Ongoing, planned and potential future activities in PQC at DG CONNECT

Fabiana Da Pieve

Program Manager
Unit “Emerging and Disruptive Technologies”
Directorate General for Communications Networks, Content, and Technology (DG CONNECT)

Commission moves on two fronts

Post-Quantum Cryptography (PQC)

Research priorities under Horizon Europe (HE):

- cryptanalysis, security of PQC implementations, integration into protocols, PETs…

Under Digital Europe Programme:

- Transition of the PKI
- EU testing infrastructure

insert PQC horizontally in several clusters of HE

A number of projects but no targeted Specific Grant agreements

Urgency to transition to PQC likely higher than expected

Real threat … not only HW, but also algorithmic optimization

European Quantum Communication Infrastructure (EuroQCI) & Quantum Flagship

Make the first-generation quantum networks **with the sole QKD functionality applicable – and some few beyond QKD applications**

DEP, CEF, IRIS2, with a first satellite demonstrator Eagle-1

Accelerate the development of next generation(s) Quantum Network Technology (HE, Quantum Flagship)

Both open and **targeted Specific Grant agreements**

EuroQCI

QSN PARTNERSHIP

QIA QUANTUM INTERNET ALLIANCE

(some) Ongoing, past, just started EU projects
Horizon Europe, DEP, H2020

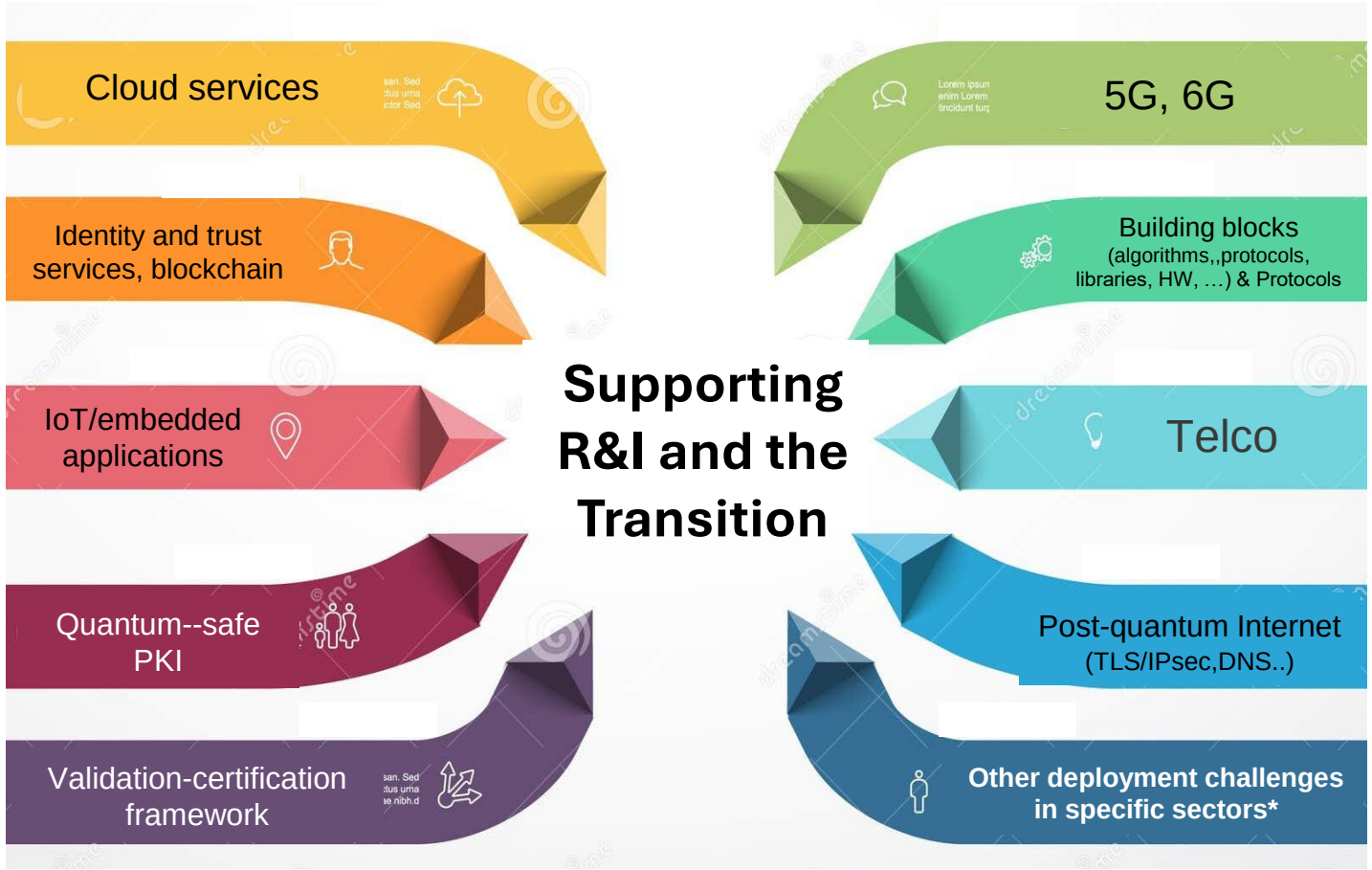
PQCRYPTO

QUBIP, PQC4eMRTD, PQ-REACT, PROMETHEUS, PRIViLEDGE

QUBIP, PQCRYPTO

PQC4eMRTD, PiQASO, HAPKIDO (NL, national)

