



Roadmap for the Transition to Post-Quantum Cryptography (PQC)

Juraj Kubica

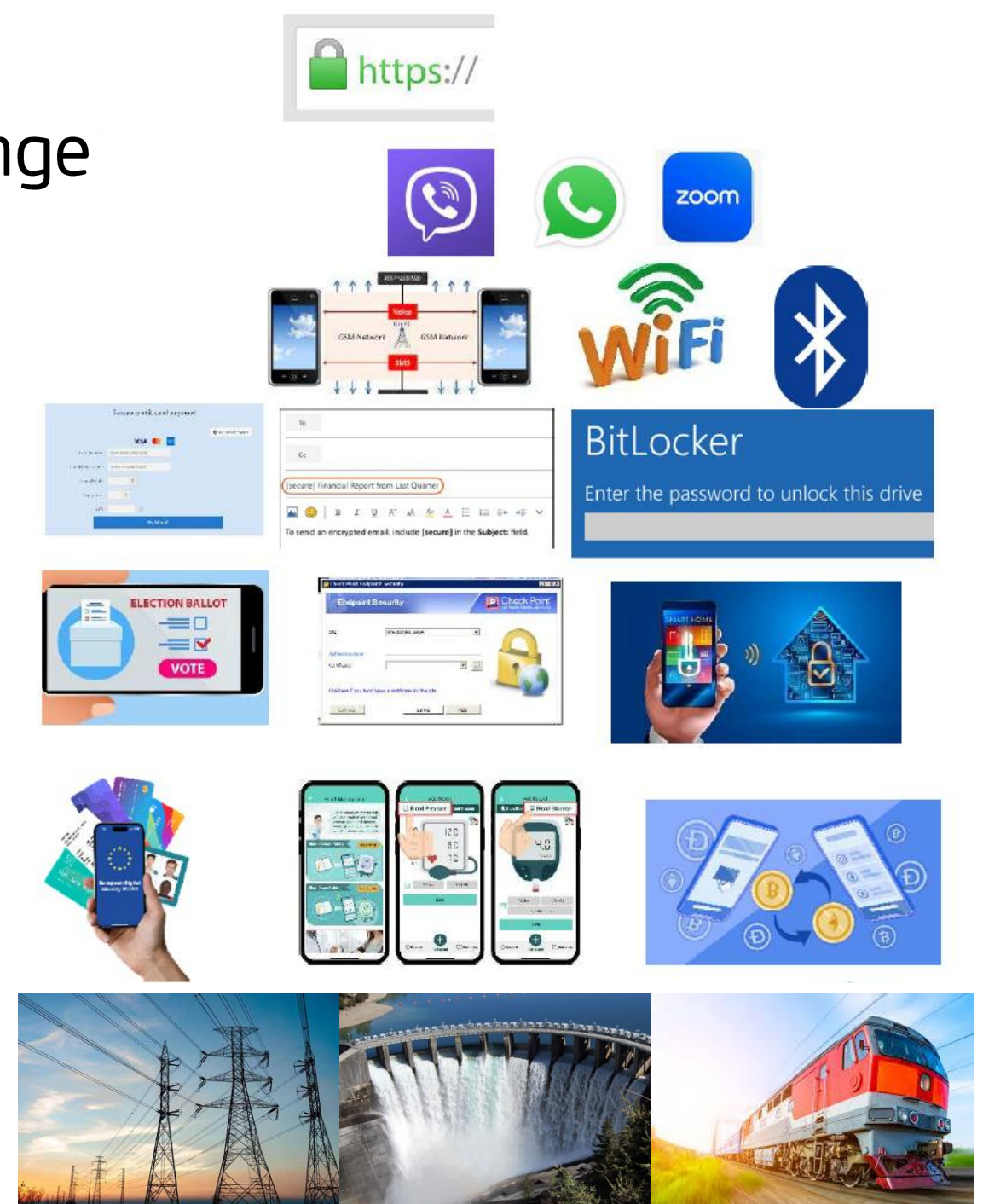
Policy Officer

Unit Emerging and Disruptive Technologies

Directorate General for Communications Networks, Content, and Technology (DG CNECT)

