INT-UQKD
Quantum Key Distribution

International Use Cases

Satellite-Terrestrial Quantum Key Distribution & Post Quantum Cryptography Applications and Services

Introducing INT-UQKD

The International Use Cases for Operational Quantum Key Distribution Applications and Services project (INT-UQKD) was launched in Luxembourg in September 2022. Its primary objective is to enable quantum-safe communications links for specific use cases in operational IT environments – particularly in regulated sectors that have very strong security requirements – and to demonstrate the technology's maturity for commercial use.

- The INT-UQKD project uses quantum key distribution (QKD) technologies, exploits the quantum properties of light and leverages existing optical communication infrastructures to securely exchange encryption keys between two or more locations. This creates a network of interconnected trusted nodes from which a wide range of security services are established.
- Quantum-safe communications links have been demonstrated successfully by INT-UQKD over existing terrestrial optical fibre networks. The next step is to complement the capabilities of INT-UQKD with satellite-based QKD, enabling very secure communication over long distances not economically feasible over terrestrial networks.

The project is funded by the European Space Agency (ESA) under the Advanced Research in Telecommunications Systems (ARTES) R&D programme in satellite communications technologies, services and applications.

with Starion, prime contractor (Luxembourg).

The project is set up on an international collaboration with partners in Luxembourg (POST Luxembourg, HITEC Luxembourg and the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg), Canada (evolutionQ) and Singapore (SpeQtral).

INT-UQKD
Quantum Key Distribution

Addressing the quantum threat

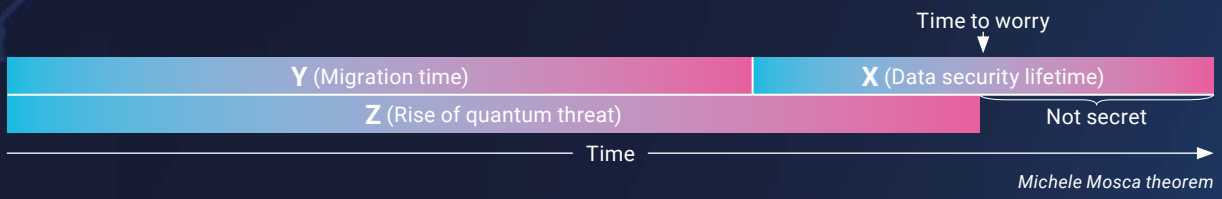
Cryptography is essential to protect communications and safeguard data throughout its lifetime. With large-scale, error-free quantum computers on the horizon, many existing cryptographic techniques that underpin today's global communications networks are at risk. New quantum-safe technologies need to be developed and validated to safeguard critical data communication services and IT infrastructures in the post-quantum era.

The INT-UQKD project combines terrestrial and satellite QKD solutions with post-quantum cryptography (PQC) elements to provide a secure, sustainable communications solution. It is designed to be quantum-safe across a wide range of interconnected networks and integrated with existing 'last mile' local networks.

INT-UQKD's hybrid approach ensures resilience by removing any single point of vulnerability. This security in depth ensures that any threat targeting either QKD or PQC will not critically impact service delivery security: an adversary would need to master and simultaneously exploit potential vulnerabilities within PQC and QKD to succeed.

Why do we need a quantum-safe solution?

Resilient quantum-safe cryptography is required to protect users and IT systems against attacks and threats posed by future quantum computers on today's IT infrastructure and sensitive data.



X = Time that critical data needs to stay secure – varies according to type of data

Y = Time required to implement a quantum-safe solution on a global scale

Z = How long it will take for large-scale, error-free quantum computers to emerge

If Y + X > Z = Risks are high because secrets are no longer secured.

