Update from WP6T1

Quantum Technologies

Susanne Naegele-Jackson, FAU/DFN

Task leader WP6T1

SIG-Quantum

01 December 2025

GÉANT 5 Phase 2:

- Work Package 6: Network Development
  - Task 1: Subtask: Quantum Technologies

Agenda

- KMS Pathfinder
- Whitepaper: Towards Quantum-Safe Networking
- Quantum Training
- Events

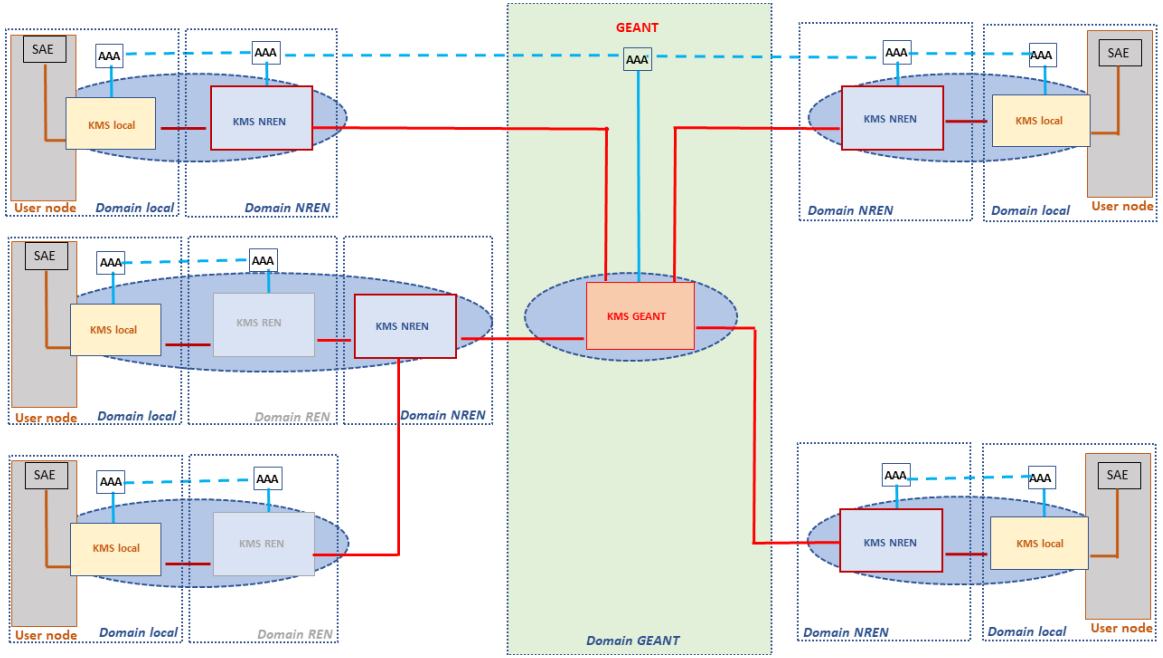
GN5-2: Work Package 6: Network Development

- **GN5-2: WP6 Network Development**
  - *Task 1: Technologies*
    - Fibre Sensing
    - Network Programmability
    - Quantum Technology

- Work in the NREN context around joint topics of interest
  - Explore technologies before they become deployment/production ready
  - Through pilots towards production services
  - For single or multi-domain deployment

KMS Pathfinder (I)

- Investigation of issues around QKD Key Management Service (KMS)
- Aims to explore
  - Creation, management, use of cryptographic keys
  - Requirements and possibilities for smooth and secure cross-domain quantum communication
  - Certificates and authentication
  - Monitoring and management issues



- Implementation involves locations in
  - Germany, Spain, Poland and Greece
  - With central KMS placed at GÉANT-based VM as needed for Quantum Key Distribution
  - Connected via IPSec tunnels (no Quantum links)

KMS Pathfinder (II)

