Developing the European roadmap on PQC

Agenda

Brief reminder of the threat

Existing productions from DE/FR/NL

Recommendation from the EU Commission

Creation of the workstream

Ongoing work

Timeline and next steps

Questions?

September 11: kick-off meeting for the EU workstream on PQC

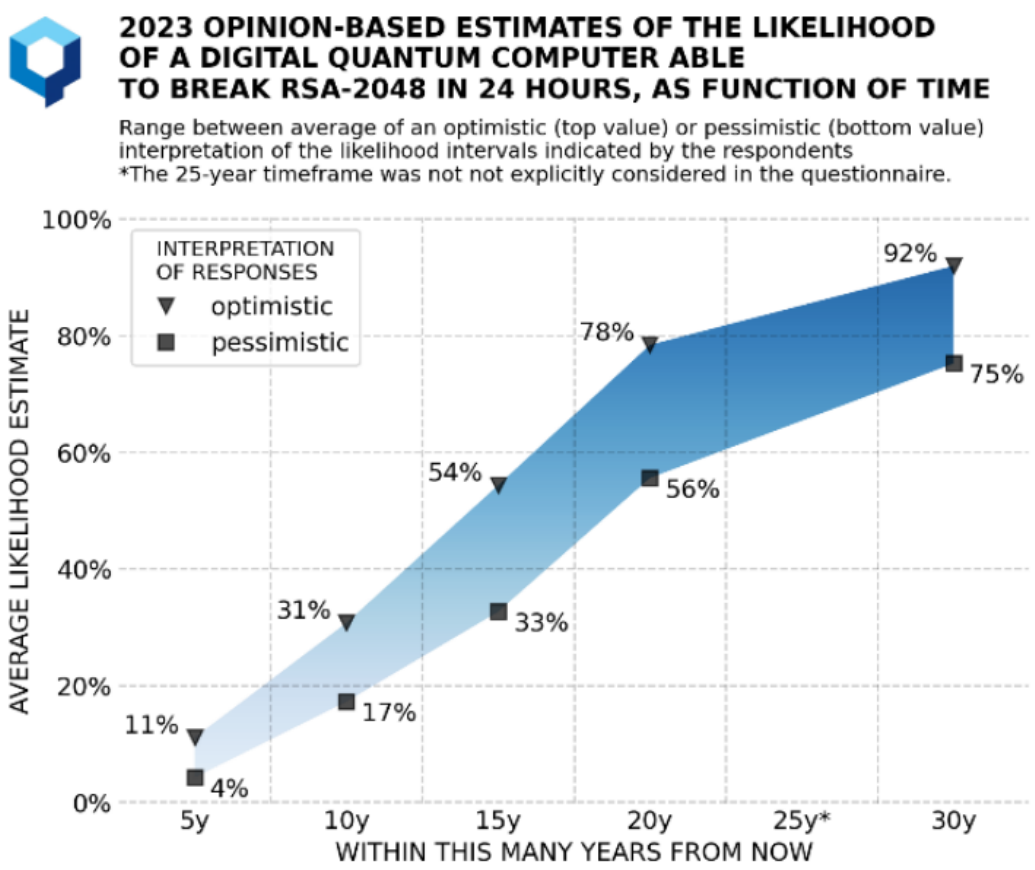
Brief reminder of the threat

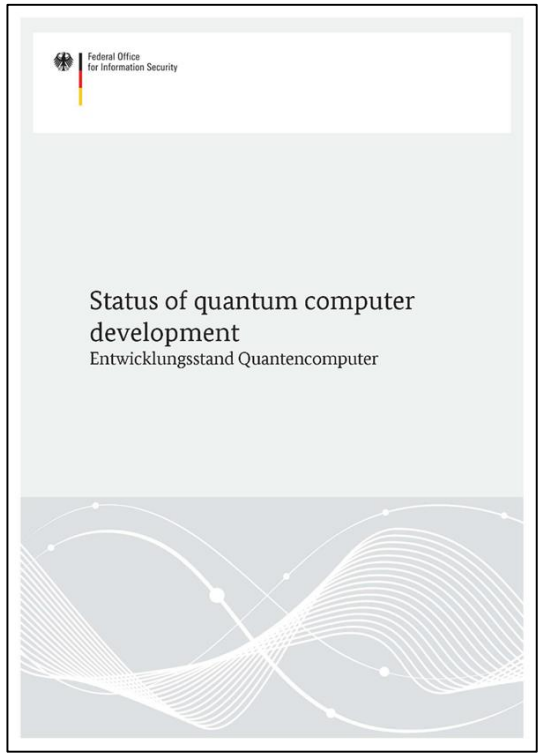