The benefits of a hybrid approach

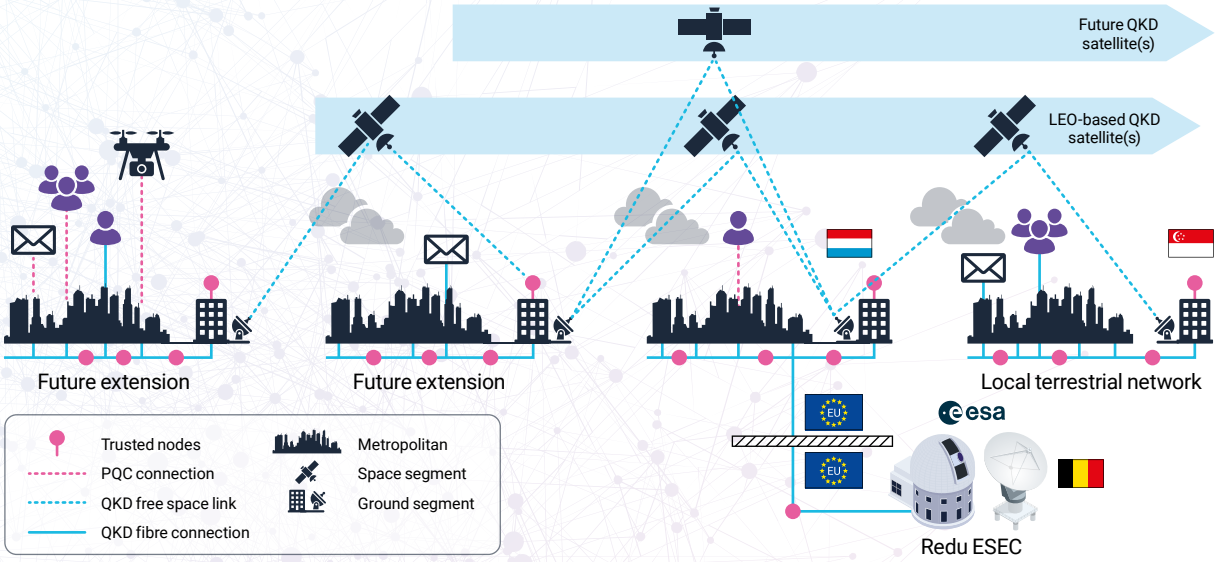
Deploying a quantum communication infrastructure (QCI) at national and European levels is essential to address emerging quantum threats and ensure the security and resilience of communication systems. The challenge is to deploy a solution that is truly resilient against persistent threat actors.

Combining QKD with PQC creates a hybrid approach that leverages the strengths of both technologies to protect digital communications that are fundamentally dissimilar:

- QKD relies on the principles of quantum mechanics to directly enable secure symmetric-key exchange, providing potentially unconditionally secure key establishment.
- PQC is built on complex mathematical problems, such as lattice-based, code-based, multivariate and hash-based structures – this ensures that the encryption algorithms themselves are resistant to classical and quantum attacks.

Because PQC and QKD are based on entirely different principles and the types of threats facing them are distinct, there is no shared vulnerability that could create a single point of failure.