- Three open source software-based KMS systems were evaluated
  - a KMS system developed by SURF
  - a KMS system developed by the University of the Basque Country (EHU)
  - a KMS system developed by the Hochschule Darmstadt in Germany
- The EHU and SURF packages were selected for future work in the pathfinder
- Currently
  - Still one domain, future investigations will also include multi-domain scenarios

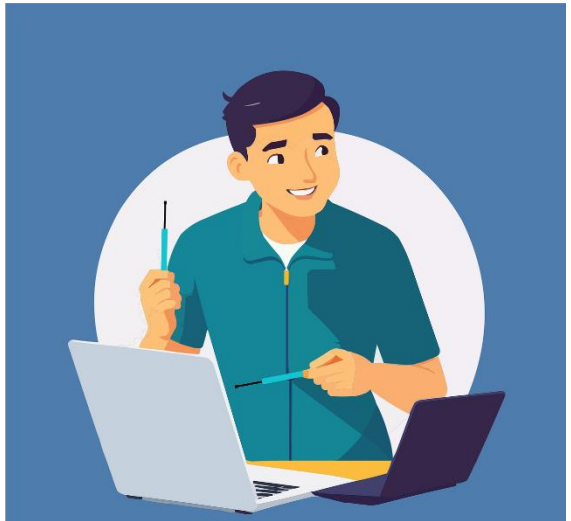


Image by Mohamed Hassan from Pixabay

Image by Tyli Jurafrom Pixabay

Whitepaper: Towards Quantum-Safe Networking (I)

- “Towards Quantum-Safe Networking“, https://zenodo.org/records/17506351
- step-by-step approach towards quantum-safe networks
  - Where Post Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) technology is applied and integrated over time
  - Goal is to harden networks and ensure quantum-safe security with the adoption of cryptographic methods that are resistant to attacks by quantum computers
  - Provides a series of recommendations for NRENs for the gradual implementation
    - When transitioning from pre-quantum cryptography to PQC
    - When integrating QKD and PQC into existing network infrastructures

Image by OpenClipart-Vectors from Pixabay

Encryption Algorithms

Classical cryptography distinguishes between:

- **Asymmetric-key algorithms** such as Elliptic Curve Cryptography (ECC) and Rivest–Shamir–Adleman (RSA) (which use two different keys – a public key and a private key – to encrypt and decrypt data); and
- **Symmetric-key algorithms** such as AES (where the same secret key is used to encrypt and decrypt a message)

➔ AES is still considered a quantum-resistant encryption standard, particularly AES-256

➔ RSA (based on difficulty of integer factorization), ECC and discrete logarithm-based algorithms (e.g. Diffie-Hellman) will be compromised

PQC algorithms are categorized into:

- Hash-based cryptography (algorithms such as SPHINCS+)
- Lattice-based cryptography (algorithms such as Kyber and Dilithium).
- Multivariate quadratic equations (MQE)-based cryptography) and algorithms such as classic McEliece

➔ By combining classical and PQC algorithms in hybrid approaches, compatibility can be ensured, and security can be provided against current threats while preparing against future vulnerabilities

Image by Pete Linforth from Pixabay

NIST/Federal Information Processing Standards (FIPS)

- National Institute of Standards and Technology (NIST), https://csrc.nist.gov/projects/post-quantum-cryptography

- August 2024: Secretary of Commerce approved three Federal Information Processing Standards (FIPS) for PQC:
  - **FIPS 203: primary standard for general encryption**
  - Standard based on the CRYSTALS-Kyber algorithm (Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)); small encryption keys for easy exchange between two parties.
  - HQC (fifth algorithm to be standardized in 2027) will become the backup algorithm for general encryption.
  - **FIPS 204: primary standard for protection of digital signatures**
  - Standard based on the CRYSTALS-Dilithium algorithm (Module-Lattice-Based Digital Signature Algorithm (ML-DSA)).
  - **FIPS 205: intended as backup method for digital signatures**
  - Standard that uses the Sphincs+ algorithm (Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)). Employs a different math approach from ML-DSA in case ML-DSA turns out to be vulnerable.
  - **FIPS 206: under development** – Built around the FALCON algorithm (FFT (Fast-Fourier Transform) over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA))