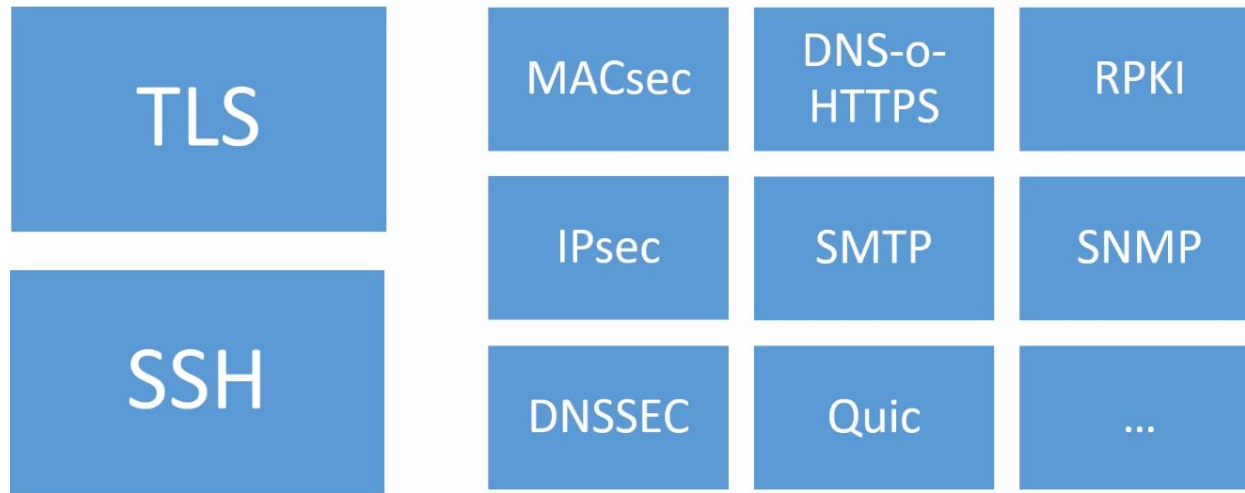
PQC migration is a **huge** challenge

Web browsing
Email - Messaging apps - Teleconferences
Mobile communications
Wireless networks (802.11x, Bluetooth, ...)
Virtual Private Networks (VPN)
IoT communications
Electronic payments (e-commerce)
Enterprise security – (Hard) disk security
Electronic voting
Digital wallet – digital identities
eHealth – mhealth
Distributed Ledger Technology (Bitcoin, Ethereum...)
Operational Technology (OT) / legacy systems ...



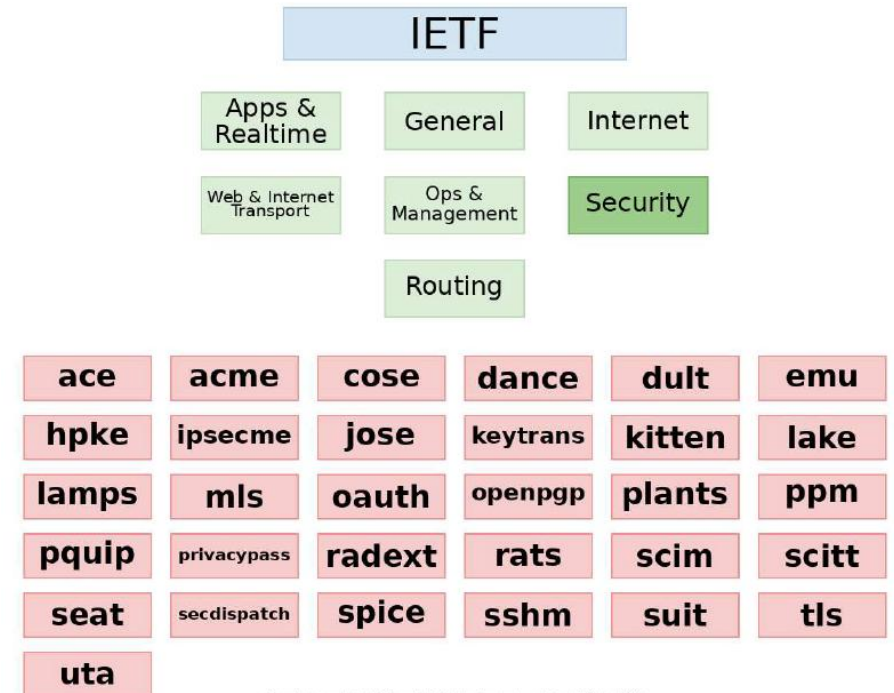
Even simply to secure the internet is an immense challenge...

