Xacobeo 2027

CESGA

GALICIA SUPERCOMPUTING CENTER

QUANTUM COMMUNICATION INFRASTRUCTURES AND PROJECTS

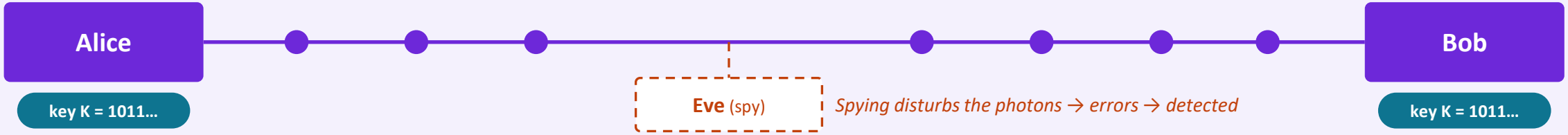
XUNTA DE GALICIA

CSIC
CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS

Visit: https://www.cesga.es

Quantum key distribution (QKD) in a nutshell

Sharing secret keys whose security comes from the laws of physics, not from hard maths problems



1 What is it for?

- **Sharing a secret key** between two distant sites: data centres, governments, banks, hospitals…
- **The key then encrypts the data** with standard ciphers (AES, or a one-time pad).
- **Long-lasting protection:** data intercepted today cannot be decrypted later, not even with a quantum computer.

2 What makes it different?

RSA / ECC	Hard maths problems. A large quantum computer breaks them.
PQC	New maths problems, in software. Believed hard, but not proven.
QKD	Laws of physics: spying is detected. Needs dedicated hardware; limited distance.

PQC and QKD are complementary, not rivals.

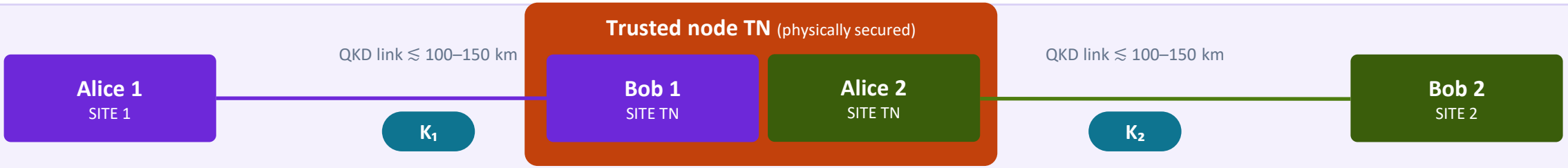
3 Which physics is behind it?

- **Measuring disturbs:** reading a quantum state the wrong way changes it.
- **No-cloning:** an unknown quantum state cannot be copied.
- **Entanglement:** correlations that only Alice and Bob can share.

→ Any spy leaves detectable errors

Trusted-node QKD networks

How today's QKD networks go beyond ≈ 100 km: chaining links and relaying the key through secure nodes



1. Each link generates its own key with QKD: K_1 (SITE1 – SITE TN) and K_2 (SITE TN – SITE 2)

2. Node TN sends $K_1 \oplus K_2$ to SITE 2 over an ordinary public channel

3. B computes $(K_1 \oplus K_2) \oplus K_2 = K_1$: A and B now share K_1

Why are they needed?

- **Fibre absorbs light:** beyond ≈ 100–150 km almost no photons arrive.
- **No amplifiers:** classical signals are amplified, but quantum states cannot be copied or amplified.

Advantages

- **Any distance** with today's commercial equipment.
- **Networks, not just links:** keys can be routed between any pair of sites.
- **Deployed today:** Beijing–Shanghai (2000 km, 32 nodes); EuroQCI national networks.

Limitations

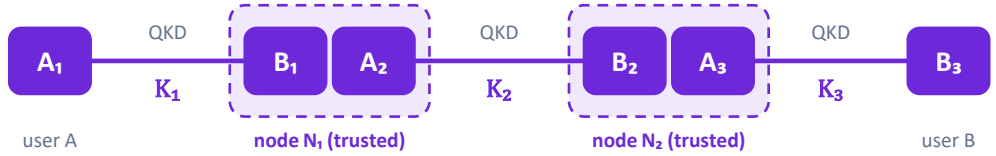
- **Each node sees the key in clear,** so it must be trusted and physically protected.
- **Not end-to-end security.**
- **Long-term fix:** quantum repeaters and the quantum Internet (next slide).

