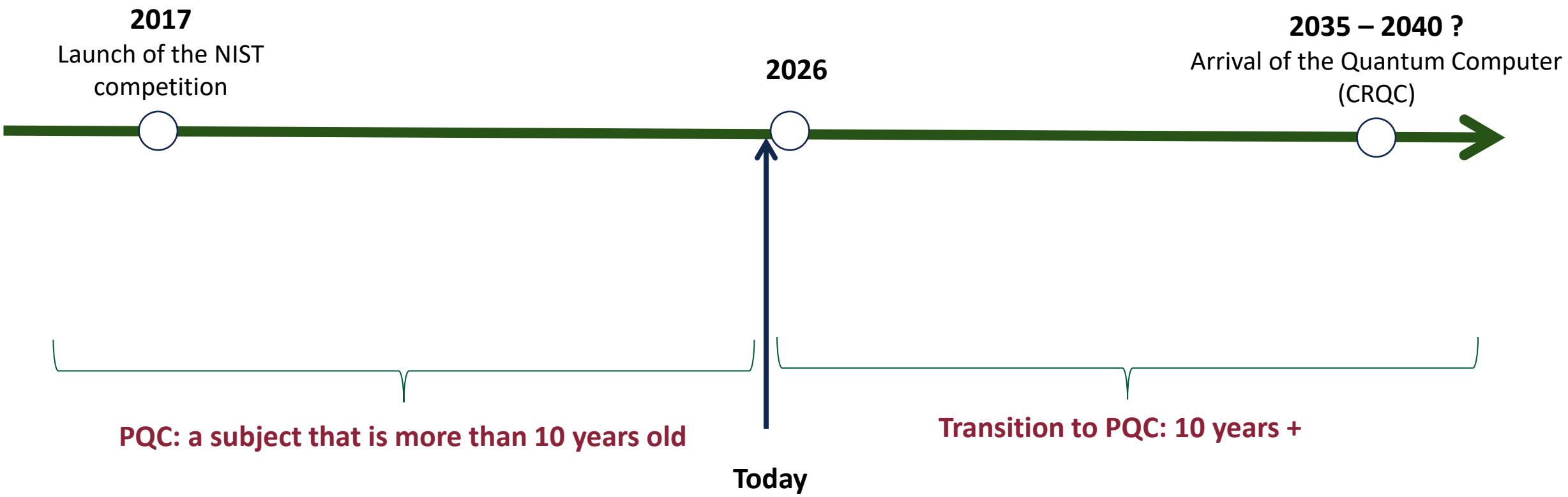
EUROPEAN CONFERENCE ON PQC MIGRATION – 02-03 DECEMBER 2025

PQC: why is it important?

- Large-scale quantum computers, once available, will be able to **break most of the public-key cryptography in use today**.
- The quantum threat must be addressed today.
- **PQC:** the most realistic way forward to respond to the quantum threat.



PQC: A challenge for the next decade



Past actions (2017-2025)

Past actions (2017-2025)

Launch of the NIST competition

Position papers:
ANSSI technical recommendations on PQC algorithms/hybridisation

Normalisation of 3 algorithms by the NIST

Past actions (2017-2025)

Launch of the NIST competition

Position papers:
ANSSI technical recommendations on PQC algorithms/hybridisation

Normalisation of 3 algorithms by the NIST

Ecosystem knowledge:
3 ANSSI market studies (solution providers, users, and consulting companies)

Past actions (2017-2025)

Launch of the NIST competition

Position papers:
ANSSI technical recommendations on PQC algorithms/hybridisation

Normalisation of 3 algorithms by the NIST

Ecosystem knowledge:
3 ANSSI market studies (solution providers, users, and consulting companies)

Certification:
Creation of a PQC scope for ITSEFs certification
Launch of pilot evaluations
First accredited ITSEF and first security visas
Update of recommendations for EU certification (ACM)

Past actions (2017-2025)

Launch of the NIST competition

Position papers:
ANSSI technical recommendations on PQC algorithms/hybridisation

Normalisation of 3 algorithms by the NIST

Ecosystem knowledge:
3 ANSSI market studies (solution providers, users, and consulting companies)

Certification:
Creation of a PQC scope for ITSEFs certification
Launch of pilot evaluations
First accredited ITSEF and first security visas
Update of recommendations for EU certification (ACM)

