Quantum Communication and Quantum Key Distribution activities within the GÉANT community

Piotr Rydlichowski

Poznań Supercomputing and Networking Center

Poznań, Poland

16.06.2022

Outline

- Quantum Technologies - background
- Quantum Manifesto, Quantum Flagship and Digital Europe programs
- Quantum Key Distribution and Quantum Cryptography background
- Quantum Key Distribution Technologies and NRENs, activities within GÉANT
- Examples of activities at NRENs
- Outline for future activities and current status of EuroQCI
- Existing projects
- Summary

Quantum Technologies - background

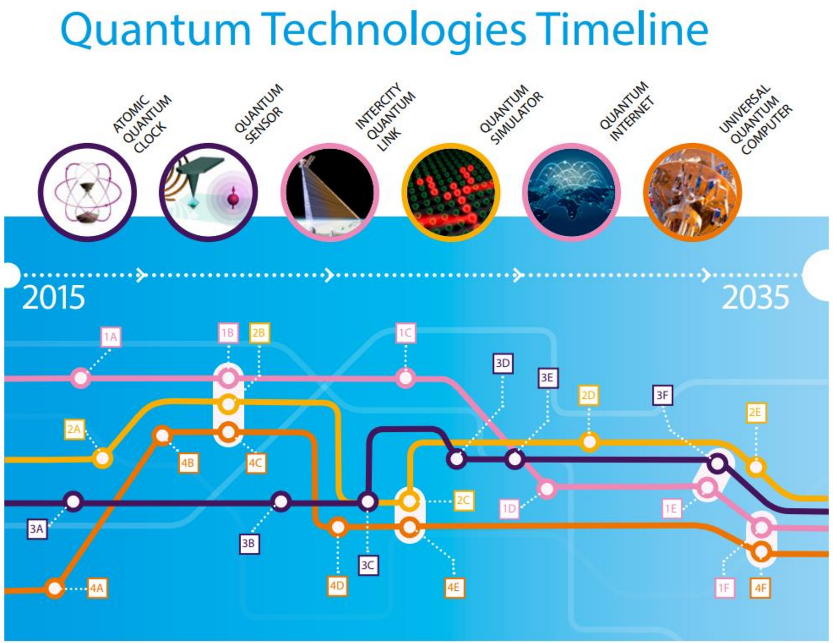
- **Allow for the manipulation and exploitation** of effects described by quantum mechanics.

- **We are currently in the process of 2nd quantum revolution** where quantum mechanics effects are used to enhance the capabilities of current measurement, simulation, computation and communication technologies.

- **„Quantum Manifesto” EU document released in 2016**. Recognizes importance of quantum area for Europe and drafts schedule for the research and real life applications. Foundation for future programs.

- **Since Quantum Manifesto many programs have been started** by the European Comission to support the topic: Quantum Flagship, SU-ICT-04-2019, Quantum Internet Alliance, activities in ESA, Quantum Communication Infratructure (QCI). **These will be followed under Digital Europe Program in 2021 – 2027.**

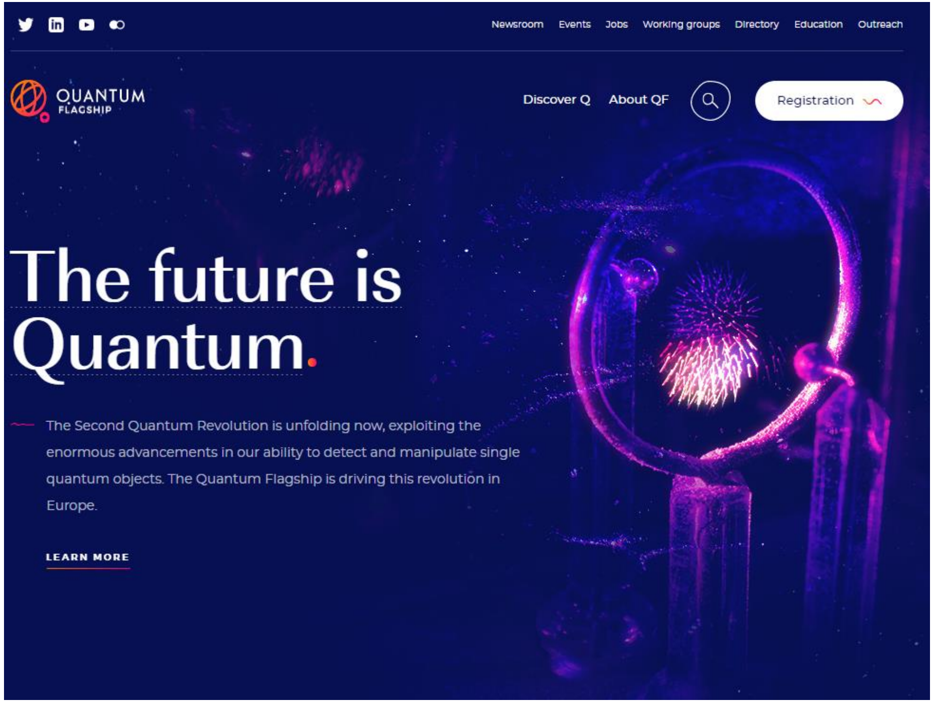
Quantum Manifesto, Quantum Flagship and Digital Europe Programs



	1. Communication	2. Simulators	3. Sensors	4. Computers
0 – 5 years	A Core technology of quantum repeaters B Secure point-to-point quantum links	A Simulator of motion of electrons in materials B New algorithms for quantum simulators and networks	A Quantum sensors for niche applications (incl. gravity and magnetic sensors for health care, geosurvey and security) B More precise atomic clocks for synchronisation of future smart networks, incl. energy grids	A Operation of a logical qubit protected by error correction or topologically B New algorithms for quantum computers C Small quantum processor executing technologically relevant algorithms
5 – 10 years	C Quantum networks between distant cities D Quantum credit cards	C Development and design of new complex materials D Versatile simulator of quantum magnetism and electricity	C Quantum sensors for larger volume applications including automotive, construction D Handheld quantum navigation devices	D Solving chemistry and materials science problems with special purpose quantum computer > 100 physical qubit
> 10 years	E Quantum repeaters with cryptography and eavesdropping detection F Secure Europe-wide internet merging quantum and classical communication	E Simulators of quantum dynamics and chemical reaction mechanisms to support drug design	E Gravity imaging devices based on gravity sensors F Integrate quantum sensors with consumer applications including mobile devices	E Integration of quantum circuit and cryogenic classical control hardware F General purpose quantum computers exceed computational power of classical computers