INT-UQKD Network architecture



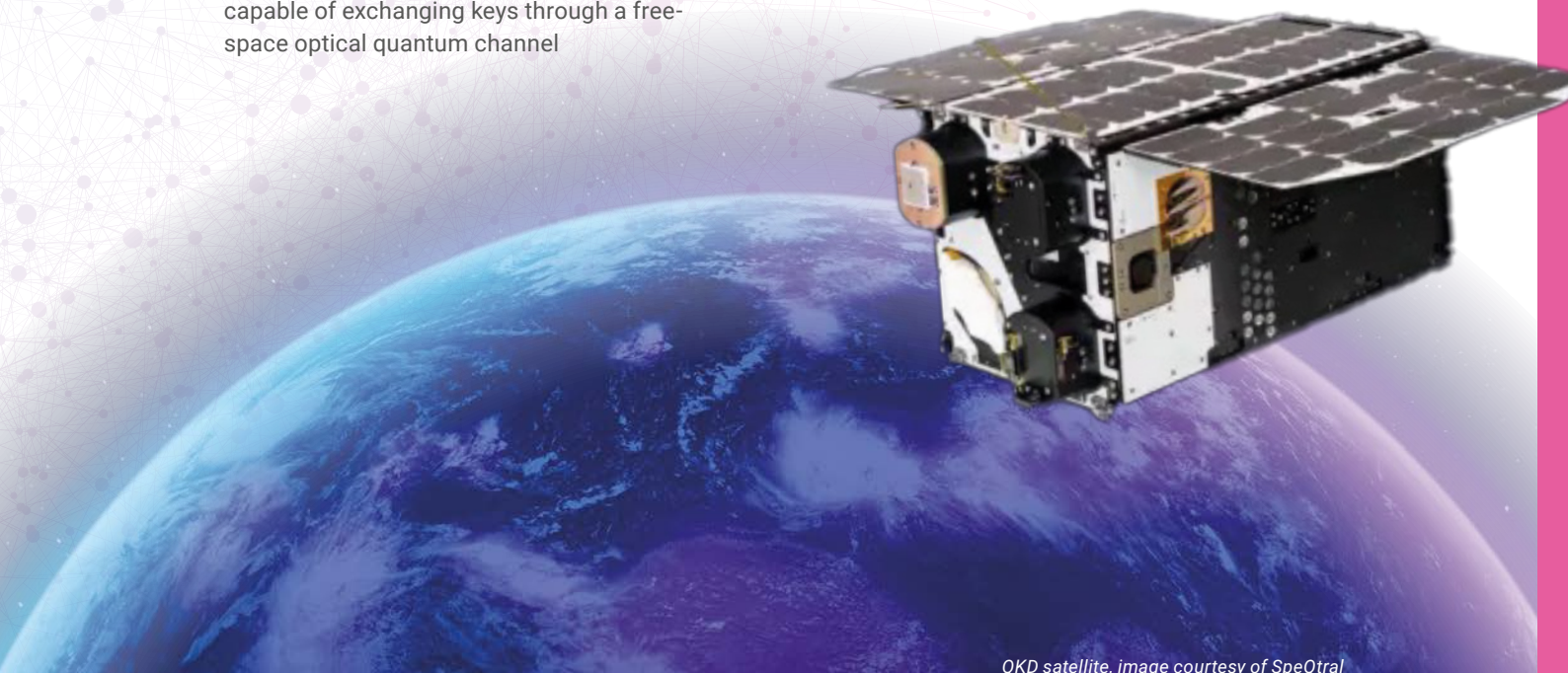
INT-UQKD high-level system architecture

System architecture

The system comprises these building blocks to deliver quantum-safe data services:

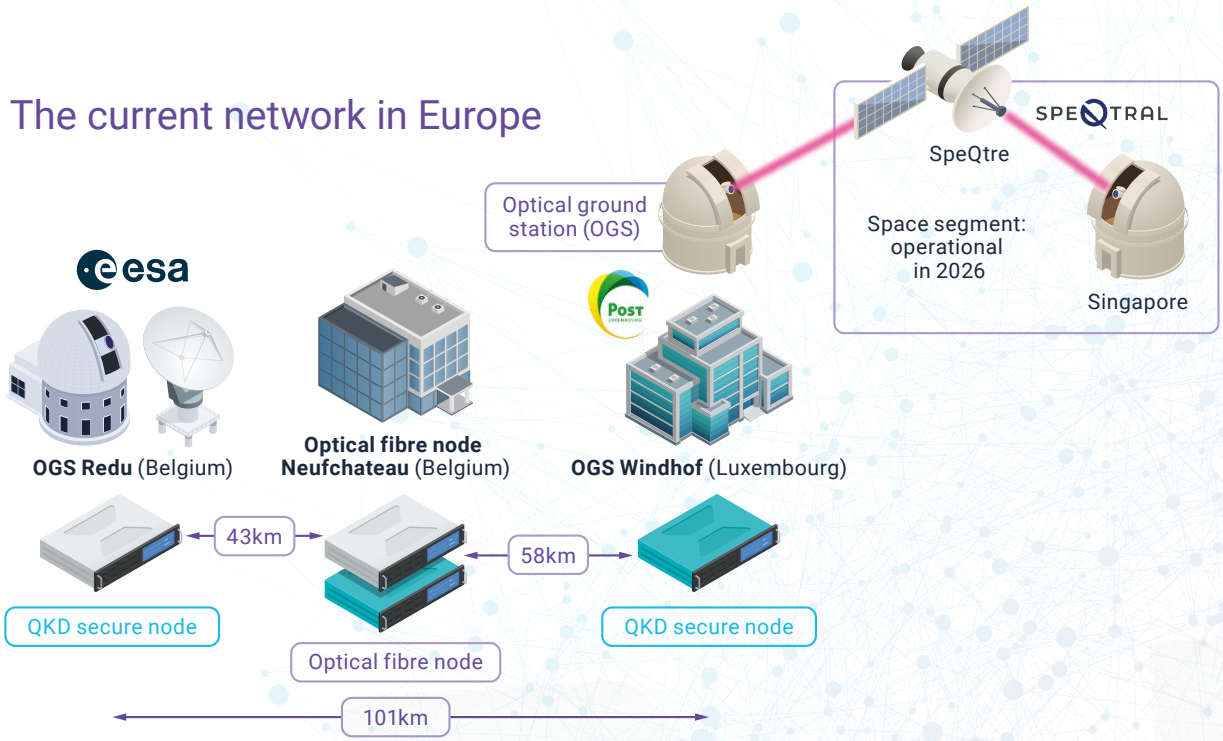
- QKD connectivity between core customer sites that become the backbone of the network. They can be either:
  - **Terrestrial:** implemented over existing terrestrial optical fibre communication networks
  - **Space:** through low Earth orbit (LEO) satellites capable of exchanging keys through a free-space optical quantum channel
- PQC connectivity to remote endpoints, enabling secure connectivity using classical communication channels (such as 5G/6G, RF link or ethernet).