Expected Timelines (I)

- **It is expected to take several years**
  - to transition from quantum-vulnerable pre-quantum cryptography to quantum-resistant PQC algorithms
    - due to interoperability and security standards across different platforms
    - devices must be maintained
    - it will not be possible to transition all public-key cryptography in use in one instance

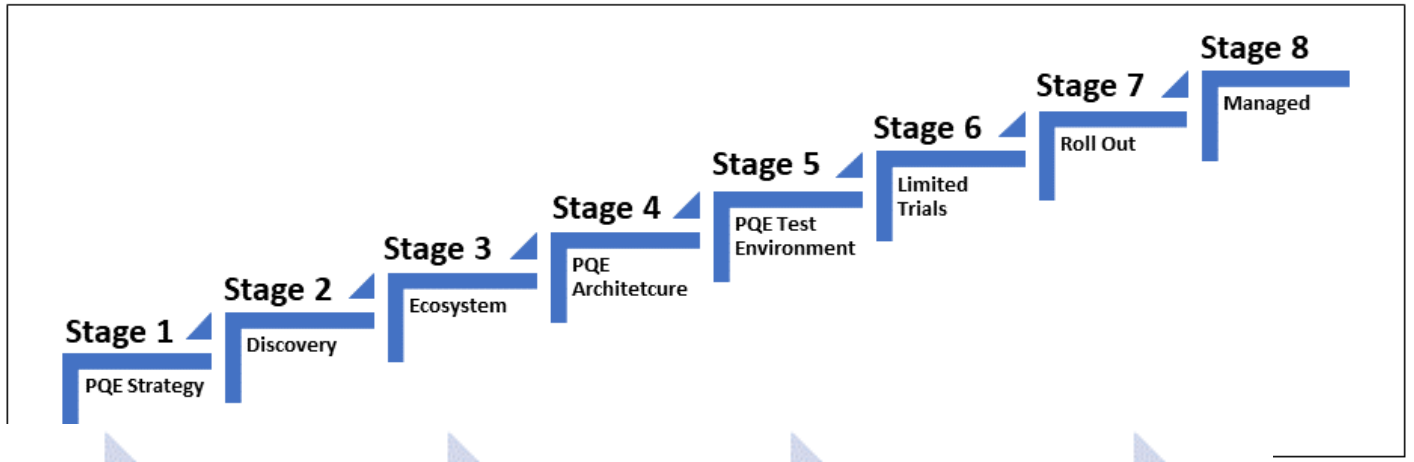
- A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (June 2025)
- Quantum Europe Strategy (July 2025)

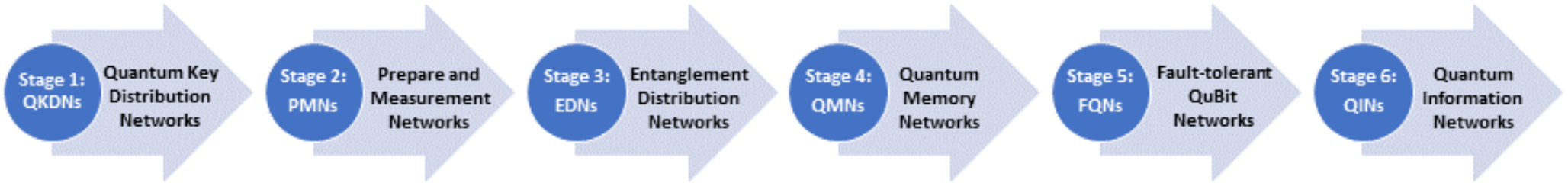
- **Where to start?**
  - Start out with standardized and tested hybrid solutions which include PQC to replace vulnerable public-key encryption methods such as RSA or discrete logarithm-based algorithms wherever applicable
  - Start deploying QKD infrastructure in pilot locations, focusing on high-value research applications, and gradually expand this network to cover more campus and research institution connections
  - Work on hybrid cryptography: combining classical encryption for routine traffic with QKD for high-priority or sensitive communication, ensuring that traditional networks can interoperate with quantum-safe techniques