WORK IN ECCG CHAIRED BY ENISA



CONFIDENTIAL6G, XTRUST-6G

QUBIP, ERC EPOQUE (integ. in procotols), ERC ARTICULATE (libraries), SAFECrypto, PiQASO (HW), ERC ISOCRYPT (non-lattice based), ERC BRIDGE

QUBIP, PQ-REACT

QUBIP, PQCRYPTO

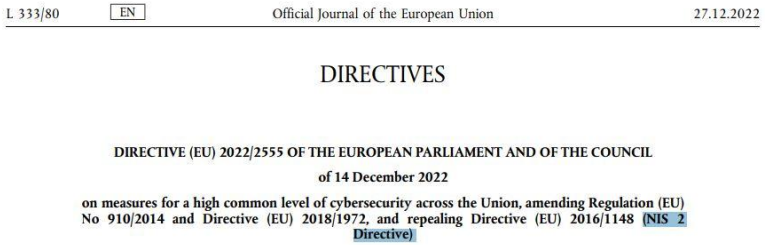
Automotive (PQCSA)
Financial sector (NGI-TALER, EPOQUE)
Administrations (Q-PrEP)
Several industrial sectors (PIQASO)
Defence (SMiEQ)
Work of PQC in space, energy grids …

Evaluations started for submissions to the PKI call, managed by European Cybersecurity Competence Centre (ECCC)

Policy Framework

PQC indirectly and directly addressed in several EU policies and legislations

NIS 2



L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

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) 2016/1148 (NIS 2 Directive)

Economic Security Strategy

EUROPEAN COMMISSION

HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

Brussels, 20.6.2023
JOIN(2023) 20 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL

ON "EUROPEAN ECONOMIC SECURITY STRATEGY"

Commission's White Paper

EUROPEAN COMMISSION

Brussels, 21.2.2024
COM(2024) 81 final

WHITE PAPER

How to master Europe's digital infrastructure needs?

Recommendation on PQC

EUROPEAN COMMISSION

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

Cyber Resilience Act

Official Journal of the European Union EN L series

2024/2847 20.11.2024

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 October 2024

on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

ProtectEU

EUROPEAN COMMISSION

Strasbourg, 1.4.2025
COM(2025) 148 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on ProtectEU: a European Internal Security Strategy

Roadmap for a Coordinated Transition across EU

New PQC workstream in the NIS Cooperation Group created

First version of the Roadmap released (June 2025):

Timeline:

- By 31/12/2026. PQC roadmaps defined in each MS. Planning for high- and medium-risk use cases will be underway.
- By 21/12/2030: high-risk use case migrated: critical infrastructure (eg 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.

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

Strong hook to the Cyber Resilience Act in the Roadmap

Necessity for consideration of EU Cybersecurity Policies in National Actions

Next steps

Feedback loops on several fronts

Examples:

Work ongoing to incorporate comments/feedback by several actors on the PQC Roadmap, received through an open call for contributions

Open Public Consultation on the proposal for a revision of the ‘EU Standardisation Regulation’ - ddl: 17/12/2025

https://single-market-economy.ec.europa.eu/consultations/public-consultation-proposal-revision-regulation-eu-no-10252012-also-called-eu-standardisation_en

Digital Identities & Post-quantum Digital Trust

New digital signatures and advanced cryptographic schemes for enhanced privacy

→ Continued support to our researchers for contributing to international efforts

→ The Commission recognizes the need for fostering global collaboration

Space

Envision additional activities (in conjunction with DG DEFIS) to secure Space tomorrow’s architecture

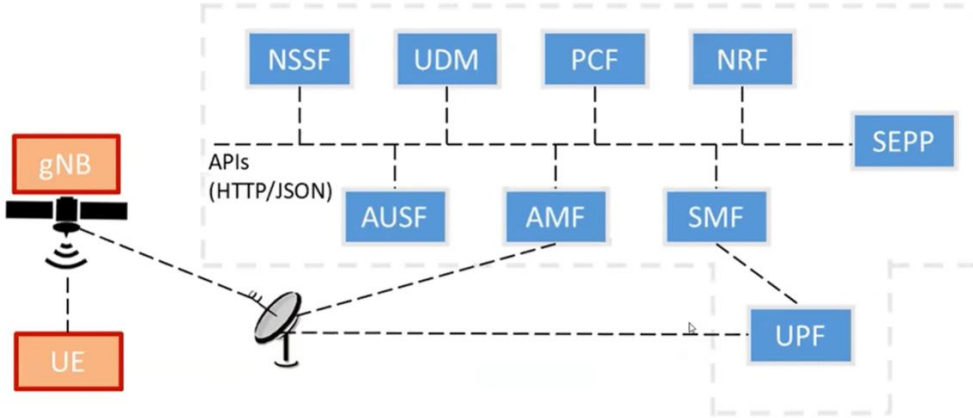
your input is welcome !