Securing the internet



From the seminar by Bart Preneel at the IPEN event
on post-quantum cryptography

...NIST published three PQC standards in August 2024



Security Area active WGs from IETF Datatracker /wsg/ — retrieved 18 May 2026

Working groups at IETF

Recent policy initiatives

April 2024



Brussels, 11.4.2024
C(2024) 2393 final

COMMISSION RECOMMENDATION

of 11.4.2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Having regard to Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148¹ (NIS 2 Directive).

HAS ADOPTED THIS RECOMMENDATION

1. SCOPE AND OBJECTIVES

The purpose of this Recommendation is to foster the transition to Post-Quantum Cryptography for the protection of digital infrastructures and services for public administrations and other critical infrastructures in the Union by enabling Member States to:

- (1) define a 'Post-Quantum Cryptography Coordinated Implementation Roadmap' aimed at synchronising the efforts of Member States to design and implement national transition plans while ensuring cross-border interoperability;
- (2) support the evaluation and selection of relevant Post-Quantum Cryptography EU algorithms with the help of cybersecurity experts, and further adoption of such algorithms as Union standards that should be implemented across the Union as part of the Post-Quantum Cryptography Coordinated Implementation Roadmap.
- (3) take appropriate and proportionate measures to prepare for this transition.

2. COORDINATED IMPLEMENTATION ROADMAP ADDRESSING THE TRANSITION TO POST-QUANTUM CRYPTOGRAPHY

- (4) This Recommendation encourages Member States to coordinate their actions at Union level through a dedicated Member States forum. For this purpose, the Commission recommends that Member States take advantage of existing structures at Union level in the area of cybersecurity and establish a sub-group of the NIS Cooperation Group. Such sub-group could include representatives of national

June 2025

Roadmap for a Coordinated Transition across the EU

<https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography>

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

Part 1, Version: 1.1, EU PQC Workstream

January 2026

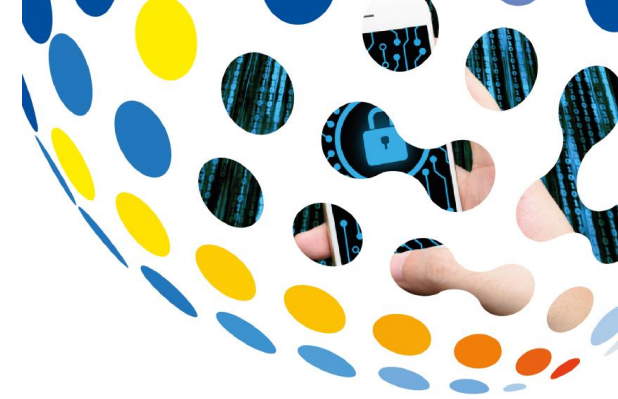
A cybersecurity simplification package [COM\(2026\) 13](#) – a proposed directive **amending NIS2** with targeted changes including the first explicit PQC requirement written directly into the directive text. The key provision is in [Article 7\(2\)\(k\)](#), which would require Member States to adopt national policies “for the transition to post-quantum cryptography, taking into account the transition timelines and relevant requirements set out in applicable Union legal acts and policies.”

Proposal to revise the Cybersecurity Act (**CSA2**) aims to expand ENISA's mandate to increase EU cybersecurity resilience.

The EU PQC Roadmap (looking more closely)

A Coordinated Implementation Roadmap for the Transition to PQC Cryptography

<https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography>



A Coordinated Implementation
Roadmap for the Transition to
Post-Quantum Cryptography

Part 1, Version: 1.1, EU PQC Workstream

A separate PQC workstream in the NIS Cooperation Group was created. First version of the Roadmap released in June 2025:

- ❖ By **31/12/2026**: PQC roadmaps defined in each MS. Planning for high- and medium-risk use cases will be underway.
- ❖ By **31/12/2030**: high-risk use case migrated: critical infrastructure (e.g. water, energy, health care, finance and transportation) and high-risk domains. Quantum-safe software and firmware upgrades are enabled by default. Transition planning for medium-risk ones.
- ❖ By **31/12/2035**: All of the migrations should be completed for every risk level.

From 11 August to 29 September 2025, the NIS Cooperation Group ran a survey to ask for feedback on the PQC Roadmap.

The **results of the public consultation on the EU Roadmap** as well as a document with Frequently Asked Questions (**FAQ**) on the Roadmap have been published.