Whitepaper: Towards Quantum-Safe Networking (VI)

- Maturity models
  - Maturity considerations for PQC
  - Maturity considerations for QKD

Levels	0: Initial / Not Possible	1: Possible	2: Prepared	3: Practiced	4: Sophisticated
Knowledge	N/A	System knowledge, cryptographic inventory	Algorithm IDs	Performance, awareness, security	
Process	N/A	Updateability, reversibility		Policies, testing, enforceability, transition mechanism, effectiveness	Automa scalabili real-tim
System property	N/A	Extensibility	Cryptographic modularity, algorithm intersection, algorithm exclusion,	Hardware modularity, backwards compatibility,	Context indepen interope

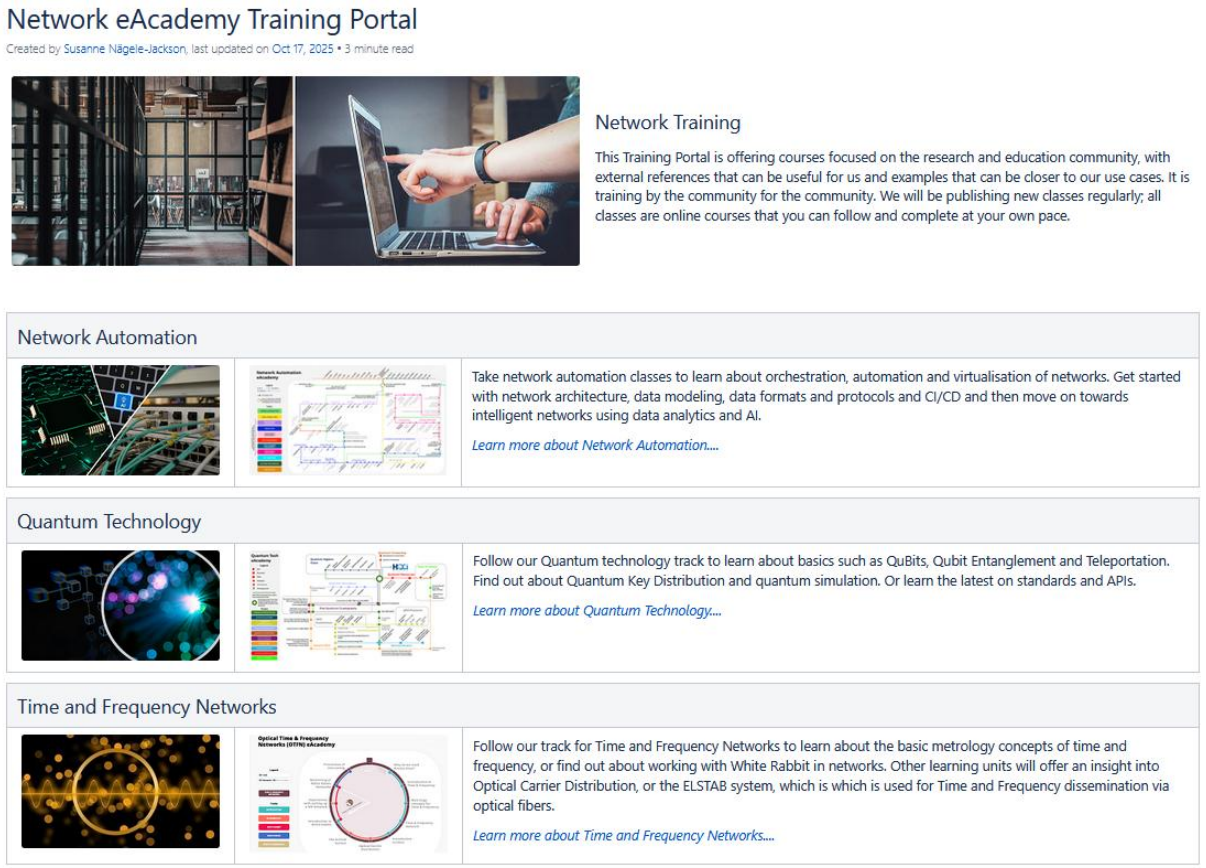




Quantum Training (I)

- WP6: Network eAcademy
  - Tracks on
    - Network Automation
    - Quantum Technology
    - Time and Frequency Networks
    - *Coming soon:* Artificial Intelligence

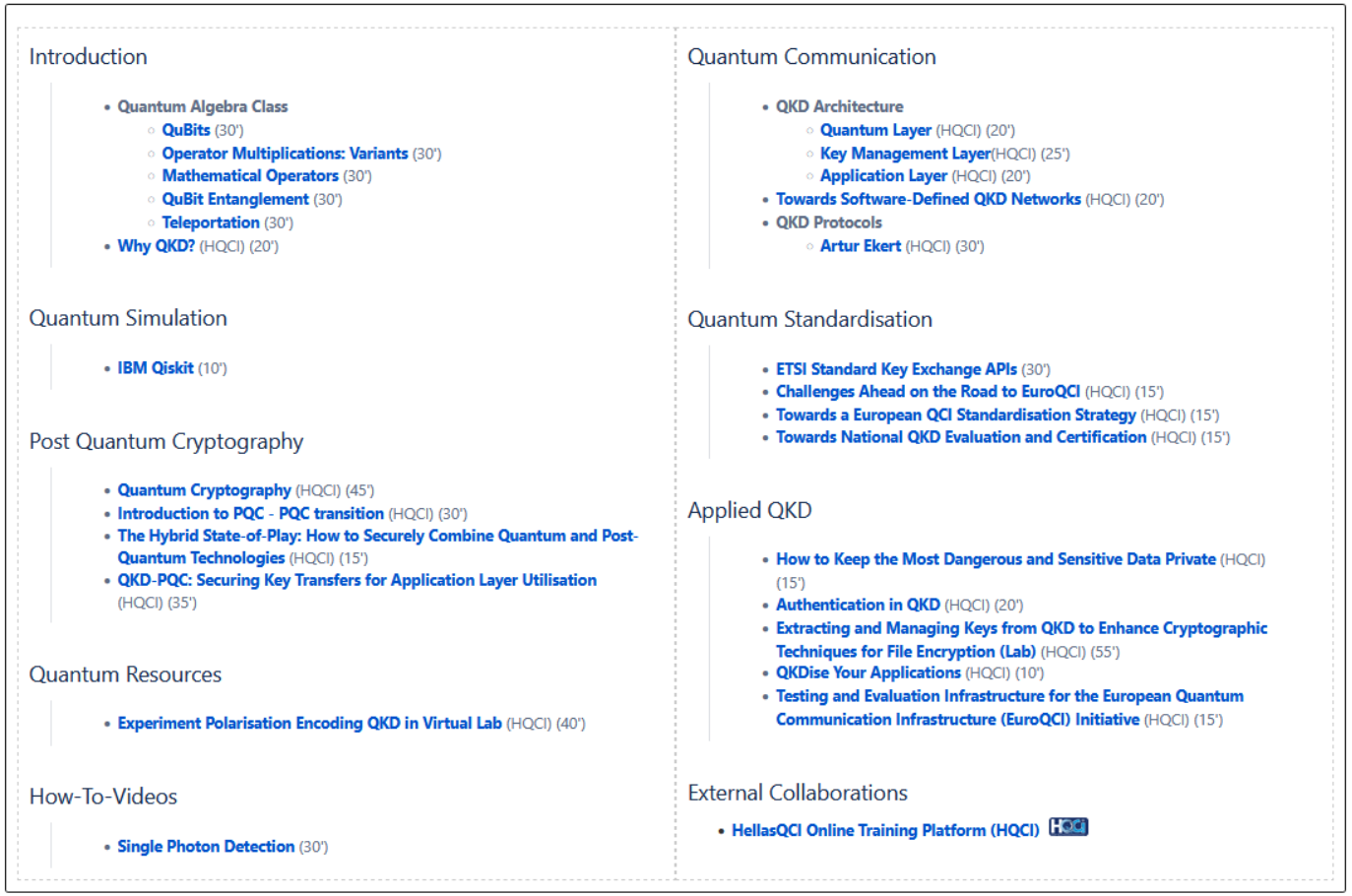
- Network eAcademy: Quantum Technology, https://wiki.geant.org/spaces/NETDEV/pages/870744159/Quantum+Technology+Training