https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf

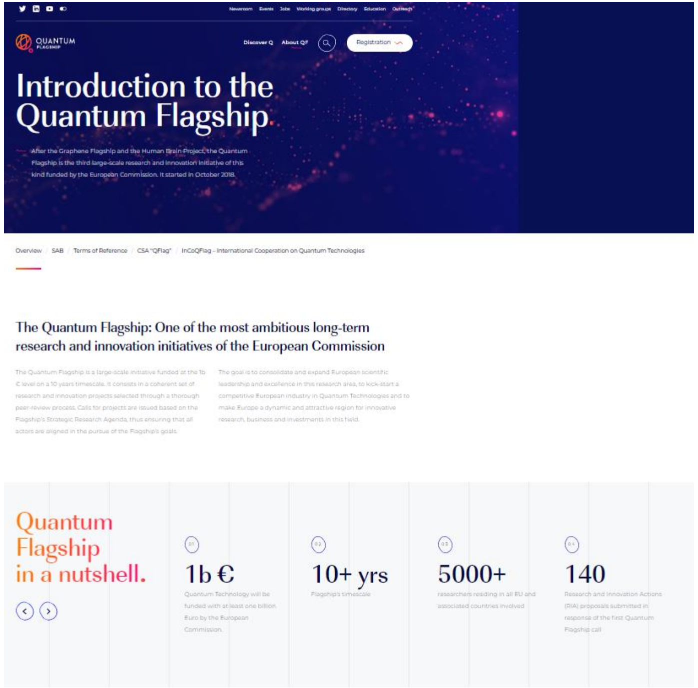
Quantum Manifesto, Quantum Flagship and Digital Europe Programs



The future is Quantum.

The Second Quantum Revolution is unfolding now, exploiting the enormous advancements in our ability to detect and manipulate single quantum objects. The Quantum Flagship is driving this revolution in Europe.

https://qt.eu/



Introduction to the Quantum Flagship.

After the Graphene Flagship and the Human Brain Project, the Quantum Flagship is the third large-scale research and innovation initiative of this kind funded by the European Commission. It started in October 2018.

The Quantum Flagship: One of the most ambitious long-term research and innovation initiatives of the European Commission

The Quantum Flagship is a large-scale initiative funded at the 1b € level on a 10 years timescale. It consists in a coherent set of research and innovation projects selected through a thorough peer-review process. Calls for projects are issued based on the Flagship's Strategic Research Agenda, thus ensuring that all actors are aligned in the pursue of the Flagship's goals.

The goal is to consolidate and expand European scientific leadership and excellence in this research area, to kick-start a competitive European industry in Quantum Technologies and to make Europe a dynamic and attractive region for innovative research, business and investments in this field.

Quantum Flagship in a nutshell.

1b €
Quantum Technology will be funded with at least one billion Euro by the European Commission.

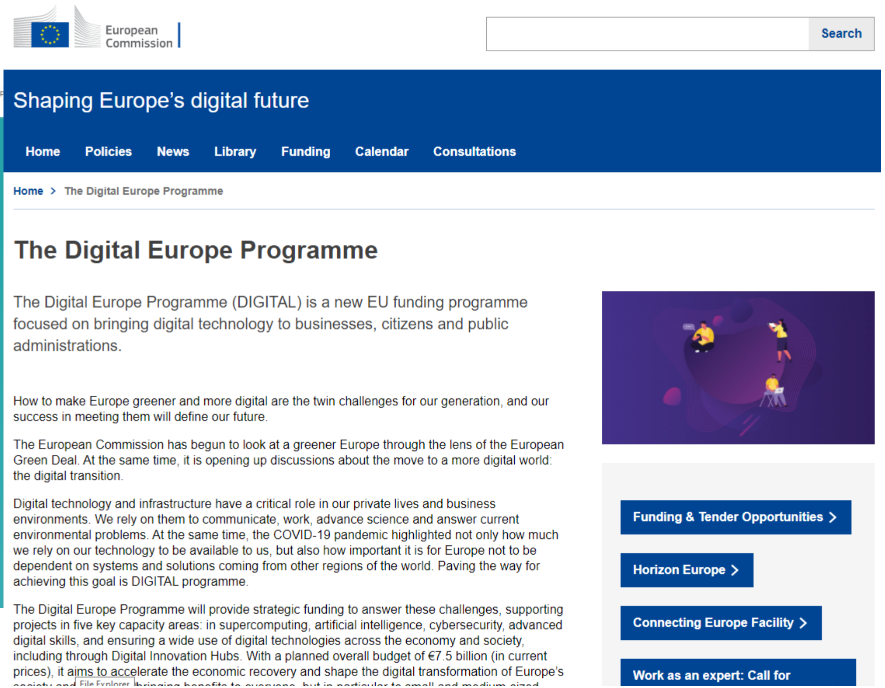
10+ yrs
Flagship's timescale

5000+
researchers residing in all EU and associated countries involved

140
Research and Innovation Actions (RIA) proposals submitted in response of the first Quantum Flagship call

Quantum Manifesto, Quantum Flagship and Digital Europe Programs

https://leading-the-digital-decade.eu/



European Commission

Search

Shaping Europe’s digital future

Home Policies News Library Funding Calendar Consultations

Home > The Digital Europe Programme

The Digital Europe Programme

The Digital Europe Programme (DIGITAL) is a new EU funding programme focused on bringing digital technology to businesses, citizens and public administrations.

How to make Europe greener and more digital are the twin challenges for our generation, and our success in meeting them will define our future.

The European Commission has begun to look at a greener Europe through the lens of the European Green Deal. At the same time, it is opening up discussions about the move to a more digital world: the digital transition.

Digital technology and infrastructure have a critical role in our private lives and business environments. We rely on them to communicate, work, advance science and answer current environmental problems. At the same time, the COVID-19 pandemic highlighted not only how much we rely on our technology to be available to us, but also how important it is for Europe not to be dependent on systems and solutions coming from other regions of the world. Paving the way for achieving this goal is DIGITAL programme.