From QKD to the quantum Internet

QKD uses quantum properties to obtain something classical; the quantum Internet distributes the quantum states themselves

Classical Internet: distributes bits → **QKD network:** distributes secret keys (classical bits) → **Quantum Internet:** distributes qubits and entanglement

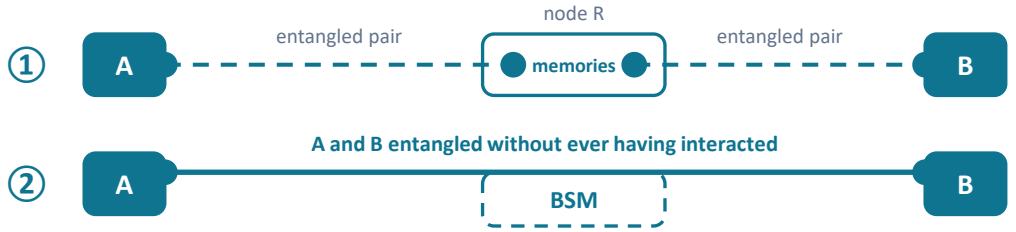
TODAY — QKD network with trusted nodes



Classical channel: $N_1 \to N_2$: $K_1 \oplus K_2$ · $N_2 \to B_3$: $K_1 \oplus K_3$ ⇒ **A_1 and B_3 share K_1**

- **Short segments:** each link ($\lesssim$ 100–150 km) generates its own key with point-to-point QKD
- **Classical relay:** at each node the key is classical and is forwarded encrypted with a one-time pad
- **Cost:** arbitrary reach, but every node knows the key and must be physically protected
- **Example:** Beijing–Shanghai, 2000 km of fibre with 32 trusted nodes; 4600 km with the Micius satellite

FUTURE — Quantum Internet: entanglement



- **Entanglement swapping:** a Bell measurement at the intermediate node joins two pairs into one long-distance pair
- **Quantum repeater:** memories + swapping + purification (no-cloning forbids amplification)
- **Uses:** End-to-end QKD without trusted nodes (E91, DI-QKD), teleportation, distributed and blind computing, networked clocks and sensors

Stages towards the quantum Internet (Wehner, Elkouss and Hanson, Science 2018)

1 · Trusted nodes → 2 · Prepare and measure → 3 · Entanglement distribution → 4 · Quantum memories → 5 · Few-qubit, fault-tolerant → 6 · Quantum Internet