Strong hook to the Cyber Resilience Act in the Roadmap
Necessity to develop national industrial policies

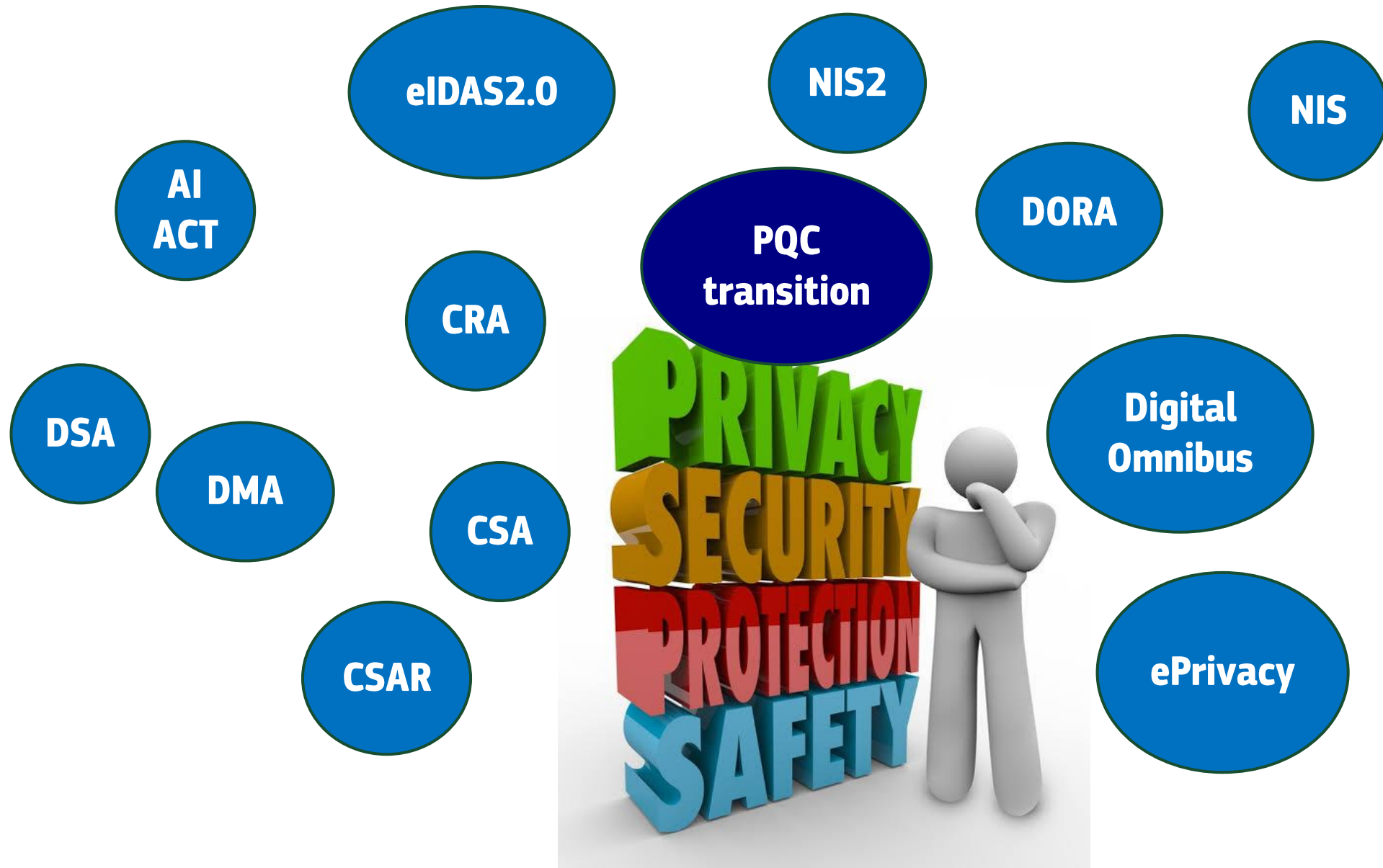
Beneficial steps, no just another regulation

Many steps in the PQC transition are part of the **no-regret moves** that need to be done by all responsible actors.

Algorithm failure must be treated as an expected lifecycle event.

- Crypto-agility principle,
 - Zero-trust architecture,
 - Compilation of the cryptographic bill of materials (CBOM)
 - and many other
- are important regardless of the advent of cryptographically relevant quantum computers.

The EU Digital landscape is a complex puzzle!