NTN and TN

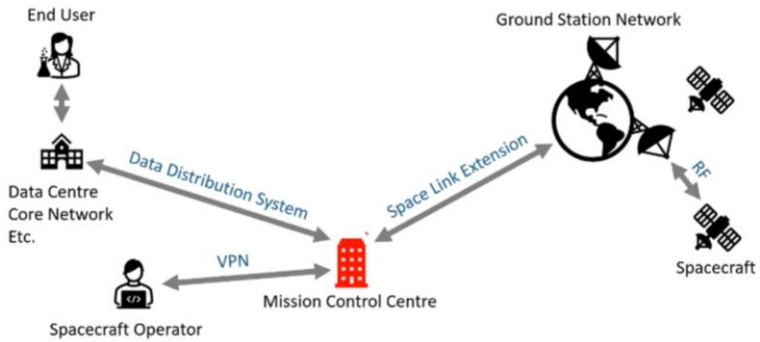
Real-world threat vectors across space and ground segments

TN and NTN have very different conditions

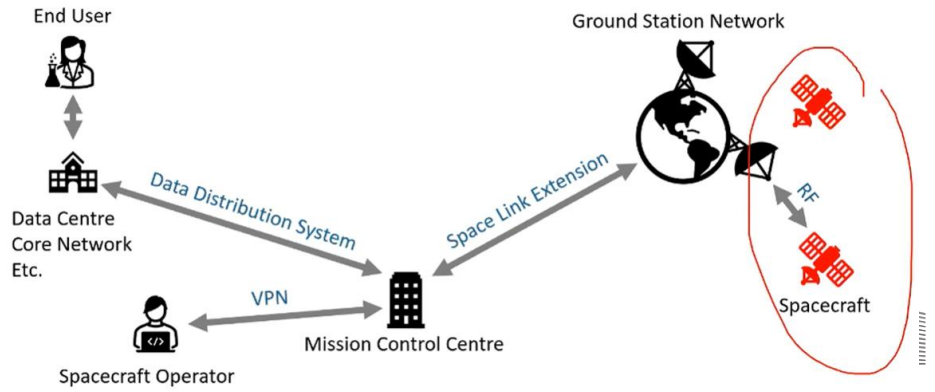
Multiple vulnerabilities that are TELCO-specific & Multiple vulnerabilities Space-specific



Mission control software



Onboard software



*Ideas welcome to support further the sector but input does not bind the Commission in any way

Other areas ?

2030 Complete migration for critical use cases
2035 Complete migration for all feasible Use Case

User Segment and Ground Segment are thus directly impacted by PQC transition !

Satellite-based communication system

→ Traditionally: pre-shared keys, OTAR, ASIC cryptographic implementation

CCSDS SDLS protocol

→ per se is based on HMAC like primitives & inherently symmetric

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

Other missions …

not always possible to pinpoint where one infrastructure ends and another begins

*Ideas welcome but input does not bind the Commission in any way

The state of the PQC transition

The transition to post-quantum cryptography, metaphorically

Stefan-Lukas Gazdag[1](✉) and Sophia Grundner-Culemann[2](✉)

[1] genua GmbH, Kirchheim near Munich, Germany
stefan-lukas_gazdag@genua.de
[2] Ludwig-Maximilians-Universität, Munich, Germany
grundner-culemann@nm.ifi.lmu.de

Abstract. *Are we there yet? Are we there yet? No, kids, the road to quantum-safety is long and sturdy. But let me tell you a story:*
Once upon a time, science discovered a great threat to Cryptography World: The scalable quantum computer! Nobody had ever seen one, but everyone understood it would break the mechanisms used to secure Internet communication since times of yore (or the late 20th century, anyway). The greatest minds from all corners of the land were gathered to invent, implement, and test newer, stronger tools. They worked day and night, but alas, when smaller quantum computers already started to emerge, no end to their research was in sight. How could that be?
This paper provides a collection of carefully wrought, more or less creative and more or less consistent metaphors to explain to audiences at all expertise levels the manifold challenges researchers and practitioners face in the ongoing quest for post-quantum migration.

Fig. 1: The well captured current state of the transition to post-quantum cryptography. On the left one can see where we started, on the right one can clearly see where we are right now. Picture of Sisyphus by Titian via Wikimedia *Punishment_sisyph.jpg* in the public domain.

https://eprint.iacr.org/2024/1487.pdf

Thank you for your kind attention

cnect-c4@ec.europa.eu
fabiana.da-pieve@ec.europa.eu