The Digital Europe Programme will provide strategic funding to answer these challenges, supporting projects in five key capacity areas: in supercomputing, artificial intelligence, cybersecurity, advanced digital skills, and ensuring a wide use of digital technologies across the economy and society, including through Digital Innovation Hubs. With a planned overall budget of €7.5 billion (in current prices), it aims to accelerate the economic recovery and shape the digital transformation of Europe’s society and File Explorer bringing benefits to everyone, but in particular to small and medium-sized

Funding & Tender Opportunities >

Horizon Europe >

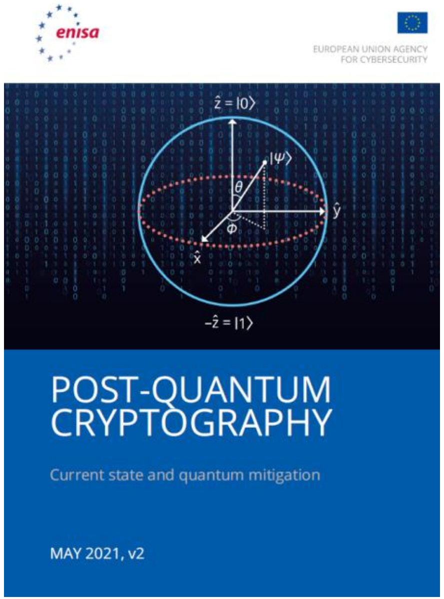
Connecting Europe Facility >

Work as an expert: Call for

https://digital-strategy.ec.europa.eu/en/activities/digital-programme

Quantum Key Distribution and quantum cryptography background

- Quantum computing infrastructure can potentially disrupt existing encryption mechanism
- Store and decrypt later problem
- Post Quantum Encryption Algorithms complement the QKD technology



enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

POST-QUANTUM
CRYPTOGRAPHY

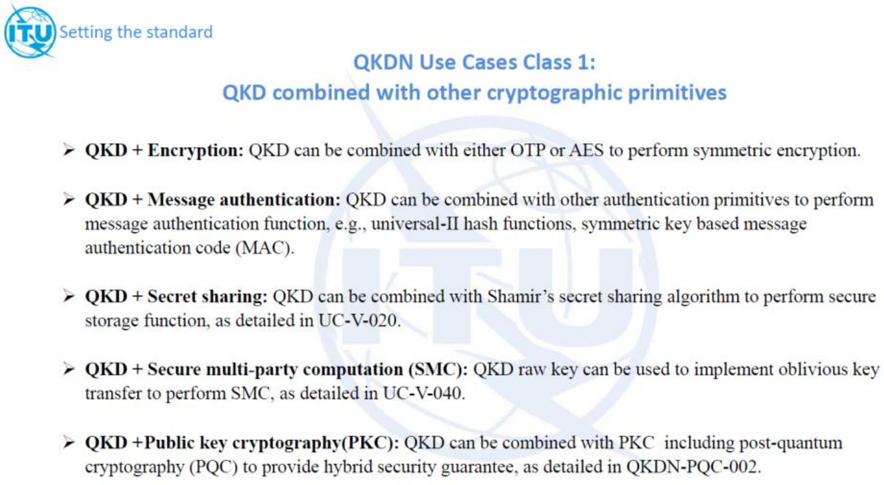
Current state and quantum mitigation

MAY 2021, v2

https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation/at_download/fullReport

Quantum Key Distribution and quantum cryptography background

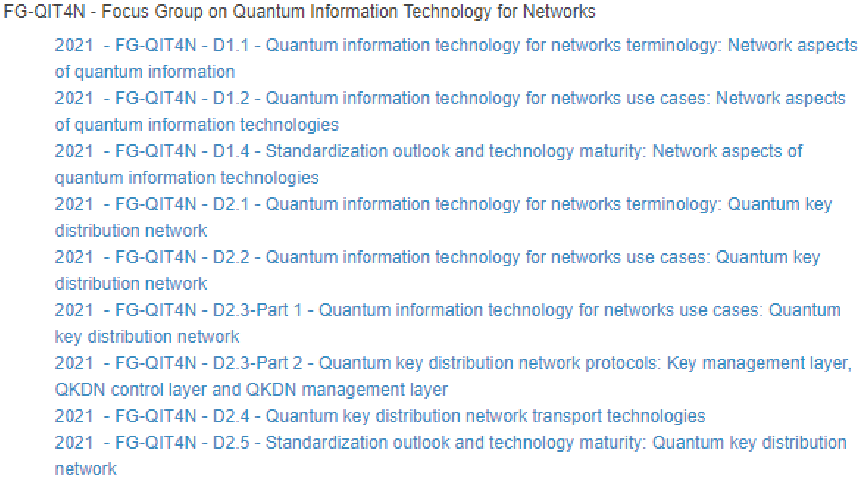
- ITU-T formed FG-QIT4N Focus Group to work on the QKD Use Cases - 6 different classes. New documents published February 2022.



Setting the standard

QKDN Use Cases Class 1:
QKD combined with other cryptographic primitives

- **QKD + Encryption:** QKD can be combined with either OTP or AES to perform symmetric encryption.
- **QKD + Message authentication:** QKD can be combined with other authentication primitives to perform message authentication function, e.g., universal-II hash functions, symmetric key based message authentication code (MAC).
- **QKD + Secret sharing:** QKD can be combined with Shamir's secret sharing algorithm to perform secure storage function, as detailed in UC-V-020.
- **QKD + Secure multi-party computation (SMC):** QKD raw key can be used to implement oblivious key transfer to perform SMC, as detailed in UC-V-040.
- **QKD +Public key cryptography(PKC):** QKD can be combined with PKC including post-quantum cryptography (PQC) to provide hybrid security guarantee, as detailed in QKDN-PQC-002.



FG-QIT4N - Focus Group on Quantum Information Technology for Networks

2021 - FG-QIT4N - D1.1 - Quantum information technology for networks terminology: Network aspects of quantum information

2021 - FG-QIT4N - D1.2 - Quantum information technology for networks use cases: Network aspects of quantum information technologies

2021 - FG-QIT4N - D1.4 - Standardization outlook and technology maturity: Network aspects of quantum information technologies

2021 - FG-QIT4N - D2.1 - Quantum information technology for networks terminology: Quantum key distribution network

2021 - FG-QIT4N - D2.2 - Quantum information technology for networks use cases: Quantum key distribution network

2021 - FG-QIT4N - D2.3-Part 1 - Quantum information technology for networks use cases: Quantum key distribution network

2021 - FG-QIT4N - D2.3-Part 2 - Quantum key distribution network protocols: Key management layer, QKDN control layer and QKDN management layer

2021 - FG-QIT4N - D2.4 - Quantum key distribution network transport technologies

2021 - FG-QIT4N - D2.5 - Standardization outlook and technology maturity: Quantum key distribution network

Quantum Key Distribution Technologies and NRENs

- From the NREN point of view the interesting aspects of quantum technologies and projects are:
  - Quantum Communication
  - Quantum Metrology in view of the T&F signals transmission and activities, it requires R&D
  - **Quantum Communication and Networks and its coexistance with existing networks in principle**
  - **Quantum Computing and its integration with quantum communication and classical HPC services**

- These areas are advanced in terms of development and real life application possibilites. Quantum computing and associated simulation still require substantial development.

- Quantum communication is a base for the **Quantum Internet Concept. Quantum Internet Proposed Research Group (QIRG) and Quantum Internet Alliance (QIA) have been launched** and discuss about standardisation.