The system architecture is infrastructure agnostic, allowing future quantum-safe extensions to enhance technical capabilities and expand the network geographically.



QKD satellite, image courtesy of SpeQtral

The current network in Europe



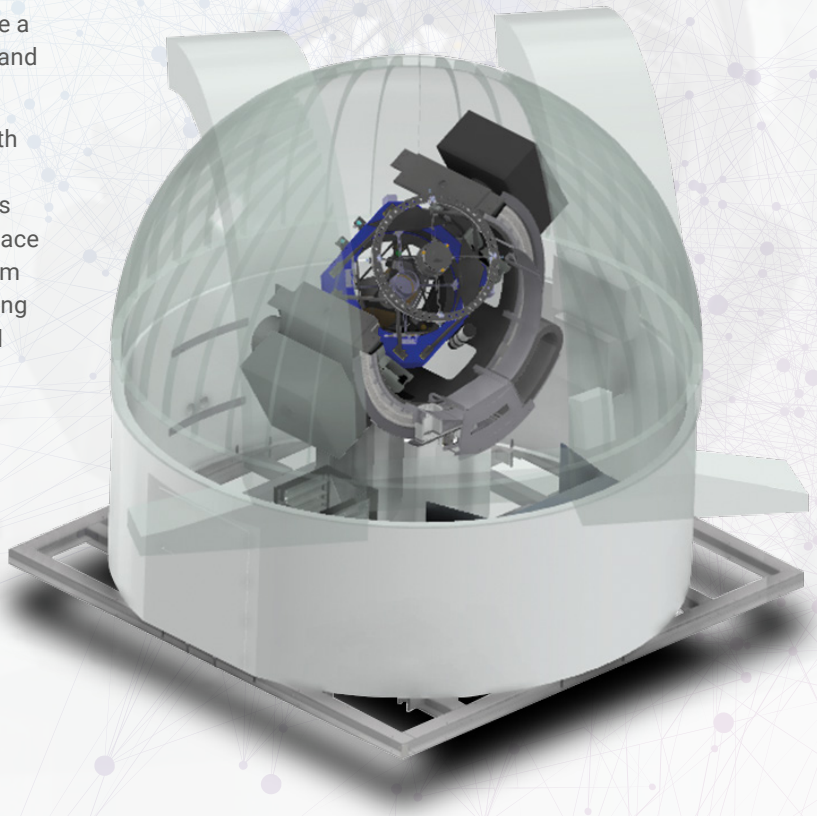
Terrestrial network (Demo-1)

The INT-UQKD project achieved its first major milestone in November 2024, when consortium partners successfully completed the initial phase in deploying an operational terrestrial network across Luxembourg and Belgium. This set the stage for the next, space-based phase.

Hybrid space-terrestrial network (Demo-2)

To overcome the distance limitations of QKD over fibre networks, the upcoming phase will demonstrate a satellite-based QKD link between Luxembourg and Singapore.

Demo-2 will utilise SpeQtral satellites, along with a newly established optical ground station in Luxembourg. Quantum-secure communications will be established between ESA's European Space Security and Education Centre (ESEC) in Belgium and Singapore, routed through Luxembourg using a combination of terrestrial fibre optic links and satellite QKD links.



OGS image courtesy of HITEC LUXEMBOURG

Project benefits

The definition, verification and validation of business-focused QKD use cases are key steps toward enabling secure, quantum-safe communications worldwide. This effort also supports the European Union's (EU's) goals of achieving digital sovereignty and strategic autonomy.