Public-key cryptography at risk: quantum computers will be able to quickly solve the mathematical problems at the basis of current public-key cryptographic standards

Risk for now: harvest now, decrypt later attacks

Risk for later, with catastrophic impacts: personification, forging signatures…

Estimates and studies

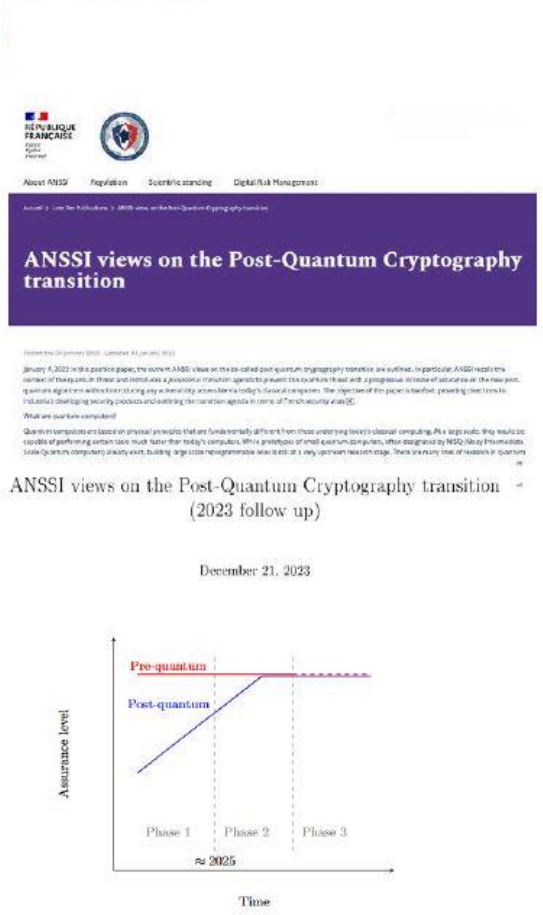


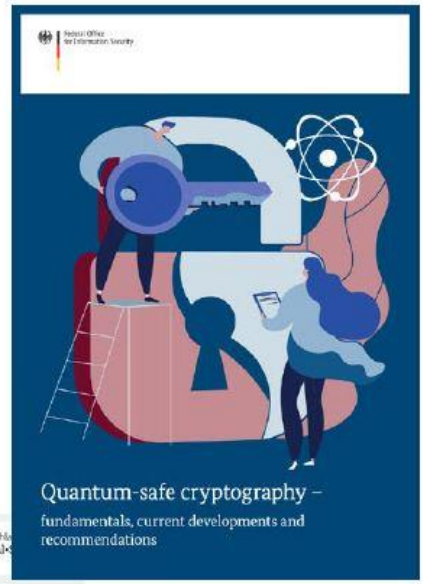


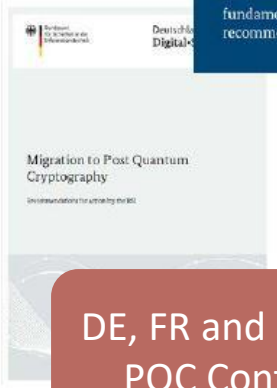
Available at
www.bsi.bund.de/qcstudie
Next update: this month