What kind of European digital future should the PQC transition help create?

concomitant challenge of digital sovereignty – the digital future will be shaped on how we act on the Eurostack

Strategic autonomy

autonomous technological choices while remaining open to international cooperation and maintaining interoperability

Interoperability

secure and trustworthy digital infrastructures should themselves be enablers of fundamental rights

new possibilities and challenges arising from emerging technologies

Innovation

technological innovation should not be seen as competing with fundamental rights

Fundamental rights

securing control over data, technology, infrastructure

Security

ePrivacy

CSAR

DMA

DSA

eIDAS2.0

NIS2

Digital
Omnibus

PROTECTION
SAFETY

Privacy, data protection and innovation by different technologies

Powerful trends are converging to reshape how organizations and regulators approach data governance in 2026.

GDPR Revision

could change fundamental definition of personal data, in the pursue of competitiveness and regulatory simplification

AI's Rapid Rise

how AI systems intersect with privacy frameworks. Debates over AI agents, AI models

Expanding Digital Regulation beyond data protection

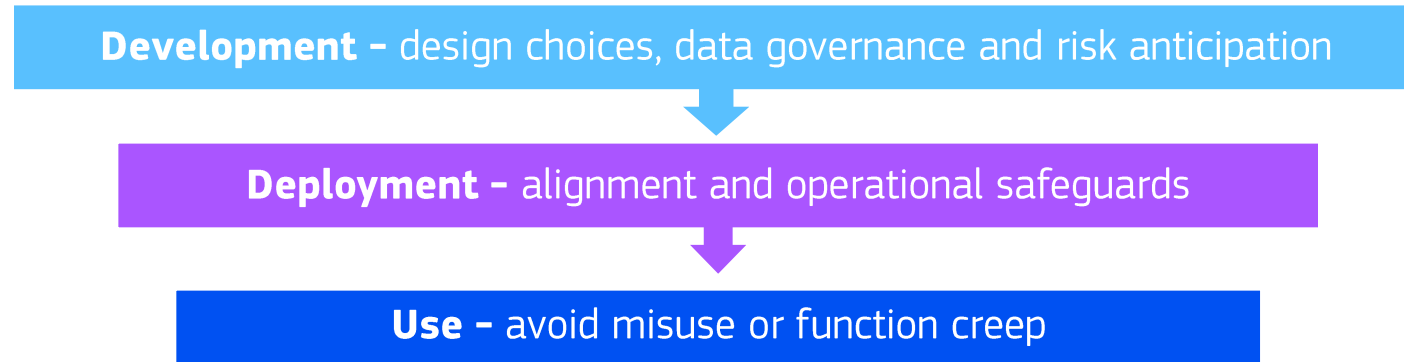
online safety, data strategy frameworks. New compliance challenges

Driving Innovation via Regulations

Tech Sovereignty Package which includes the Open Source Strategy + upcoming Quantum Act

The absence of coordinated legislation risks leading to a patchwork of divergent national rules, potentially undermining consistent INTEROPERABILITY.

We work for nurturing a culture of compliance structured around three core stages of the lifecycle of all digital applications impacted by the PQC transition



Each phase raises distinct legal, operational and governance obligations, and **compliance must be embedded from the outset rather than treated as a post hoc control mechanism**. All this is a continuous process integrating technical, legal and organisational measures for all the activities envisioned.

The PQC transition is and will be an opportunity for actions to ensure Europe can maintain leadership in a fundamental technology for economic security, to both modernise and ensure a human-centric EU digital future without compromising our core principles.



Thank you for your attention!

juraj.kubica@ec.europa.eu

What we are doing in CNECT

EXTRACT STRATEGIC INSIGHTS ON TECHNICAL AND POLICY CHALLENGES & TECHNICAL ANALYSES

- Extract the most valuable insights from scientific articles, reports and see what decisions each of them informs, for the protection of
 - data-in-transit (communications)
 - data-at-rest (stored)
 - data-in-use (AI processing, cloud applications, ...)
- Analysis of how current policy/legislative proposals impact cryptographic security and the implications on the PQC transition
- Monitor studies on attacks, advances in real-world deployments of PQC, needs for supply chain
- Follow work at standardization bodies/monitor standardization landscape (NIST, IETF, ISO, ETSI, CCSDS, 3GPP Non-Terrestrial Networks, ...)

Design of strategies

Design and contribution to:

- Specific PQC calls, but also for many other calls
 - Work Programmes
- Strategies and Roadmaps

Injection to and Analysis of Policies

Impact of different policies on PQC or link of different policies to PQC and input to policies

Work with the PQC Workstream in the NIS Cooperation Group

Contribute to the work on migration of EU bodies
(Commission, Parliament, Council, + other tenths of EU bodies)

Dialogues, work and collaboration with others

High-level international dialogues, work with ECCC and ENISA, international and EU standardization