Training:
Technical initiation to PQC at ANSSI training centre

Past actions (2017-2025)

Launch of the NIST competition

Position papers:
ANSSI technical recommendations on PQC algorithms/hybridisation

Normalisation of 3 algorithms by the NIST

Ecosystem knowledge:
3 ANSSI market studies (solution providers, users, and consulting companies)

Certification:
Creation of a PQC scope for ITSEFs certification
Launch of pilot evaluations
First accredited ITSEF and first security visas
Update of recommendations for EU certification (ACM)

Training:
Technical initiation to PQC at ANSSI training centre

EU coordination:
European PQC roadmap

Past actions (2017-2025)

Launch of the NIST competition

Position papers:
ANSSI technical recommendations on PQC algorithms/hybridisation

Normalisation of 3 algorithms by the NIST

Ecosystem knowledge:
3 ANSSI market studies (solution providers, users, and consulting companies)

PQC strategy:
Publication of ANSSI orientations for the transition to PQC

Certification:
Creation of a PQC scope for ITSEFs certification
Launch of pilot evaluations
First accredited ITSEF and first security visas
Update of recommendations for EU certification (ACM)

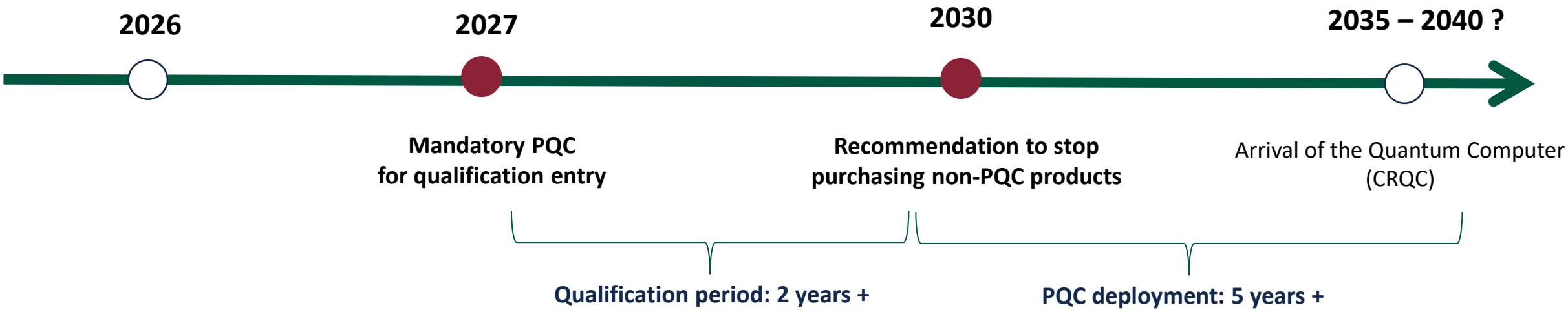
Training:
Technical initiation to PQC at ANSSI training centre

EU coordination:
European PQC roadmap

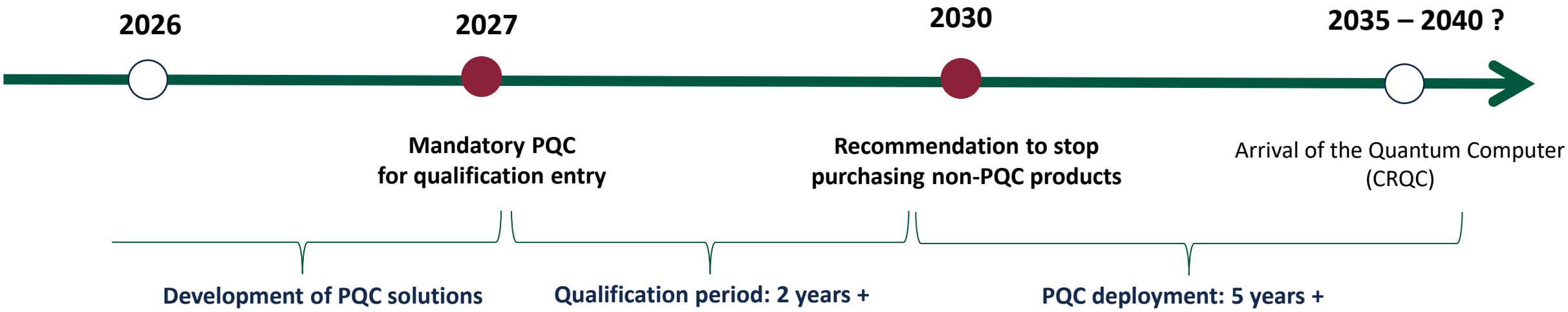
Future actions (2026+)

