

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...

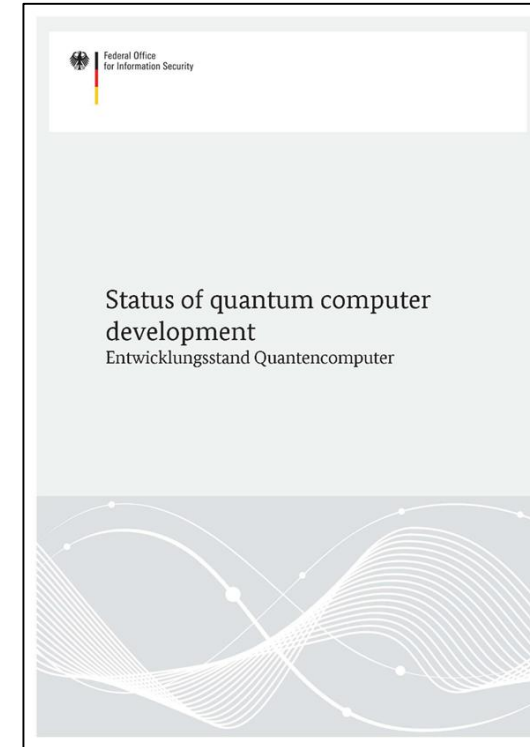
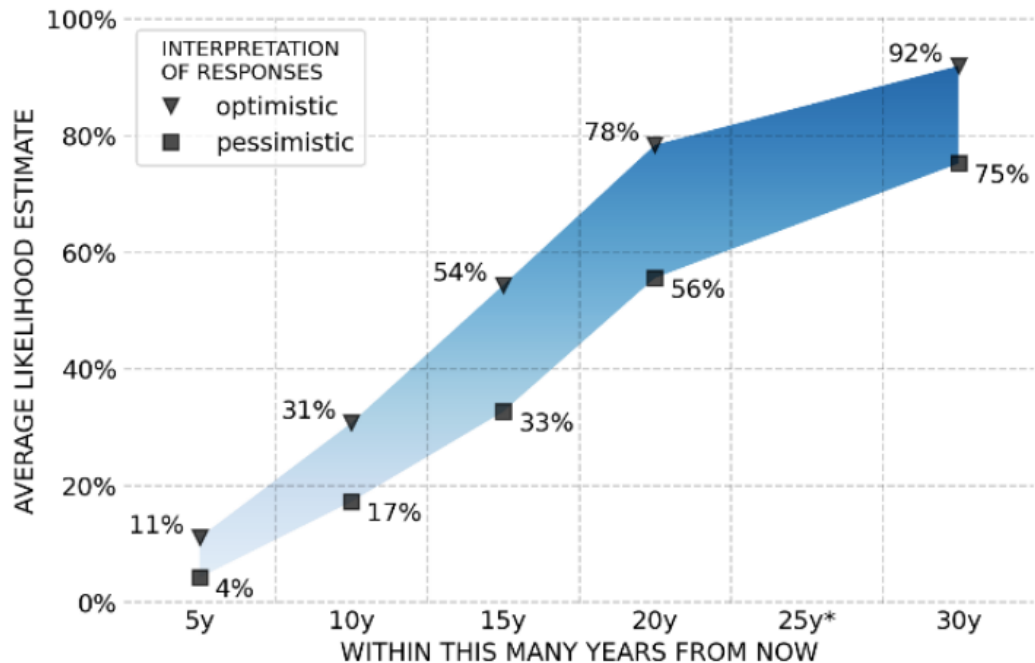
Estimates and studies



2023 OPINION-BASED ESTIMATES OF THE LIKELIHOOD OF A DIGITAL QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS, AS FUNCTION OF TIME

Range between average of an optimistic (top value) or pessimistic (bottom value) interpretation of the likelihood intervals indicated by the respondents

*The 25-year timeframe was not explicitly considered in the questionnaire.