Quantum Training (II)

New:

- external cooperation with
  - HellasQCI Online Training Platform (HQCI),
  - https://training.hellasqci.eu/
- Additional sections
  - Post Quantum Cryptography
  - Applied QKD
- new courses
  - Single Photon Detection (Hands-on-video)
  - Coming soon:
    - Introduction to QKD
    - Introduction to QKD Post Processing



Introduction

- Quantum Algebra Class
  - QuBits (30')
  - Operator Multiplications: Variants (30')
  - Mathematical Operators (30')
  - QuBit Entanglement (30')
  - Teleportation (30')
- Why QKD? (HQCI) (20')

Quantum Simulation

- IBM Qiskit (10')

Post Quantum Cryptography

- Quantum Cryptography (HQCI) (45')
- Introduction to PQC - PQC transition (HQCI) (30')
- The Hybrid State-of-Play: How to Securely Combine Quantum and Post-Quantum Technologies (HQCI) (15')
- QKD-PQC: Securing Key Transfers for Application Layer Utilisation (HQCI) (35')

Quantum Resources

- Experiment Polarisation Encoding QKD in Virtual Lab (HQCI) (40')

How-To-Videos

- Single Photon Detection (30')

Quantum Communication

- QKD Architecture
  - Quantum Layer (HQCI) (20')
  - Key Management Layer(HQCI) (25')
  - Application Layer (HQCI) (20')
- Towards Software-Defined QKD Networks (HQCI) (20')
- QKD Protocols
  - Artur Ekert (HQCI) (30')

Quantum Standardisation

- ETSI Standard Key Exchange APIs (30')
- Challenges Ahead on the Road to EuroQCI (HQCI) (15')
- Towards a European QCI Standardisation Strategy (HQCI) (15')
- Towards National QKD Evaluation and Certification (HQCI) (15')