Future actions (2026+)

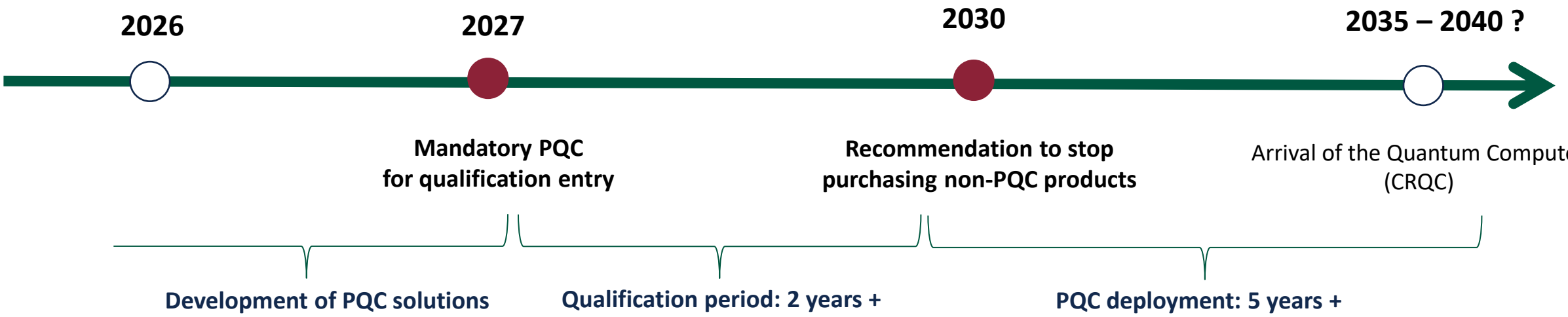
Future actions (2026+)



Future actions (2026+)



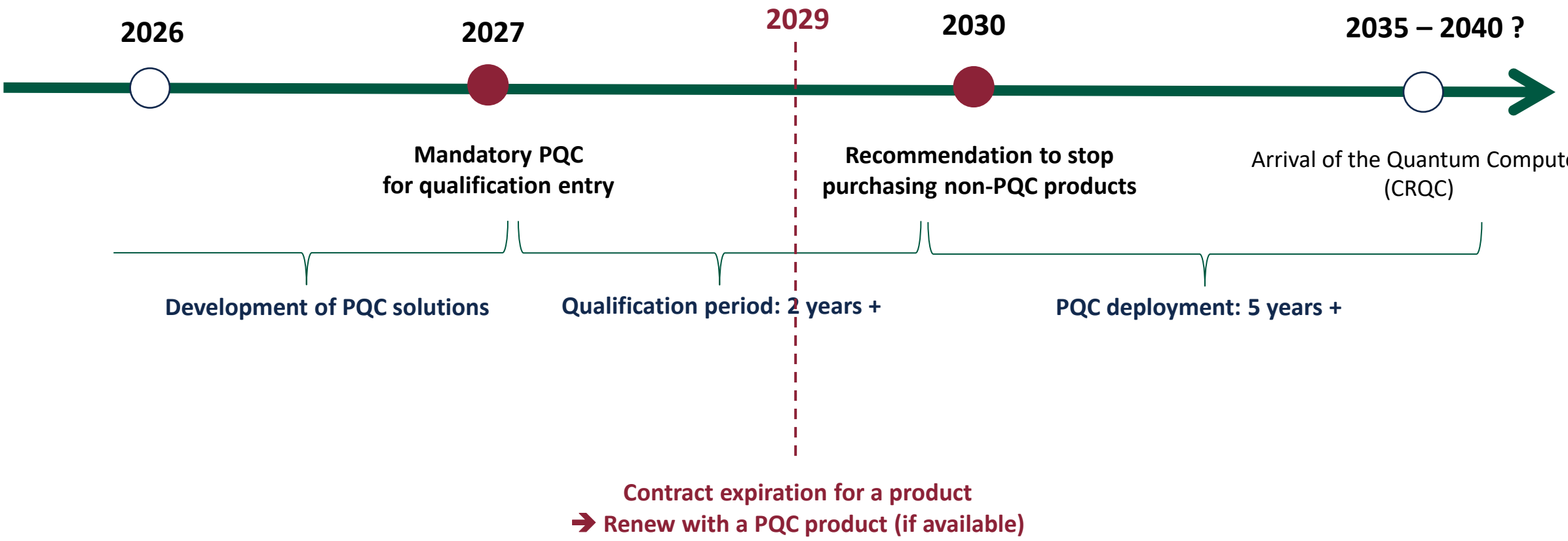
Future actions (2026+)