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/>

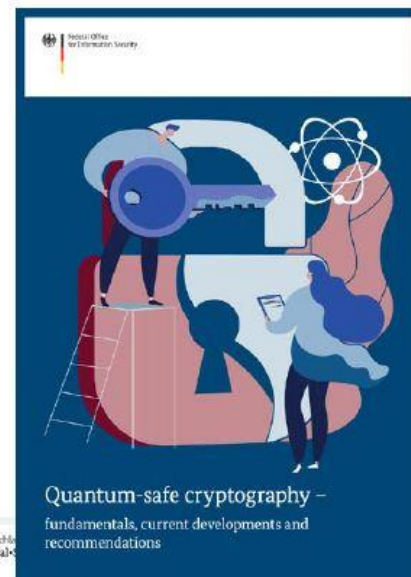
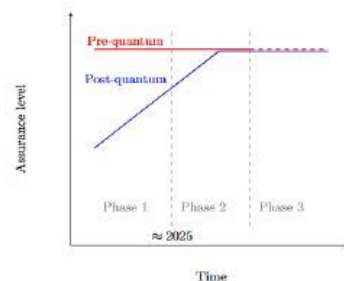
PQC symposium – December 3rd, 2024

Existing productions from FR/DE/NL



ANSSI views on the Post-Quantum Cryptography transition
(2023 follow up)

December 21, 2023



URGENT ADAPTERS	REGULAR ADAPTERS	CRYPTOGRAPHY EXPERTS
<p>Urgent Adapters Organisations which handle sensitive data or provide critical or long-lived infrastructures. These organisations should start taking first steps on PQC migration as soon as possible. Within this category, we have made a distinction between the different kind of organisations that have to move quickly, depending on why they are at risk of being attacked by a quantum computer.</p>	<p>Regular Adapters Organisations which do not handle sensitive data and do not provide critical or long-lived infrastructures with a high risk of being attacked. These organisations may, for example, still handle sensitive data, but it is unlikely that data is currently being stored for decryption by a future quantum computer.</p>	<p>Cryptography Experts Organisations that supply cryptographic standards or infrastructure. The main difference between cryptography experts and urgent adapters is that cryptography experts should have most of the necessary cryptography knowledge for PQC migration in house already, and that they are responsible for cryptographic aspects of other organisations as well.</p>

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	<i>Deprecated</i> after 2030 <i>Disallowed</i> after 2035
	≥ 128 bits of security strength	<i>Disallowed</i> after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	<i>Disallowed</i> after 2035
RSA [FIPS186]	112 bits of security strength	<i>Deprecated</i> after 2030 <i>Disallowed</i> after 2035
	≥ 128 bits of security strength	<i>Disallowed</i> 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	<i>Deprecated</i> after 2030 <i>Disallowed</i> after 2035
	≥ 128 bits of security strength	<i>Disallowed</i> after 2035
Elliptic Curve DH and MQC [SP80056A]	112 bits of security strength	<i>Deprecated</i> after 2030 <i>Disallowed</i> after 2035
	≥ 128 bits of security strength	<i>Disallowed</i> after 2035
RSA [SP80056B]	112 bits of security strength	<i>Deprecated</i> after 2030 <i>Disallowed</i> after 2035
	≥ 128 bits of security strength	<i>Disallowed</i> 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

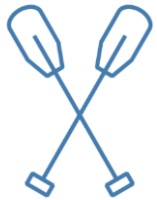
1. Foster the transition to PQC
2. Enable member states to define a PQC coordinated implementation roadmap
3. Synchronise efforts of member states
4. Evaluation and selection of PQC algorithms to be implemented in Europe
5. Implement measures to support the transition



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

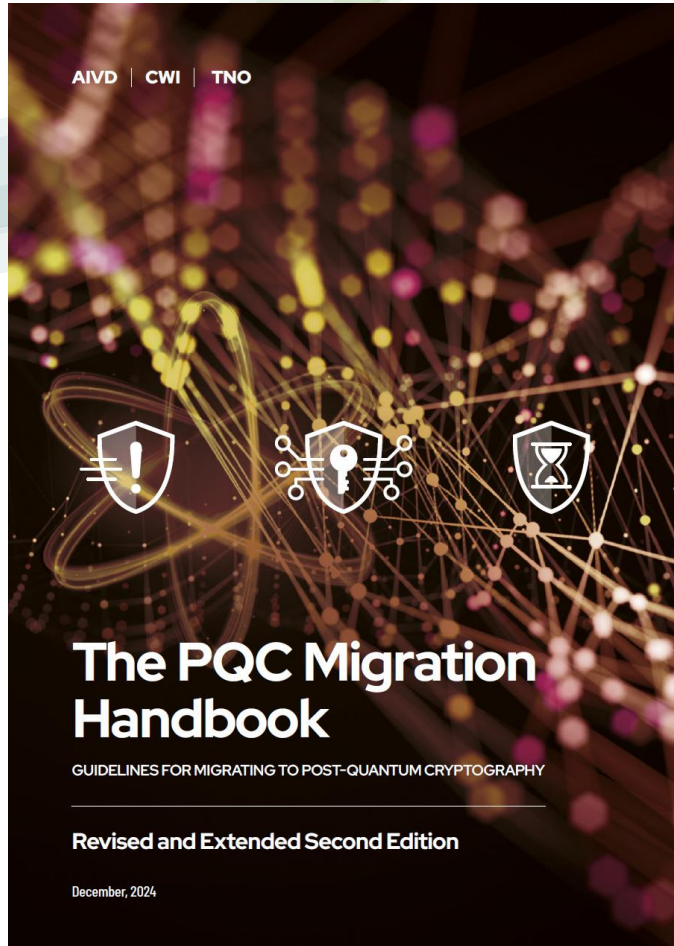
19 EU countries
+ EU Commission and ENISA
on this sailboat →