- **Quantum Key Distribution (QKD)** can be regarded as example of quantum communication and step toward more advanced quantum transmission schemes. **QKD can be used for more than only encryption keys.**

Quantum Key Distribution Technologies and NRENs, activities within GÉANT

- **Within the GN4-3 project, WP6 T1** activities have been formed and ongoing to support and follow QKD and quantum technologies advancements and its possible application in GÉANT, NRENs networks.

- **It directly involves GÉANT and NREN community in the QKD technology development validation and contacts with QKD vendors**. GÉANT/NRENs have potential capabilities and infrastructure to establish QKD distributed testbeds in MAN networks (fibers and equipment) and moreover this community already provides wide set of services that rely on cryptography. Focus on training and education.

- **GÉANT/NRENs infrastructure and experience have potential elements** to also establish and validate QKD technology in the current generation data transmission networks and services.

- **GÉANT Quantum Strategy Group has been formed.**

Quantum Key Distribution Technologies and NRENs, activities within GÉANT

The QKD theory and technologies was explored further on GÉANT recent infoshares:

- GÉANT Infoshare: Quantum Technologies - Principles, Challenges and Applications - https://events.geant.org/event/353/

- GÉANT Infoshare: Quantum Key Distribution - Practical Implementations, Challenges, R&E Use Cases and Standardisation outlook –

  https://events.geant.org/event/453/

- GÉANT Infoshare: Quantum Key Distribution (QKD) Simulation

  https://events.geant.org/event/991/

- GÉANT Infoshare: Quantum Key Distribution (QKD) Physical implementation and testbed

  https://events.geant.org/event/1006/

Quantum Key Distribution Technologies and NRENs, activities within GÉANT

- **GÉANT and selected NRENs already established small or large testbeds in different places and using different QKD and networking technologies** to validate and the results can be a subject of essential comparison that can help to decide the direction of further QKD technology development and improvement especially in the area of standardization and certification.

- It is important to note that in order to full establish and validate the QKD technology and its testbed it is essential to further **extend cooperation between GÉANT/NREN community and commercial partners and new startups that already develop the QKD equipment and have significant experience with it**.

- The added value of this cooperation is that the GÉANT/NREN community can provide the commercial partners with large, advanced networking testbed and all required use cases (existing and future) especially in the view of QCI program.

Quantum Key Distribution Technologies and NRENs, possibilities within GÉANT

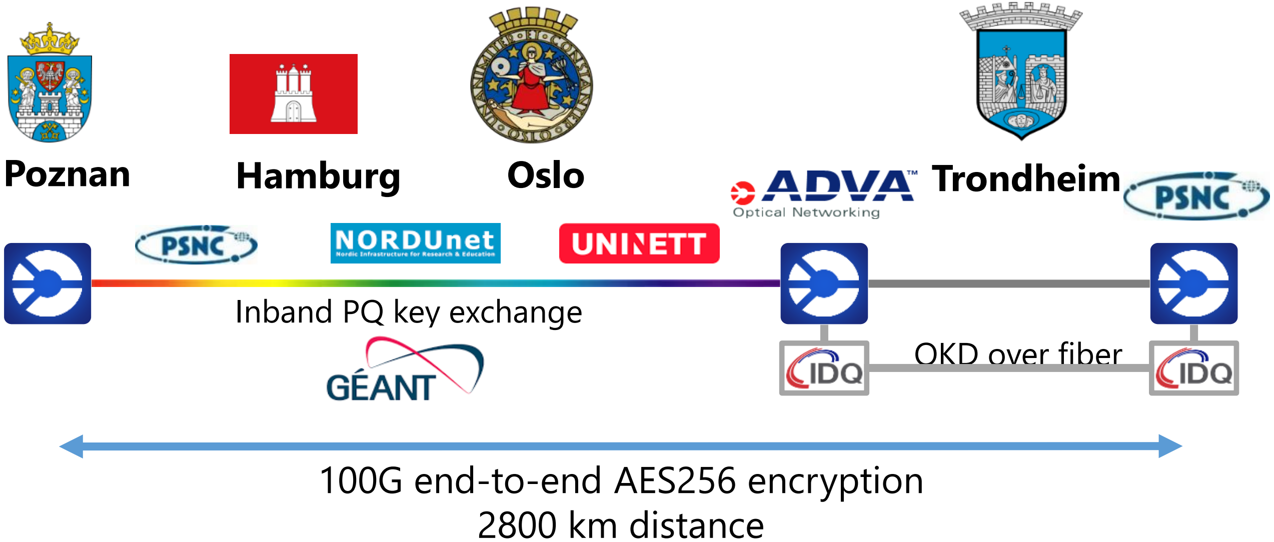
- GÉANT/NREN community together with the commercial partners have potential conditions, infrastructures and experience to establish and develop the QKD technology and connected with this services and technologies. **The testbeds, results and developed solutions can be used by both partners - GÉANT/NREN community and commercial institutions to further strengthen its own services and technologies.**

- GN4-3 WP6 T1 activities are focused to expoit above mentioned aspects. It is planned to extend **close cooperation with GÉANT/NREN T&F community**.

Examples of activities at NRENs

Selected NRENs have undertaken activities in the Quantum communication area, an example of such projects are TNC18, TNC21 presentation and demos, QIA, OPENQKD, QUAPITAL and EuroQCI.

Post Quantum and QKD algorithms demo - TNC18 conference https://tnc18.geant.org/core/event/96.html



Examples of activities at NRENs

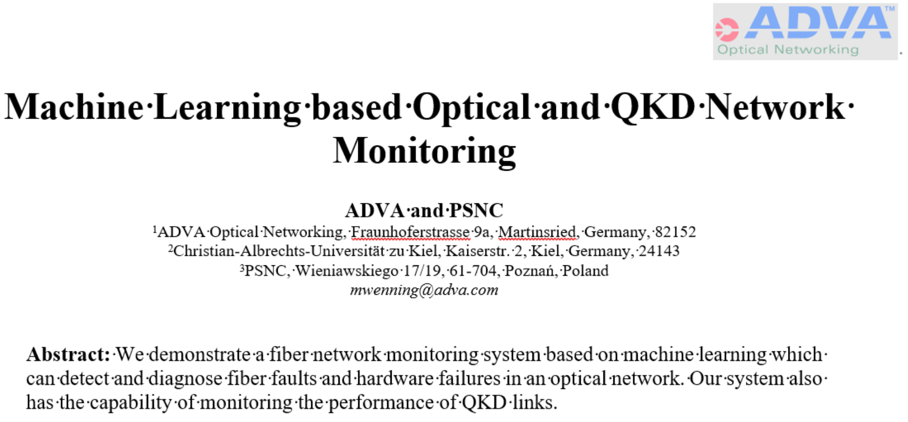
Live Demo at TNC21 and TNC22 conference – PSNC booth

KMS for Multi-vendor Interoperable QKDN

TNC 2021 Demo

ADVA, PSNC and IDQ

https://tnc21.geant.org/demonstrations/#c562



Machine Learning based Optical and QKD Network Monitoring

ADVA and PSNC

[1]ADVA Optical Networking, Fraunhoferstrasse 9a, Martinsried, Germany, 82152
[2]Christian-Albrechts-Universität zu Kiel, Kaiserstr. 2, Kiel, Germany, 24143
[3]PSNC, Wieniawskiego 17/19, 61-704, Poznań, Poland
mwenning@adva.com

Abstract: We demonstrate a fiber network monitoring system based on machine learning which can detect and diagnose fiber faults and hardware failures in an optical network. Our system also has the capability of monitoring the performance of QKD links.