Prerequisites for the transition

1. Knowledge of the information system and products' renewal timelines
2. Migration planned within the information system renewal cycle

Future actions (2026+) - Example



What to do today?

ANSSI

- Finalize the technical guidelines
- Update existing frameworks and guides
- Continue supporting ITSEFs
- Launching pilot projects to define a PQC transition plan
- Continue EU coordination

What to do today?

ANSSI

- Finalize the technical guidelines
- Update existing frameworks and guides
- Continue supporting ITSEFs
- Launching pilot projects to define a PQC transition plan
- Continue EU coordination

Solution providers

- Initiate PQC developments (if not already done)
- Define and communicate product roadmaps
- **Prepare for PQC product qualification entry in 2027**, at least for:
  - Products addressing retroactive attacks
  - Products deployed in complex environments
  - Products used in long life-cycle applications

What to do today?

ANSSI

- Finalize the technical guidelines
- Update existing frameworks and guides
- Continue supporting ITSEFs
- Launching pilot projects to define a PQC transition plan
- Continue EU coordination

ITSEFs

- Gain and strengthen expertise in evaluating:
  - Recommended PQC algorithms
  - Hybrid mechanisms
  - Side-channel attacks on certain PQC algorithms
- **Be able to evaluation PQC products by 2027**

Solution providers

- Initiate PQC developments (if not already done)
- Define and communicate product roadmaps
- **Prepare for PQC product qualification entry in 2027**, at least for:
  - Products addressing retroactive attacks
  - Products deployed in complex environments
  - Products used in long life-cycle applications

What to do today?

ANSSI

- Finalize the technical guidelines
- Update existing frameworks and guides
- Continue supporting ITSEFs
- Launching pilot projects to define a PQC transition plan
- Continue EU coordination

ITSEFs

- Gain and strengthen expertise in evaluating:
  - Recommended PQC algorithms
  - Hybrid mechanisms
  - Side-channel attacks on certain PQC algorithms
- **Be able to evaluation PQC products by 2027**

Solution providers

- Initiate PQC developments (if not already done)
- Define and communicate product roadmaps
- **Prepare for PQC product qualification entry in 2027**, at least for:
  - Products addressing retroactive attacks
  - Products deployed in complex environments
  - Products used in long life-cycle applications

Users (ministries, critical infrastructure, etc.)

- **Anticipate** the transition to PQC:
  - Identify threatened data/uses
  - Identify involved products and contact suppliers
  - Identify equipment renewal timelines
  - Renew with PQC solutions
  - Identify blocking points
- **Stop purchasing non-PQC products starting from 2030**

Conclusion

- **The transition to PQC is a major challenge for the next decade:**
  - It should be planned within **the information systems renewal cycle**, to control costs.

- **Regulatory framework and guidelines:**
  - In 2026, relevant national frameworks and guides will be updated by ANSSI to include PQC;
  - In the long term, European regulatory frameworks (CSA, CRA, etc.) can be leveraged to mandate the use of PQC.

- **The availability of trusted PQC products is necessary for a successful transition:**
  - Beyond the cybersecurity dimension, this transition is also an opportunity for the industry to remain competitive and benefit from a growing PQC market.

- **Key dates to remember:**
  - From 2027 : PQC obligation for qualification entry;
  - From 2030 : Recommendation to stop purchasing non-PQC products.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

THANK YOU !

PQC FAQ: CRYPTOGRAPHIE POST-QUANTIQUE - FAQ | ANSSI (IN FRENCH)