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



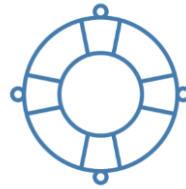
(collaboration between TNO, CWI and AIVD)

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

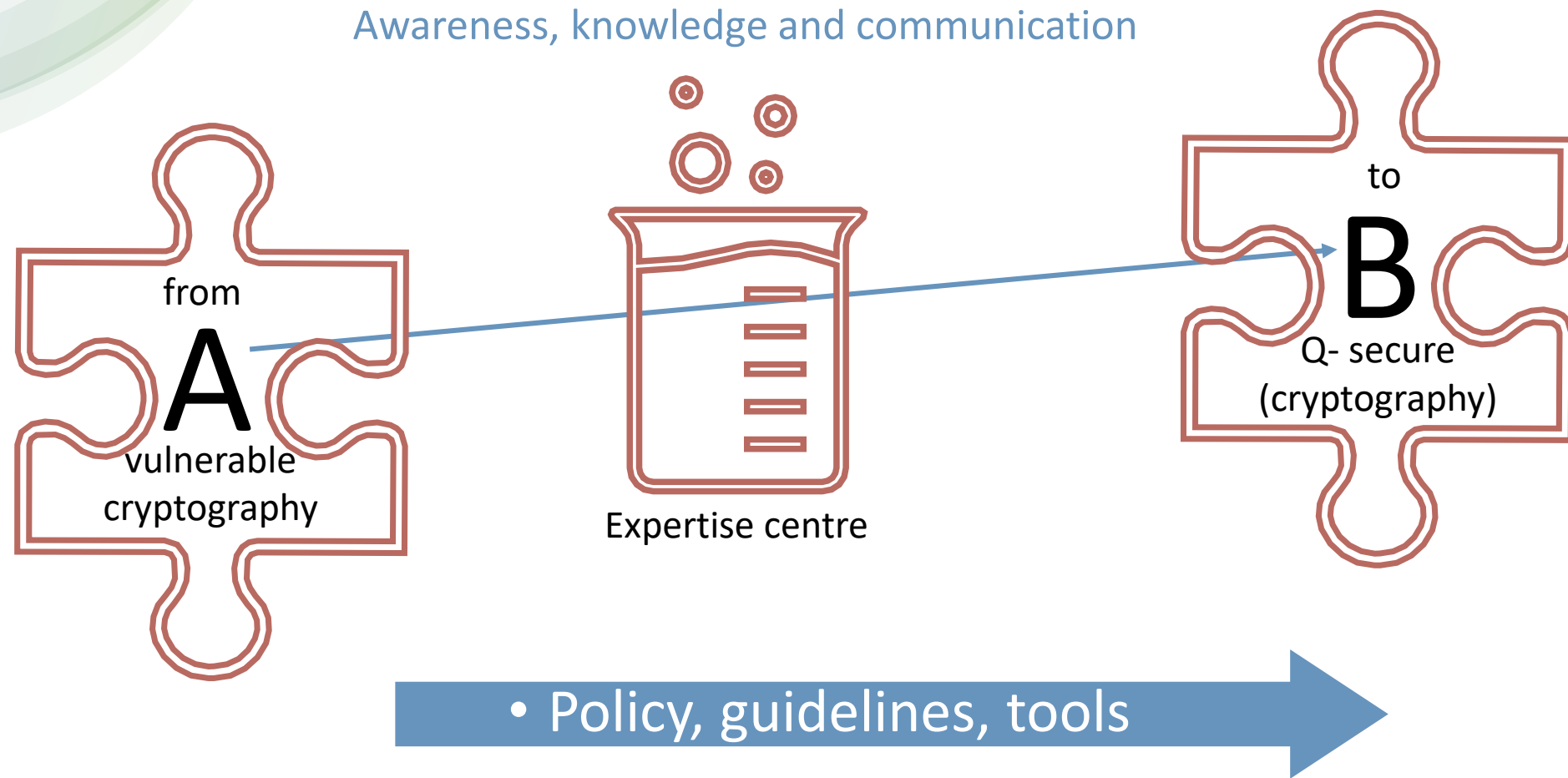
Before we dive in...