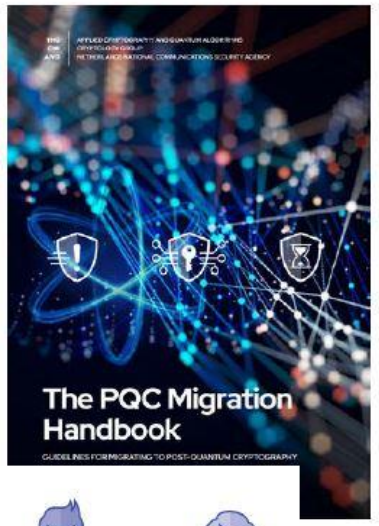
Source: Quantum Threat Timeline Report 2023: Executive Summary, Global Risk Institute, January 2024
Dr. Michele Mosca & Dr. Marco Piani
https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

Existing productions from FR/DE/NL









DE, FR and NL started working together after the PQC Conference in Amsterdam in Nov. 2023

US: NSM-10 and NIST IR 8547

National Security Memorandum 10 (NSM-10) establishes the year 2035 as the primary target for completing the migration to PQC across Federal systems [NSM10]:

> "Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a Cryptographically Relevant Quantum Computer (CRQC). To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035."

US: NSM-10 and NIST IR 8547

4.1.1. Digital Signatures

Table 2 lists currently approved quantum-vulnerable digital signature algorithm standards.

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

4.1.2. Key Establishment

Table 4 lists currently approved quantum-vulnerable key-establishment.

Table 4: Quantum-vulnerable key-establishment schemes

Key Establishment Scheme	Parameters	Transition
Finite Field DH and MQV [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
Elliptic Curve DH and MQC [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [SP80056B]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Recommendation from the EU Commission

Adopted on April 11th

Member states to develop within 2 years a comprehensive strategy for the adoption of PQC across the EU, which ensures:

- a coordinated and synchronised transition among the different member states for the deployment of PQC in public administrations and critical infrastructures;
- a more active role in the selection and adoption of algorithms.

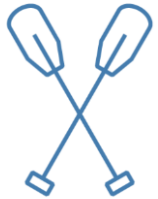
Objectives

1. Foster the transition to PQC
2. Enable member states to define a PQC coordinated implementation roadmap
3. Synchronise efforts of member states
4. Evaluation and selection of PQC algorithms to be implemented in Europe
5. Implement measures to support the transition

Recommendation from the EU Commission

Adopted on April 11th

How ?



Establish a sub-group of the NIS Cooperation Group on PQC with expert representatives from cybersecurity authorities, ENISA, relevant national stakeholders, industry and service providers, other relevant bodies…

Identify measures for defining and coordinating the development of the PQC implementation roadmap

Monitoring and assessment by the Commission in cooperation with the expert representatives of the member states