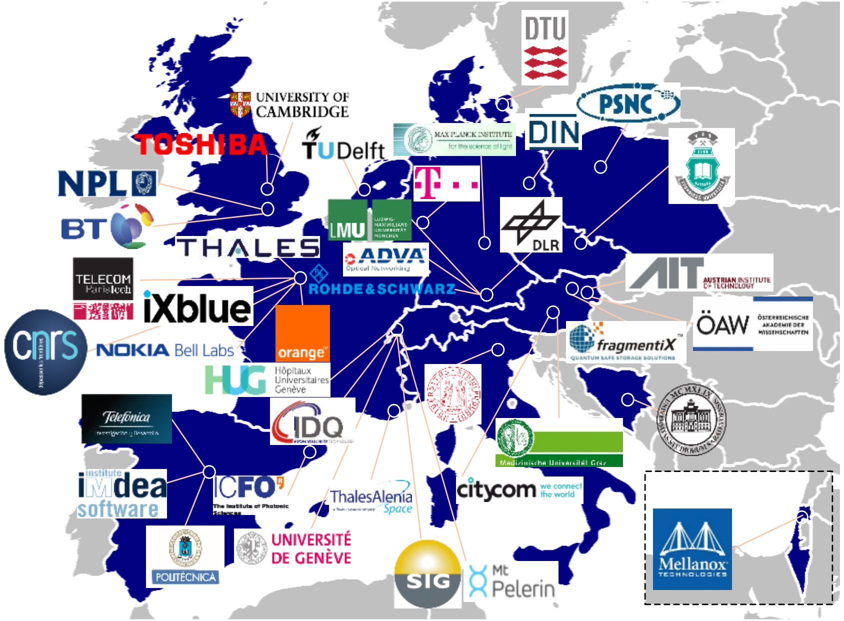
Examples of activities at NRENs

OPENQKD project

- Austrian Institute of Technology coordinator, PSNC partner
- The planned start date for works is October 2019, 3 years.
- PSNC is one of the main testbeds for new QKD solutions.
- Implementation of several scenarios and applications using QKD technology.
- Development of software for testbed management and performance monitoring, integration with existing transmission infrastructure.
- Participation in the work related to the preparation of the concept of implementing QKD technology into scientific and operational networks.
- Discussion on solutions integrating the transmission of DWDM system signals, quantum channels and time / frequency reference signals.
- Promotion of the project and its results.

Examples of activities at NRENs

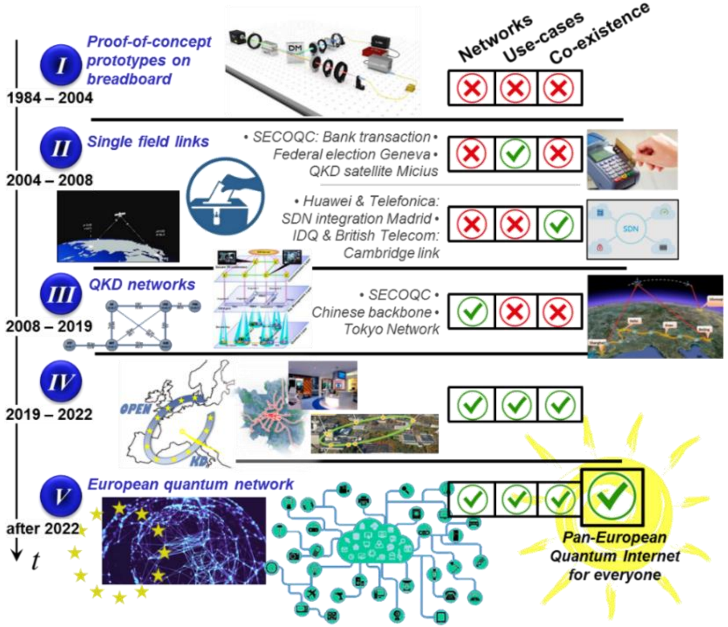
- OPENQKD Consortium

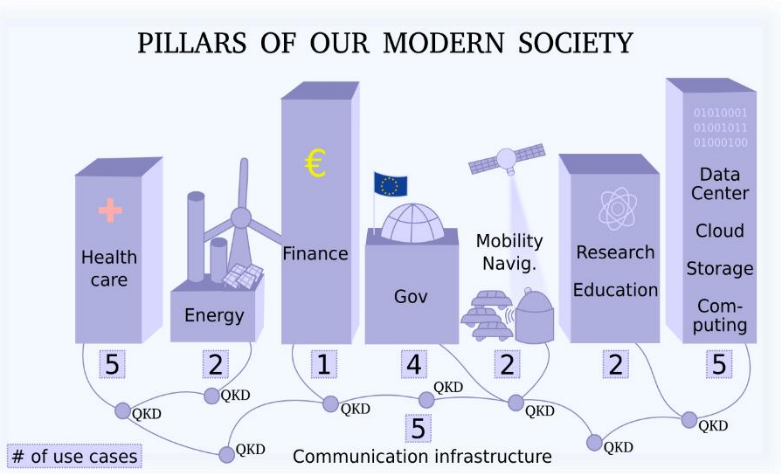


UNIVERSITY OF CAMBRIDGE
TOSHIBA
TU Delft
NPL
BT
THALES
TELECOM ParisTech
iXblue
cnrs
NOKIA Bell Labs
orange
HUG Hôpitaux Universitaires Genève
Telefónica
IDQ
imdea software
ICFO The Institute of Photonic Sciences
POLITÉCNICA
UNIVERSITÉ DE GENÈVE
ThalesAlenia Space
SIG
Mt Pelerin
citycom we connect the world
Medizinische Universität Graz
LMU
ADVA Optical Networking
ROHDE&SCHWARZ
MAX PLANCK INSTITUTE for the science of light
T
DLR
DTU
DIN
PSNC
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
ÖAW ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN
fragmentiX QUANTUM SAFE STORAGE SOLUTIONS
Mellanox TECHNOLOGIES