Current QKD (DV, CV, MDI, TF) — *laboratory demonstrations* — *long term*

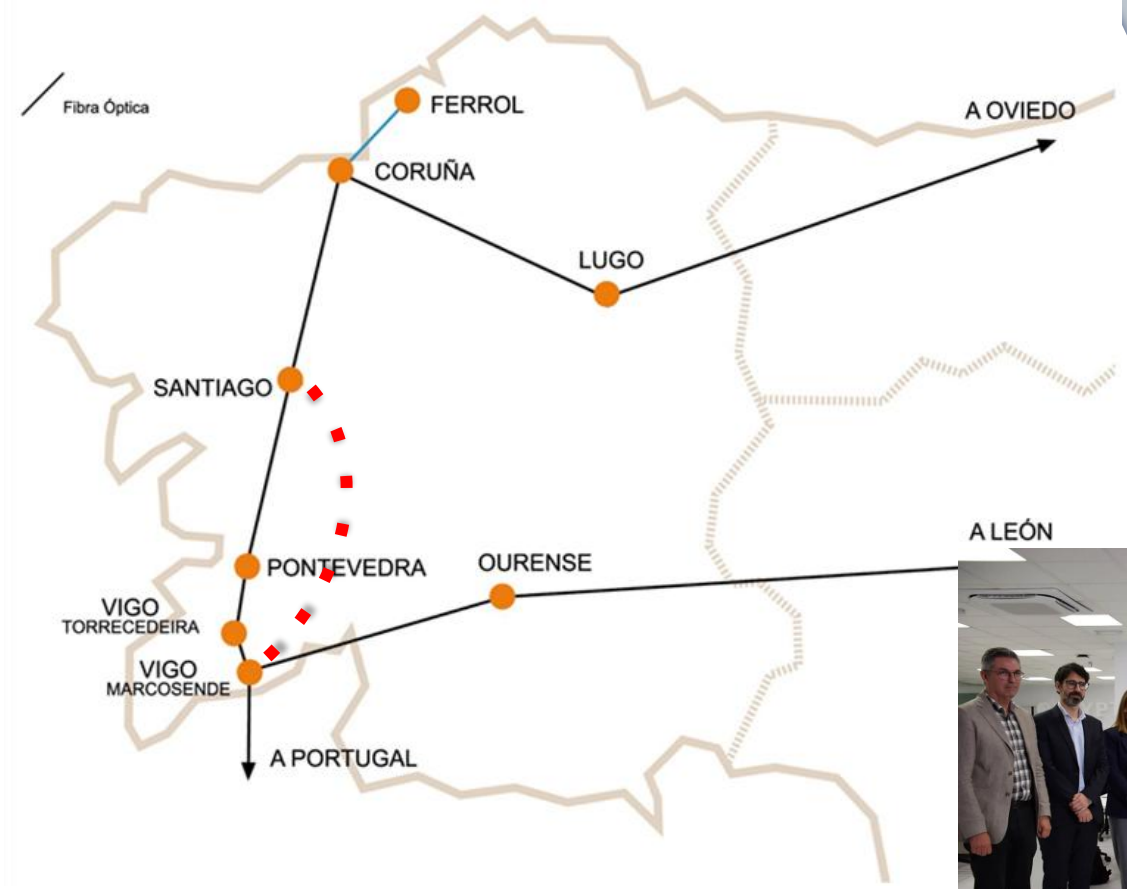
QKD families at a glance

Three ways of organising the link, from mature prepare-and-measure systems to relay-based schemes that reach furthest

	PREPARE & MEASURE *Alice prepares the states, Bob measures them*		ENTANGLEMENT-BASED *A source sends pairs; both measure*	INTERFERENCE AT AN UNTRUSTED RELAY *Both prepare; a middle station interferes and measures*	
	DV-QKD **Discrete variable**	CV-QKD **Continuous variable**	EB-QKD **Entanglement-based**	MDI-QKD **Measurement-indep.**	TF-QKD **Twin-field**
How it works	Each bit is carried by a single photon (e.g. its polarisation)	The key is encoded in the amplitude and phase of weak laser light	A central source sends entangled photon pairs to both users	Both users send photons to an untrusted station in the middle	Like MDI, but one photon reaching the middle station is enough
Record distance	**421 km** fibre, 2018	**202 km** fibre, 2020	**248 km** fibre, 2022 · satellite: 1120 km	**404 km** fibre, 2016	**1002 km** fibre, 2023
Practical reach	**≈ 100–150 km**	**≈ 50–100 km**	**≈ 50–100 km**	**≈ 100–200 km**	**≈ 400–500 km (field)**
Main strength	+ Most mature; widely commercial	+ Standard telecom parts; less cost	+ Source need not be trusted; works via satellite	+ Immune to detector hacking; star networks	+ Longest reach without repeaters
Main limitation	– Costly single-photon detectors	– Short reach	– Low key rates	– Lower rates; harder to build	– Very precise phase control between lasers
Maturity	●●●● Commercial	●●●○ Early commercial	●●○○ Pilots, satellites	●●○○ Prototypes, pilots	●○○○ Field trials

DV / CV refers to the encoding, a separate axis from the scheme (e.g. CV-MDI exists). Record: longest demonstrated distance (bar up to 1000 km). Practical reach: typical deployed links.