Creation of the workstream

Kick-off on September 11th

19 EU countries

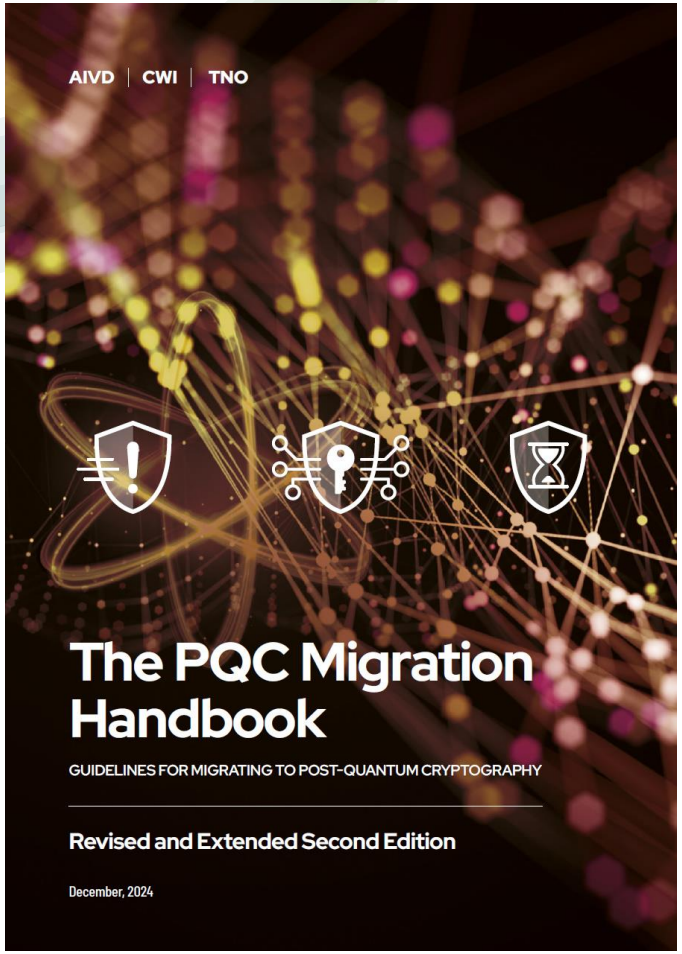
+ EU Commission and ENISA

on this sailboat →

3 plenary meetings including kick-off meeting in Brussels (Sept 11th) and two plenary meetings (Oct. and Nov.)

1 writing group DE – DK – FR – NL – SE to prepare a concept note providing a detailed outlined on the proposed approach to the elaboration of the roadmap

Update of NL PQC Migration Handbook



(collaboration between TNO, CWI and AIVD)

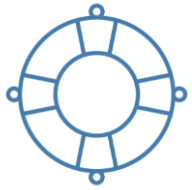
Urgent adopters should start now

→ EU member state governments are urgent adopters

- Sensitive information with a long confidentiality span (“store now decrypt later”)
- Personal Data with a long confidentiality span: e.g. health records
- Provide systems of critical infrastructure: payment transactions, energy, transportation
- Provide systems which are built to have a long life-span: water management, chemical industry, drinking water, railroads