Examples of activities at NRENs

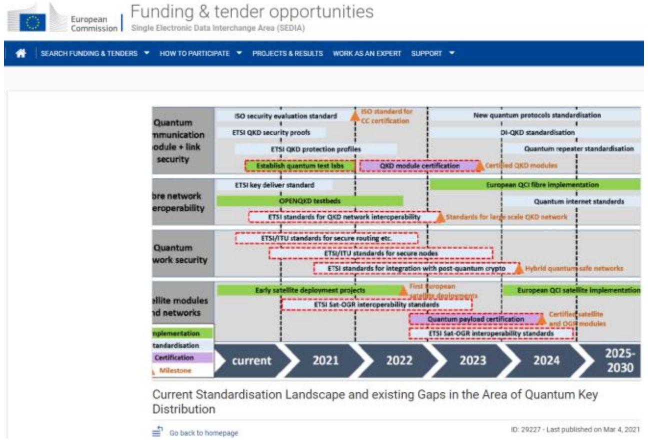
OpenQKD assumptions





Examples of activities at NRENs

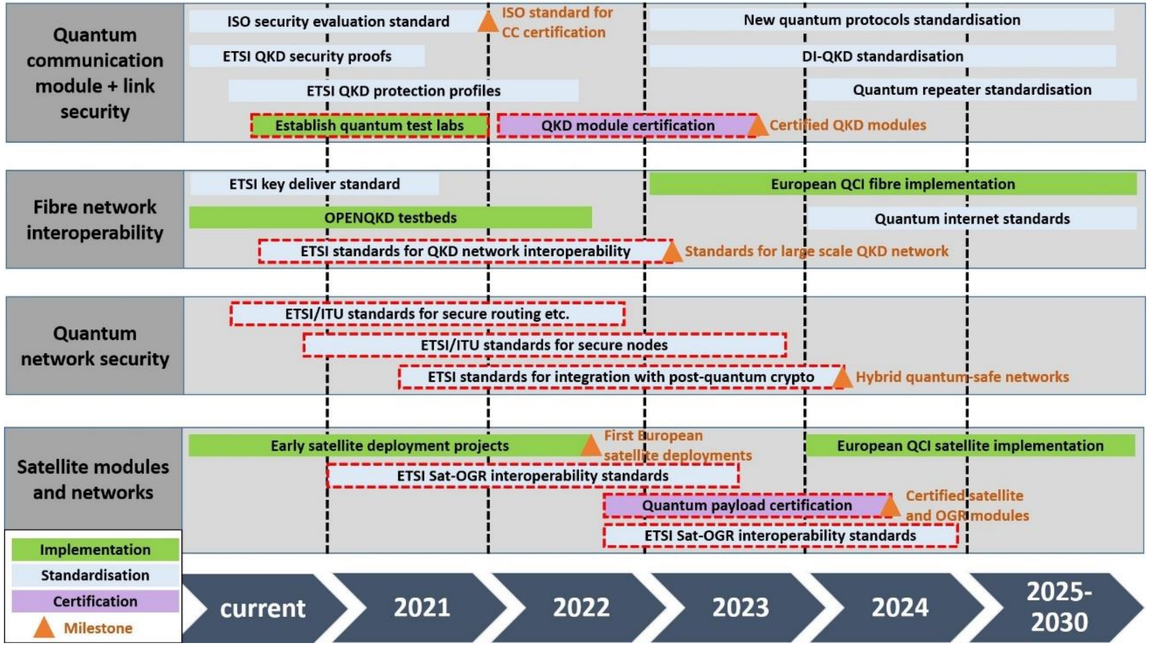
Standardization Outlook



Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution

Go back to homepage

ID: 29227 - Last published on Mar 4, 2021



Quantum communication module + link security

- ISO security evaluation standard
- ISO standard for CC certification
- New quantum protocols standardisation
- ETSI QKD security proofs
- DI-QKD standardisation
- ETSI QKD protection profiles
- Quantum repeater standardisation
- Establish quantum test labs
- QKD module certification
- Certified QKD modules

Fibre network interoperability

- ETSI key deliver standard
- European QCI fibre implementation
- OPENQKD testbeds
- Quantum internet standards
- ETSI standards for QKD network interoperability
- Standards for large scale QKD network

Quantum network security

- ETSI/ITU standards for secure routing etc.
- ETSI/ITU standards for secure nodes
- ETSI standards for integration with post-quantum crypto
- Hybrid quantum-safe networks

Satellite modules and networks

- Early satellite deployment projects
- First European satellite deployments
- European QCI satellite implementation
- ETSI Sat-OGR interoperability standards
- Quantum payload certification
- Certified satellite and OGR modules
- ETSI Sat-OGR interoperability standards

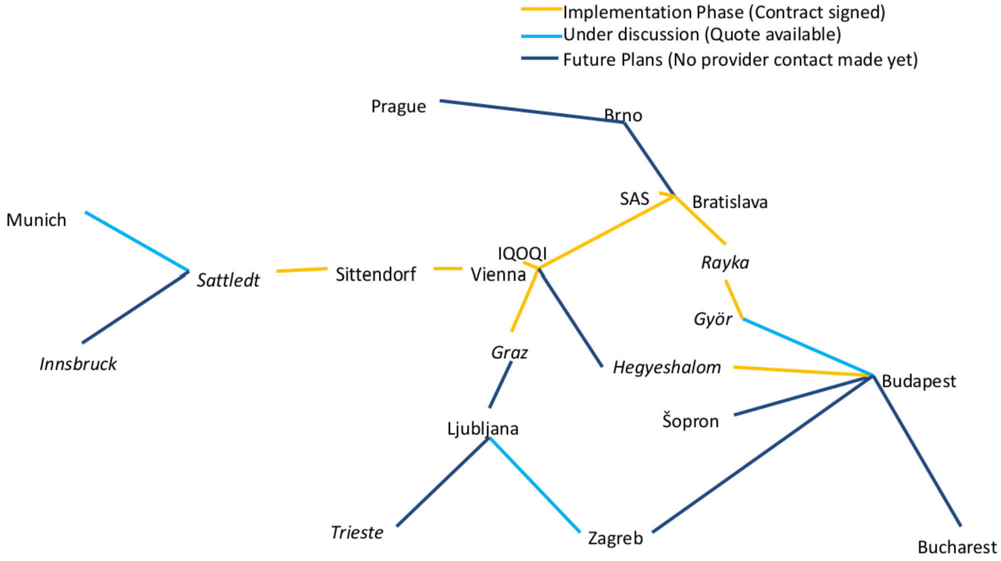
Implementation
Standardisation
Certification
Milestone