Case study: Deployment of QKD link between CESGA and the VQCC



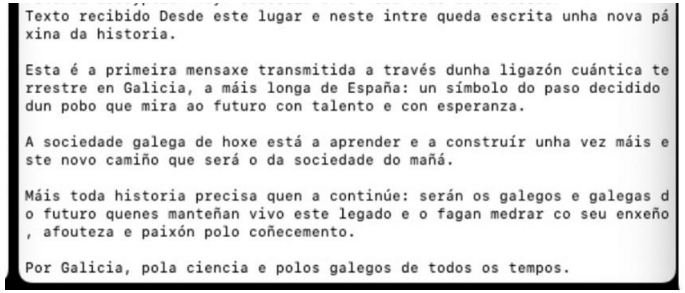
Deployment of QKD link between CESGA and the VQCC

- Platform: QUELL-XR (Quantum Telecommunications Italy, QTI) **(European technology)**
- 3-state decoy BB84 protocol encoded in time bin
- Two external superconducting single-photon detectors (Opus ONE) operating @ 2.1K. Quantum efficiency >90%.
- Link length >120 km, overall attenuation ~30 dB
- Current Secure Key Rate: 3.6 ± 0.7 Kbit/s



Link presentation (9th Oct 2025).

First message exchanged:
One time pad secure communication between the Regional Minister for Education, Science, Universities and Vocational Training (Vigo), and a civil servant (Santiago)



Texto recibido Desde este lugar e neste intre queda escrita unha nova pá
xina da historia.

Esta é a primeira mensaxe transmitida a través dunha ligazón cuántica te
rrestre en Galicia, a máis longa de España: un símbolo do paso decidido
dun pobo que mira ao futuro con talento e con esperanza.

A sociedade galega de hoxe está a aprender e a construír unha vez máis e
ste novo camiño que será o da sociedade do mañá.

Máis toda historia precisa quen a continúe: serán os galegos e galegas d
o futuro quenes manteñan vivo este legado e o fagan medrar co seu enxeño
, afouteza e paixón polo coñecemento.

Por Galicia, pola ciencia e polos galegos de todos os tempos.

Interconnecting regional QKD Networks: Hybrid key delivery across quantum domains