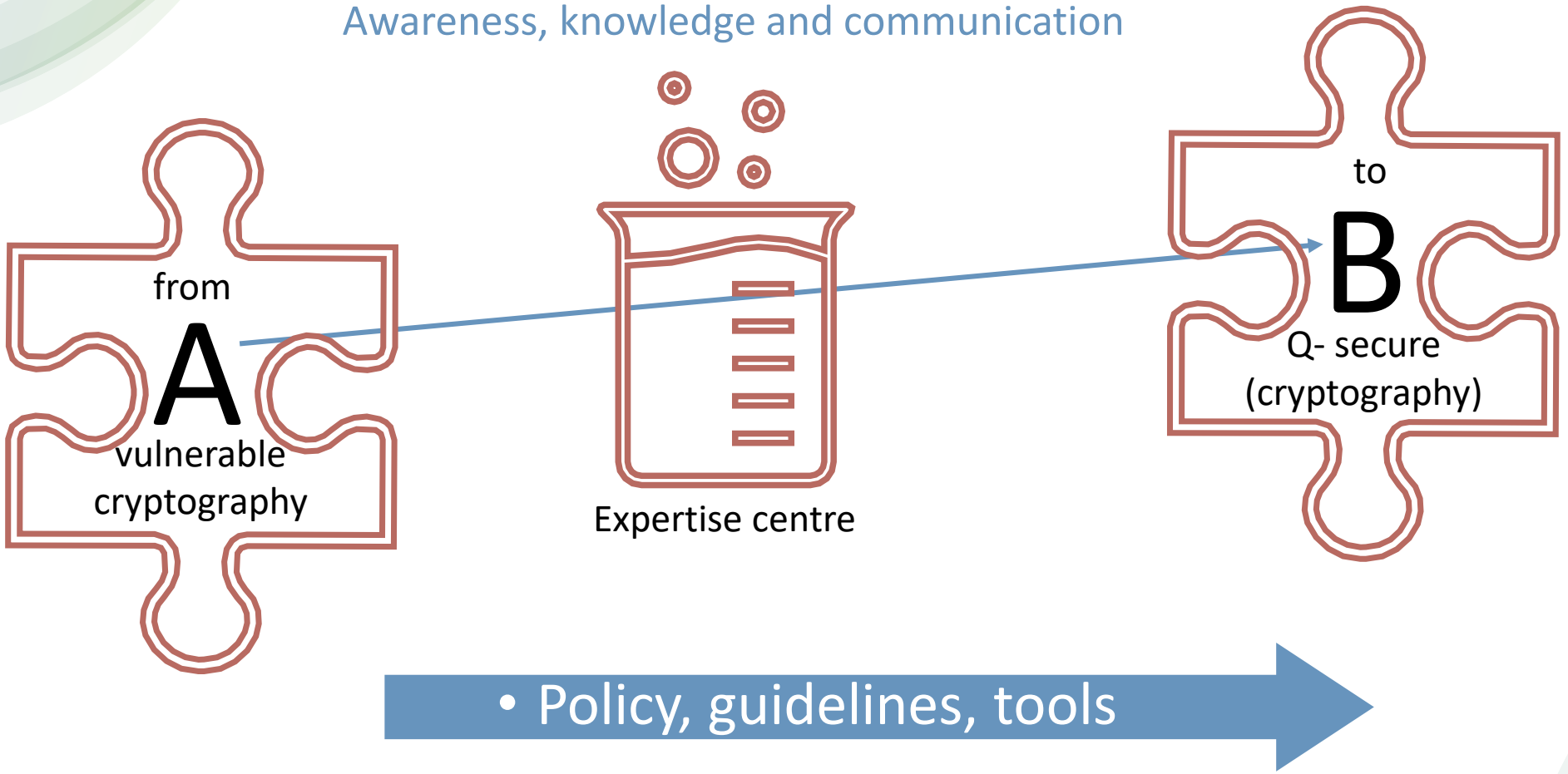
Before we dive in…

The extend to successfully implementing this change, but also to be able to handle unexpected outcomes can be increased if we can manage and – at the same time – coordinate this change on these key aspects: **organisation/people, process and technology**