current → 2021 → 2022 → 2023 → 2024 → 2025-2030

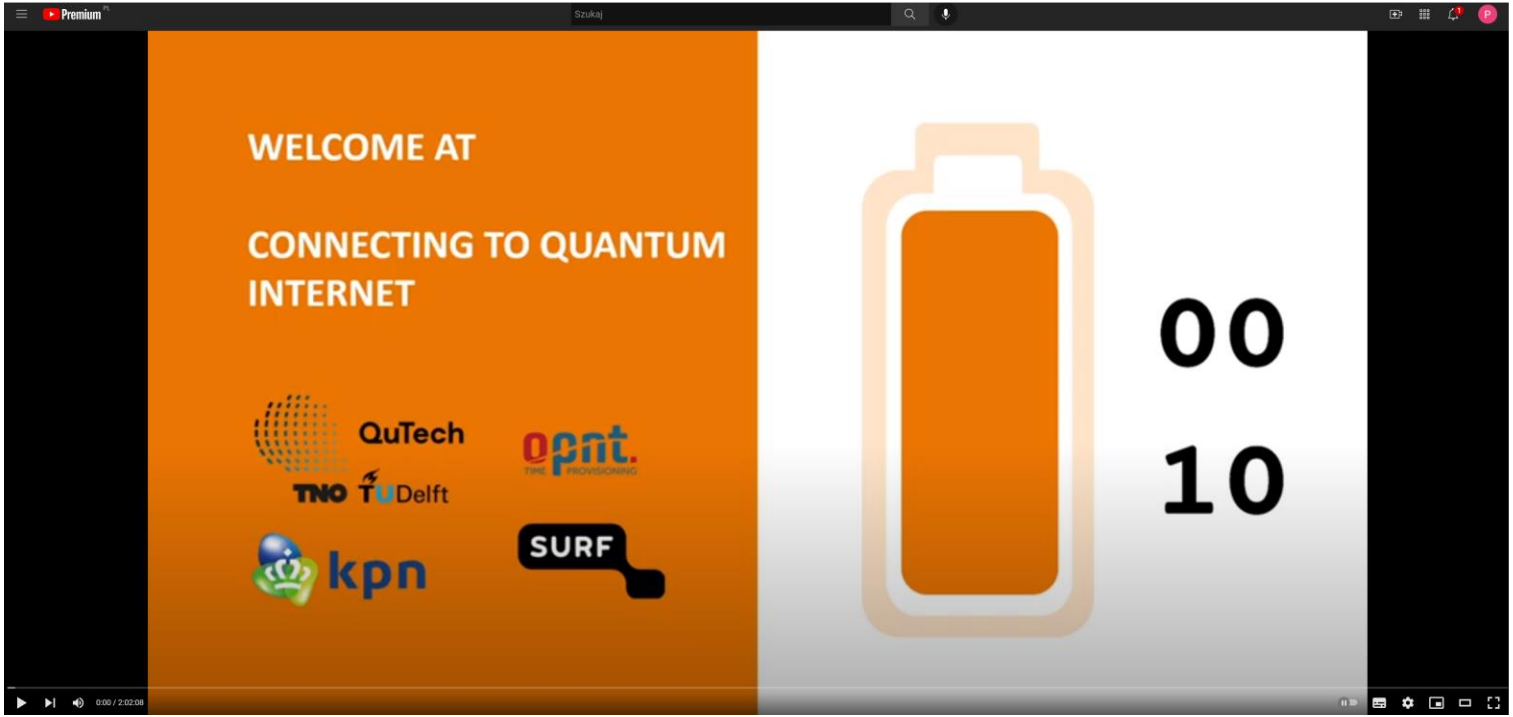
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform/29227

Examples of activities at NRENs

- QUAntum Photonic Intercity TrAnsmission Lattice (QUAPITAL) - https://quapital.eu/
- Driven by IQOQI Vienna, Austria.
- Not supported by any project.
- Step towards quantum internet
- Using existing fibre infrastructure.



Examples of activities at NRENs



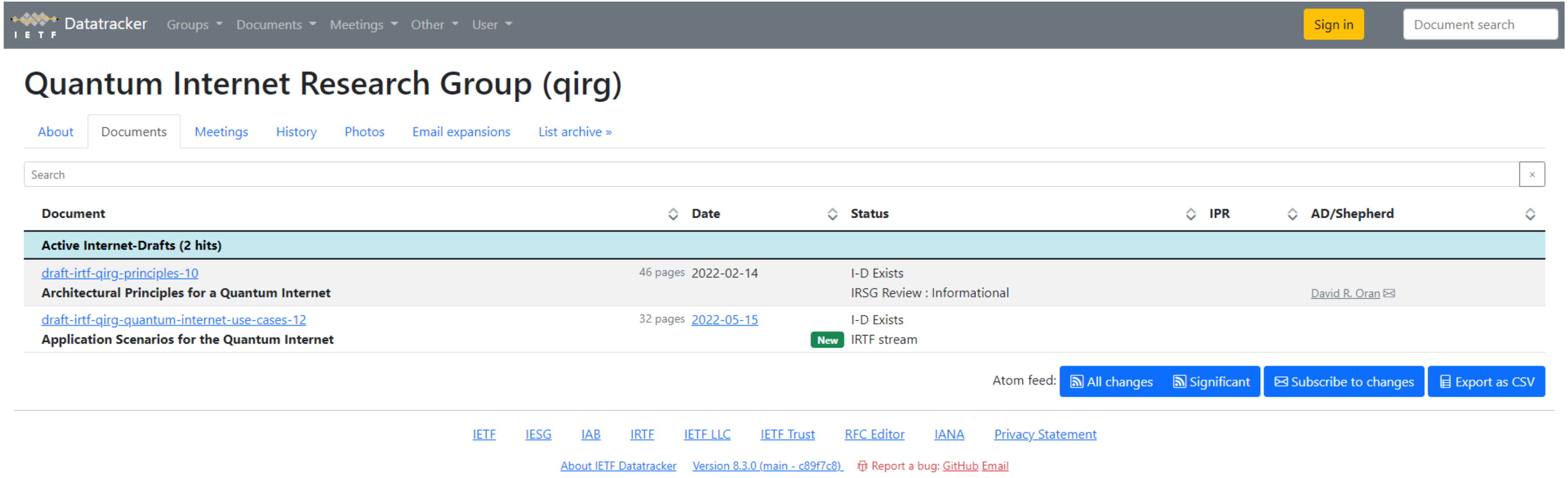
WELCOME AT

CONNECTING TO QUANTUM INTERNET

SURF webinar – „Connecting to Quantum Internet” 15th June 2021

Examples of activities at NRENs

- Input for QIRG activities



Quantum Internet Research Group (qirg)

Document		Date		Status	IPR	AD/Shepherd
Active Internet-Drafts (2 hits)						
draft-irtf-qirg-principles-10 **Architectural Principles for a Quantum Internet**	46 pages	2022-02-14		I-D Exists IRSG Review : Informational		David R. Oran ✉
draft-irtf-qirg-quantum-internet-use-cases-12 **Application Scenarios for the Quantum Internet**	32 pages	2022-05-15	New	I-D Exists IRTF stream		

https://datatracker.ietf.org/rg/qirg/documents/

Outline for future activities - EuroQCI

- The Digital Europe programme and Connecting Europe Facility will contribute to funding the EuroQCI.