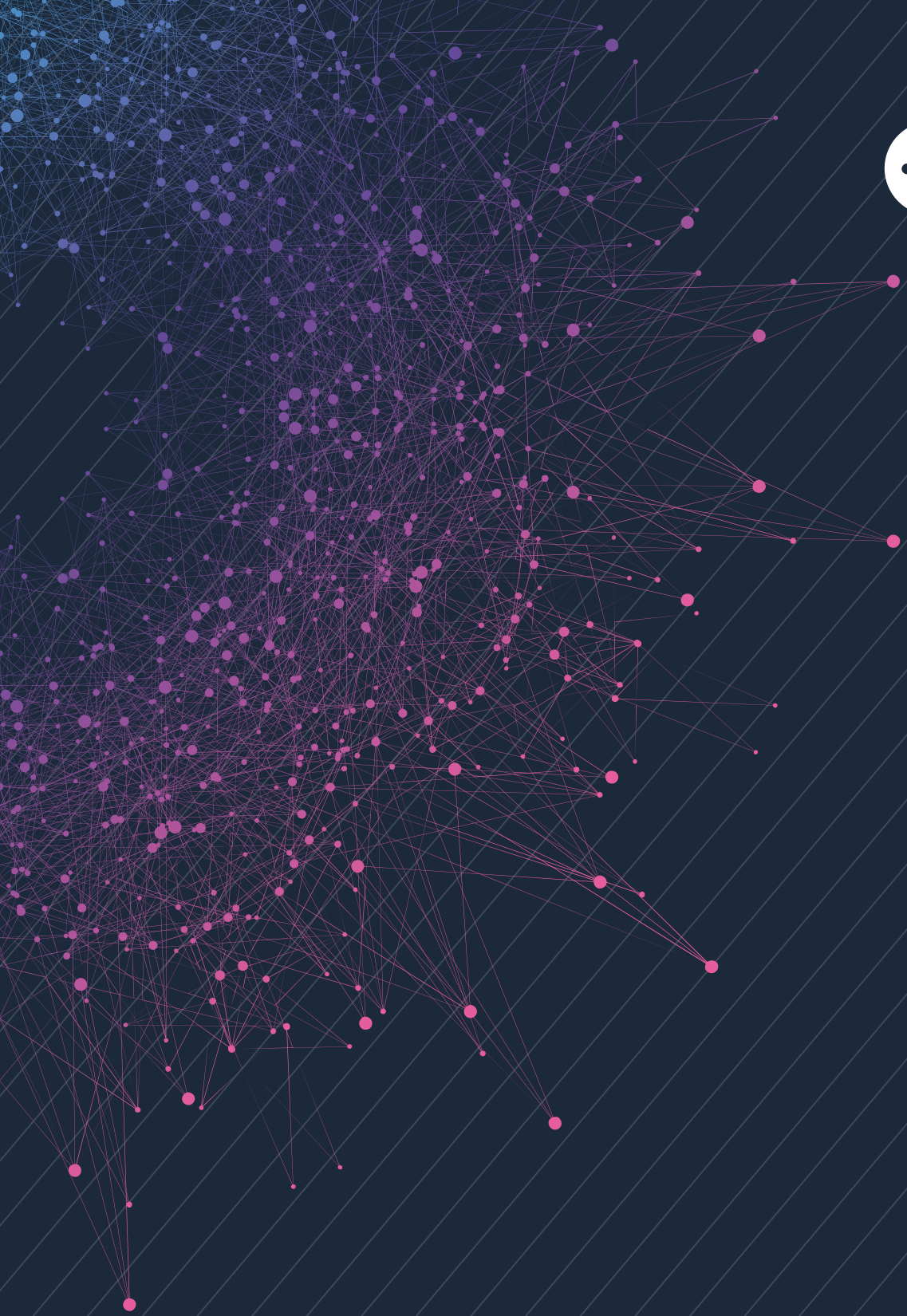
The INT-UQKD project will test and demonstrate QKD and PQC technologies in real-world operational environments. These tests will use a hybrid setup that combines optical fibre and satellite systems, ensuring smooth and secure communication across different platforms. This positions INT-UQKD at the forefront of next-generation secure communications.

The project is playing a critical role in evaluating and validating future technology options, ensuring compliance with post-quantum security standards, and guiding EU policymakers in shaping strategies for quantum communications and quantum information networks.

INT-UQKD will be essential for uncovering new economic opportunities in the field of secure connectivity.

INT-UQKD contributes to creating secure connectivity standards and aligning certification processes across the EU.

Through practical, business-focused demonstrations, INT-UQKD is generating valuable insights for commercial stakeholders aiming for rapid market entry and long-term sustainability of quantum-safe technologies, products and services tailored to the needs of institutional, corporate and individual users.



esa

INT-UQKD

Quantum Key Distribution

STARION | POST LUXEMBOURG | SNT | HITEC LUXEMBOURG | evolution | SPEQTRAL