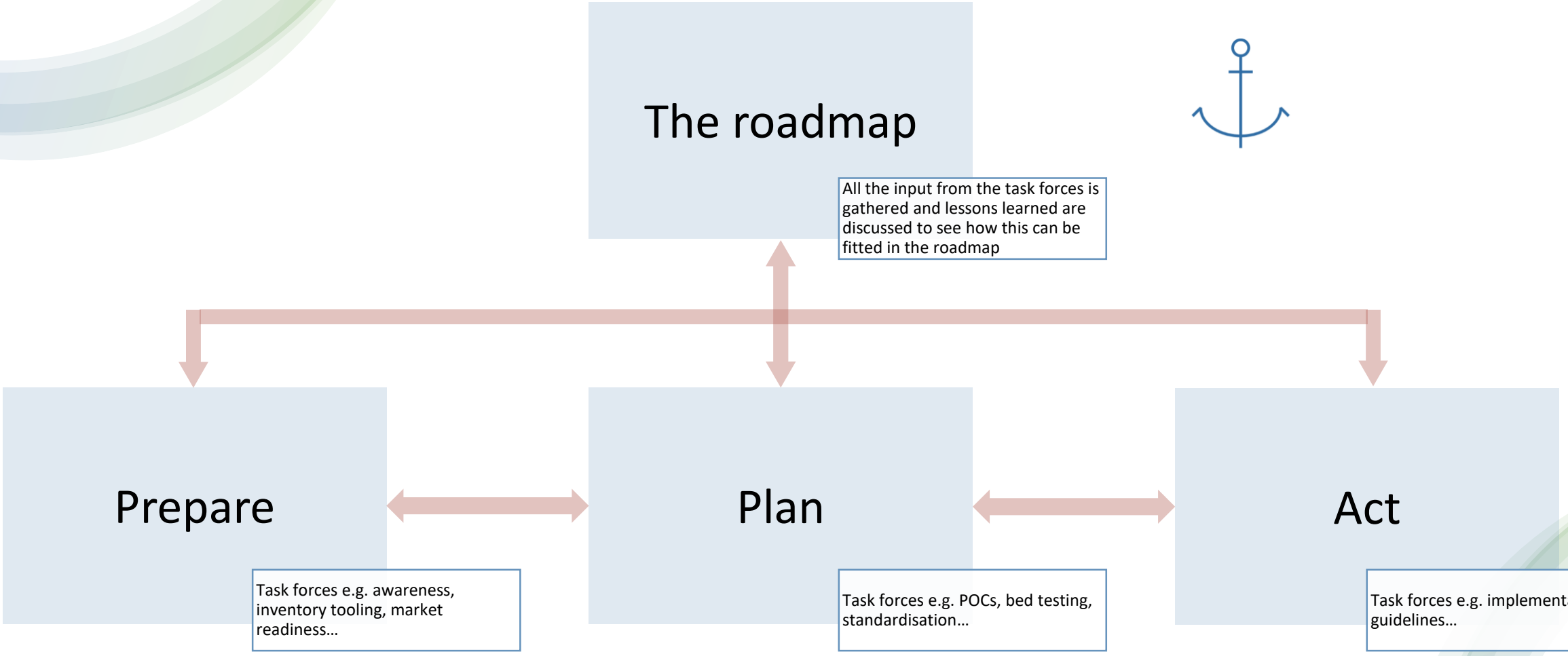


In other words: a **coordinated approach to Europe's transition** to a quantum-safe digital infrastructure is **more than a technical change**

Transition to QSC – a simplified model



Starting building the roadmap



Starting building the roadmap

Core objective
Can't be achieved without thinking about…

Policy/ support

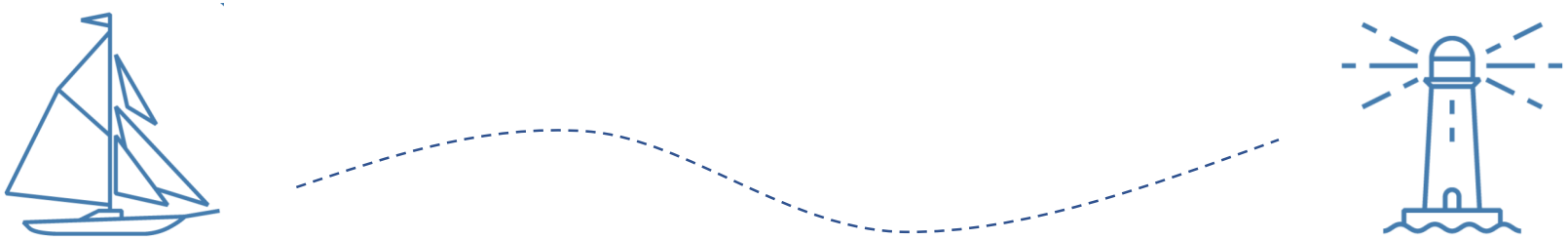
	Member states	Users	Suppliers/market
Prepare	e.g. make risk assessment…	e.g. have inventory tools…	e.g. propose tools…
Plan	e.g. create guidelines…	e.g. conducts POCs…	e.g. have testing facilities…
Act	e.g. coordinate the transition…	e.g. implement products with priorities…	e.g. propose consulting services…

Environment

- Awareness and communication (e.g. productions, events…)
- Skills, knowledge and employability (how to bring out experts?)
- Cooperation with other groups (e.g. ENISA, standardisation bodies…)
- EU funding (e.g. HEP and DEP…)

Timeline and next steps

Publish a concept paper to detail the outline of the proposed approach to elaborating the roadmap. Expected deadline: mid-2025.



Have a coordinated roadmap by the end of the workstream in 2027 on which all member states can rely!

Any questions?

What do you expect to receive as a result of the work of the EU workstream?

In what way would you be willing to contribute to the work carried out?

…

Thank you!