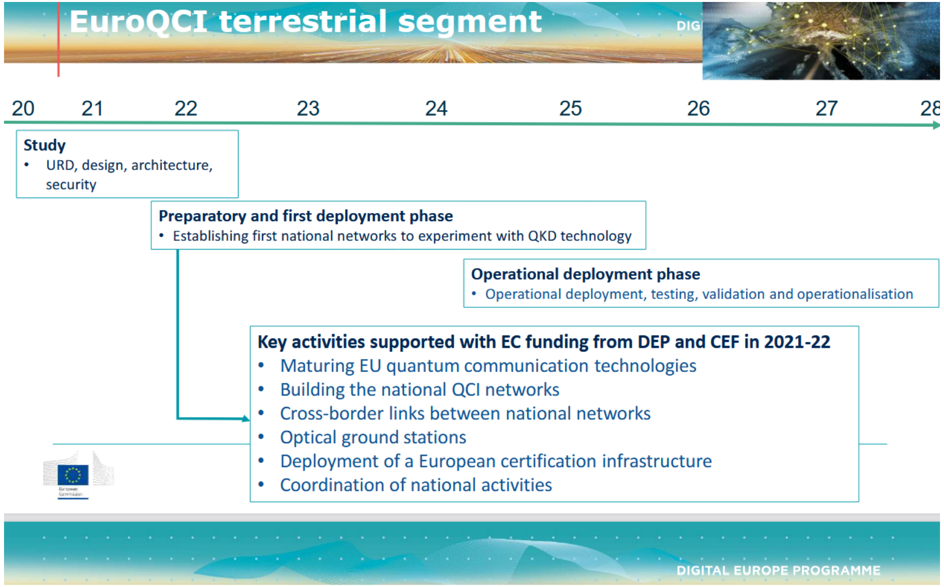
- There were two tenders in 2019 and 2020 to prepare studies for future QCI: **Assessing the user needs of a Quantum Communication Infrastructure, detailed system study for a quantum communication infrastructure.**

- QCI is funded by Member States and EC. Member States are required to prepare its own National QCI strategies and projects.

- Calls target national QCI activities, Cross-border connections and equipment development, suport for startups.

Outline for future activities - EuroQCI

- NRENs and GÉANT involved in **all** QCI calls in March 2022:



EuroQCI terrestrial segment

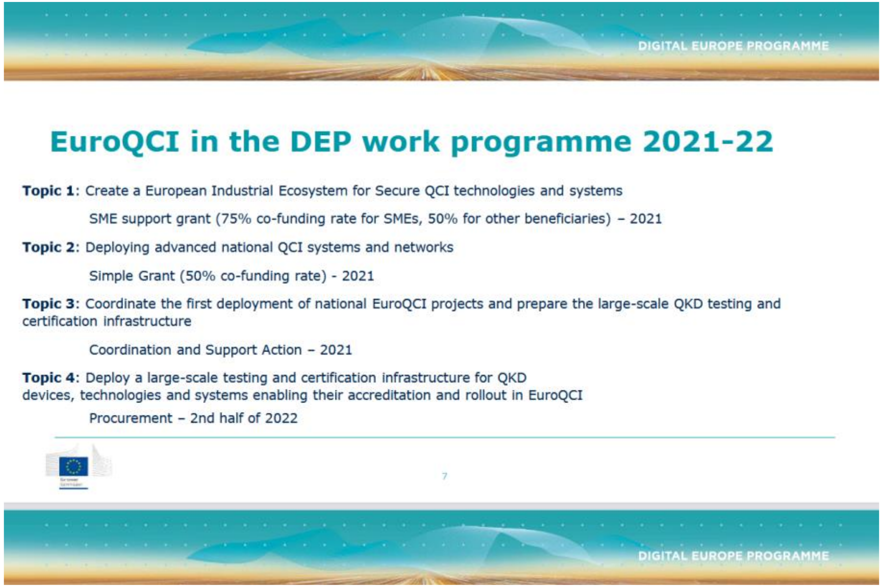
Study
- URD, design, architecture, security

Preparatory and first deployment phase
- Establishing first national networks to experiment with QKD technology

Operational deployment phase
- Operational deployment, testing, validation and operationalisation

Key activities supported with EC funding from DEP and CEF in 2021-22
- Maturing EU quantum communication technologies
- Building the national QCI networks
- Cross-border links between national networks
- Optical ground stations
- Deployment of a European certification infrastructure
- Coordination of national activities

DIGITAL EUROPE PROGRAMME



DIGITAL EUROPE PROGRAMME

EuroQCI in the DEP work programme 2021-22

Topic 1: Create a European Industrial Ecosystem for Secure QCI technologies and systems

SME support grant (75% co-funding rate for SMEs, 50% for other beneficiaries) – 2021

Topic 2: Deploying advanced national QCI systems and networks

Simple Grant (50% co-funding rate) - 2021

Topic 3: Coordinate the first deployment of national EuroQCI projects and prepare the large-scale QKD testing and certification infrastructure

Coordination and Support Action – 2021

Topic 4: Deploy a large-scale testing and certification infrastructure for QKD devices, technologies and systems enabling their accreditation and rollout in EuroQCI

Procurement – 2nd half of 2022

7

DIGITAL EUROPE PROGRAMME

Existing Projects

- European countries started national development initiatives for quantum technologies
- They complement the Quantum Flagship initiative
- The study of National Programs has been included in the GEANT white paper „Quantum Technologies Status Overview” **https://about.geant.org/wp-content/uploads/2021/12/GN4-3_White-Paper_Quantum-Technologies-Status-Overview.pdf**
- Countries:
  - Austria
  - Croatia
  - Czech Republic
  - France
  - Germany
  - The Netherlands
  - Poland
  - Switzerland
  - UK
  - …

Summary

- GN4-3 WP6 T1 group follow quantum communication technologies developments and advancements.
- GÉANT and NREN communities have the infrastructure, services and use cases to fully support Quantum communication development.
- Close cooperation established between QKD vendors, GÉANT and NRENs
- QKD and quantum communication testbeds, use cases within GÉANT and NRENs are beeing prepared and implemented.
- Close cooperation with Quantum Flagship projects.
- Announcement of results of existing QCI calls and involvement in next QCI calls – this and next year.

Thank you

Any Questions?

prydlich@man.poznan.pl

As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).