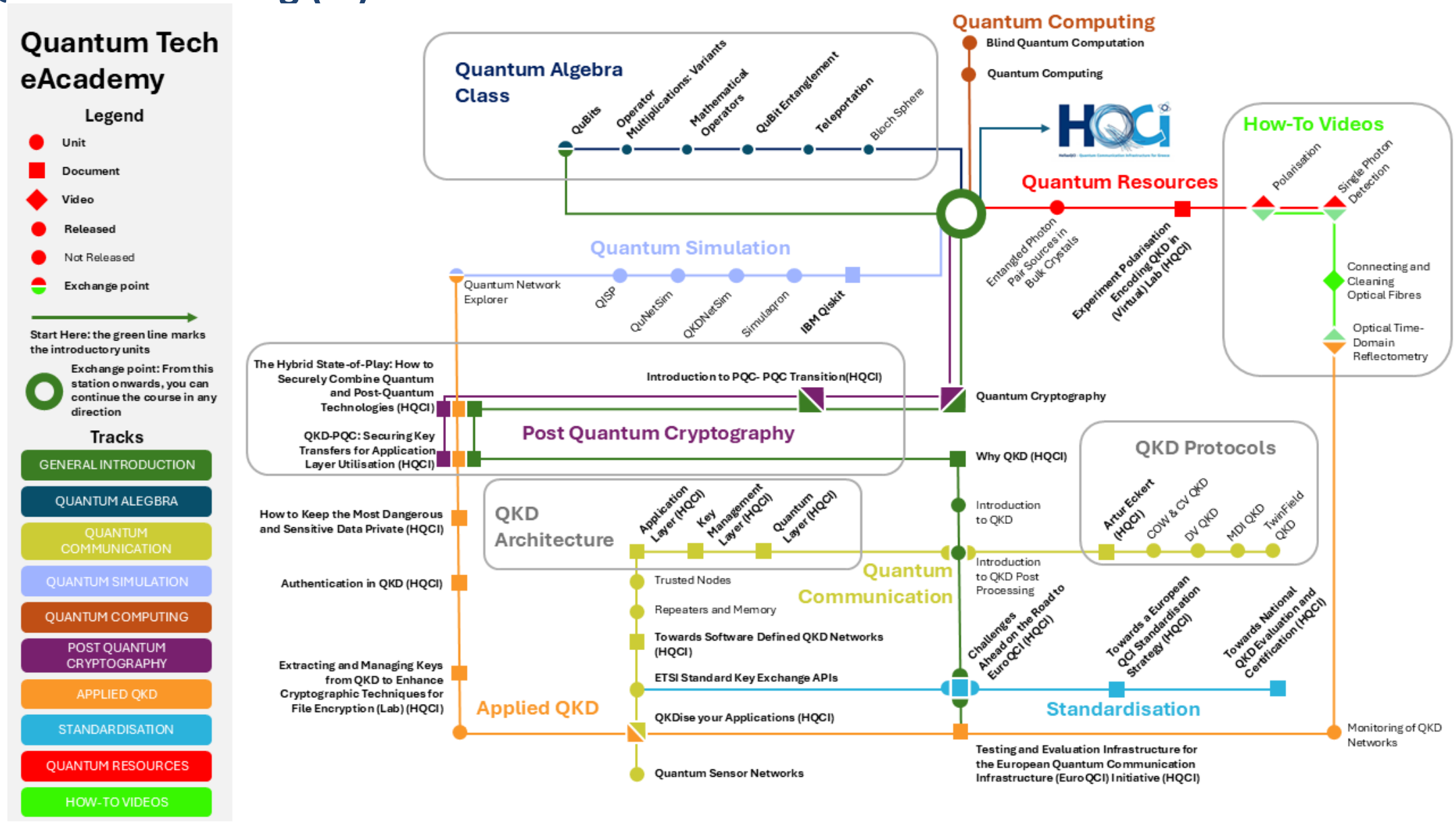
Applied QKD

- How to Keep the Most Dangerous and Sensitive Data Private (HQCI) (15')
- Authentication in QKD (HQCI) (20')
- Extracting and Managing Keys from QKD to Enhance Cryptographic Techniques for File Encryption (Lab) (HQCI) (55')
- QKDise Your Applications (HQCI) (10')
- Testing and Evaluation Infrastructure for the European Quantum Communication Infrastructure (EuroQCI) Initiative (HQCI) (15')

External Collaborations

- HellasQCI Online Training Platform (HQCI)

Quantum Training (III)