The extent 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**

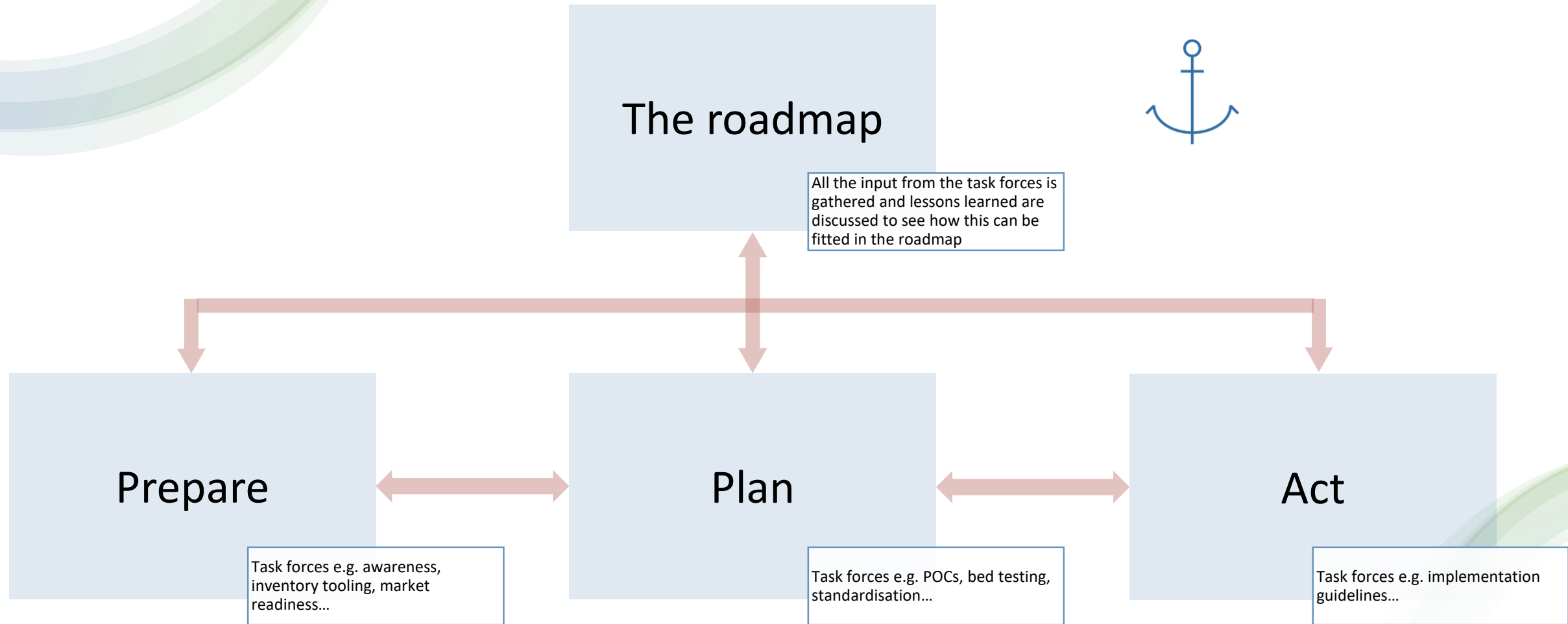


In other words: a **coordinated approach to Europe's transition to a quantum-safe digital infrastructure is more than a technical change**

Transition to QSC – a simplified model



Starting building the roadmap



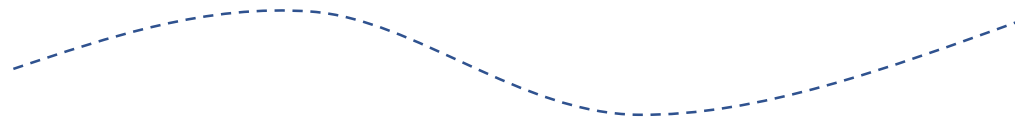
Starting building the roadmap

Core objective
Can't be achieved without thinking about...

		Member states	Users	Suppliers/market
Policy/ support	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!