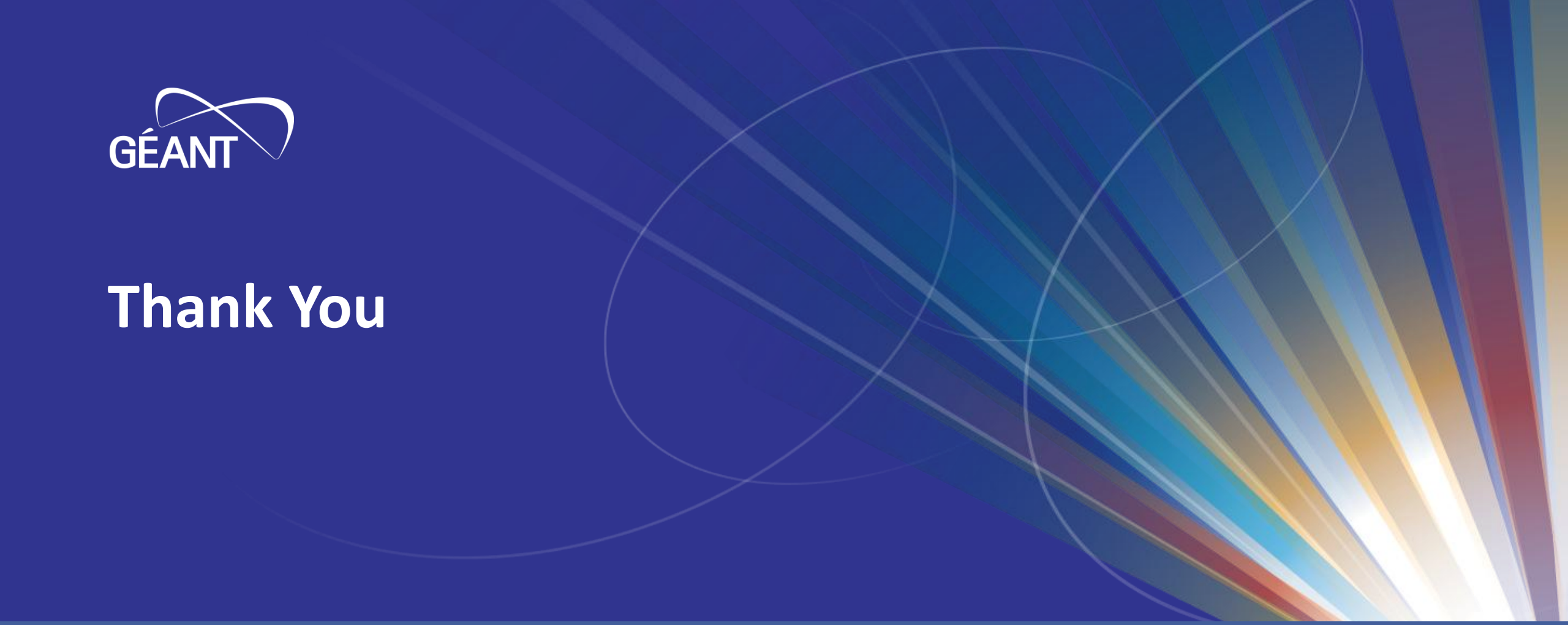


Events

- **Upcoming Infoshare: Community-Built Quantum Communication Tools**
  - **Register at https://events.geant.org/event/1949/**
  - **December 3, 2025, 14:00 CET,**
    - *"Basque open and standard-compliant KMS for quantum-safe networks by EHU"*
      - Eire Salegi Zulaika (EHU)
    - *"On the Road to Scalable Quantum Communications: The Benefits of Network Programmability"*
      - Asier Atutxa Imatz, David Franco (EHU)
    - *"EduQKD – Overview and Deployment"*
      - Wojciech Kozlowski, David Maier (SURF)

- In case you missed it….
  - Infoshare: Operational Aspects of Quantum Communication Networks
    - September 2, 2025
    - https://www.youtube.com/watch?v=cmpf9V6bhdw
  - Infoshare: Quantum KMS Architectures and Services
    - May 28, 2025
    - https://www.youtube.com/watch?v=kRKs9D7hhrA

Image by ZedH from Pixabay



Thank You

www.geant.org

Co-funded by
the European Union