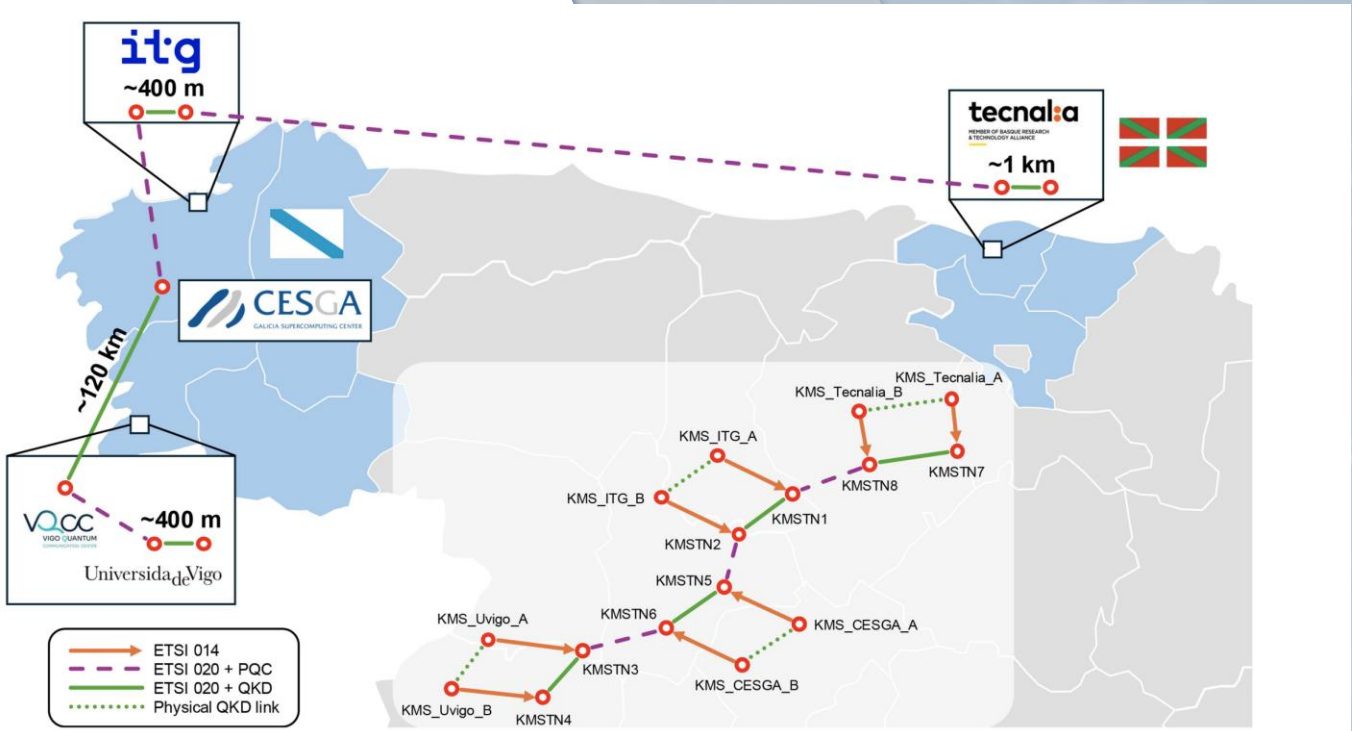


FIGURE 2. Map and network topology of our testbed, spanning the regions of Galicia and the Basque Country, in Northern Spain. The solid green lines represent links which are secured via a physical QKD link, through which keys can propagate via ETSI 020 using QKD + PQC encryption, and the dashed purple lines show links where ETSI 020 interfaces were implemented using PQC encryption only. In the inset, the dotted lines represent physical QKD links with vendor KMS, from which the KMSTN nodes extract QKD keys via ETSI 014 calls (orange arrows).

D. Barral et al., "Interconnecting Regional QKD Networks: Hybrid Key Delivery Across Quantum Domains," in IEEE Transactions on Quantum Engineering, vol. 7, pp. 4102117-4102117, 2026, Art no. 4102117, doi: 10.1109/TQE.2026.3728800.
keywords: {ETSI;Joining processes;Security;Management;Architecture;Computer architecture;Quantum key distribution;Relays;Timing;Databases;Key delivery service;network management and operations;post-quantum cryptography (PQC);quantum key distribution (QKD)},

- **Vigo (VQCC) – Santiago (CESGA) quantum link**

The supply of QKD (Quantum Key Distribution) equipment for the Vigo–Santiago quantum link is funded by MICINN with European Union NextGenerationEU funds, Recovery, Transformation and Resilience Plan **(Component 17, Investment 1)** and by the Xunta de Galicia's own funding through the "Complementary R&D&I Plans with the Autonomous Communities" in Quantum Communications.



The deployment of dark fibre for the Vigo–Santiago quantum link is funded by the European Union – NextGenerationEU, Recovery, Transformation and Resilience Plan (**Component 21, Investment 15)** "Improvement of university digital infrastructures, equipment, technologies, teaching and digital assessment"



- COMPLEMENTARY PLAN FOR QUANTUM COMMUNICATIONS

Supported by MICINN with European Union NextGenerationEU funding, Recovery, Transformation and Resilience Plan **(Component 17, Investment 1)** and by the Xunta de Galicia's own funding through the "Complementary R&D&I Plans with the Autonomous Communities" in Quantum Communications.

Financiado por la Unión Europea NextGenerationEU

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

Plan de Recuperación, Transformación y Resiliencia

AXENCIA GALEGA DE INNOVACIÓN

- QMIO quantum infrastructure

Quantum SPAIN

España | digital 2026

Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea NextGenerationEU

RED ESPAÑOLA DE SUPERCOMPUTACIÓN

"This work has been financially supported by the Ministry of Economic Affairs and Digital Transformation of the Spanish Government through the QUANTUM ENIA project call - Quantum Spain project, and by the European Union through the Recovery, Transformation and Resilience Plan - NextGenerationEU within the framework of the Digital Spain 2026 Agenda".

- FINISTERRAE III

XUNTA DE GALICIA

CSIC

Consejo Superior de Investigaciones Científicas

Unión Europea

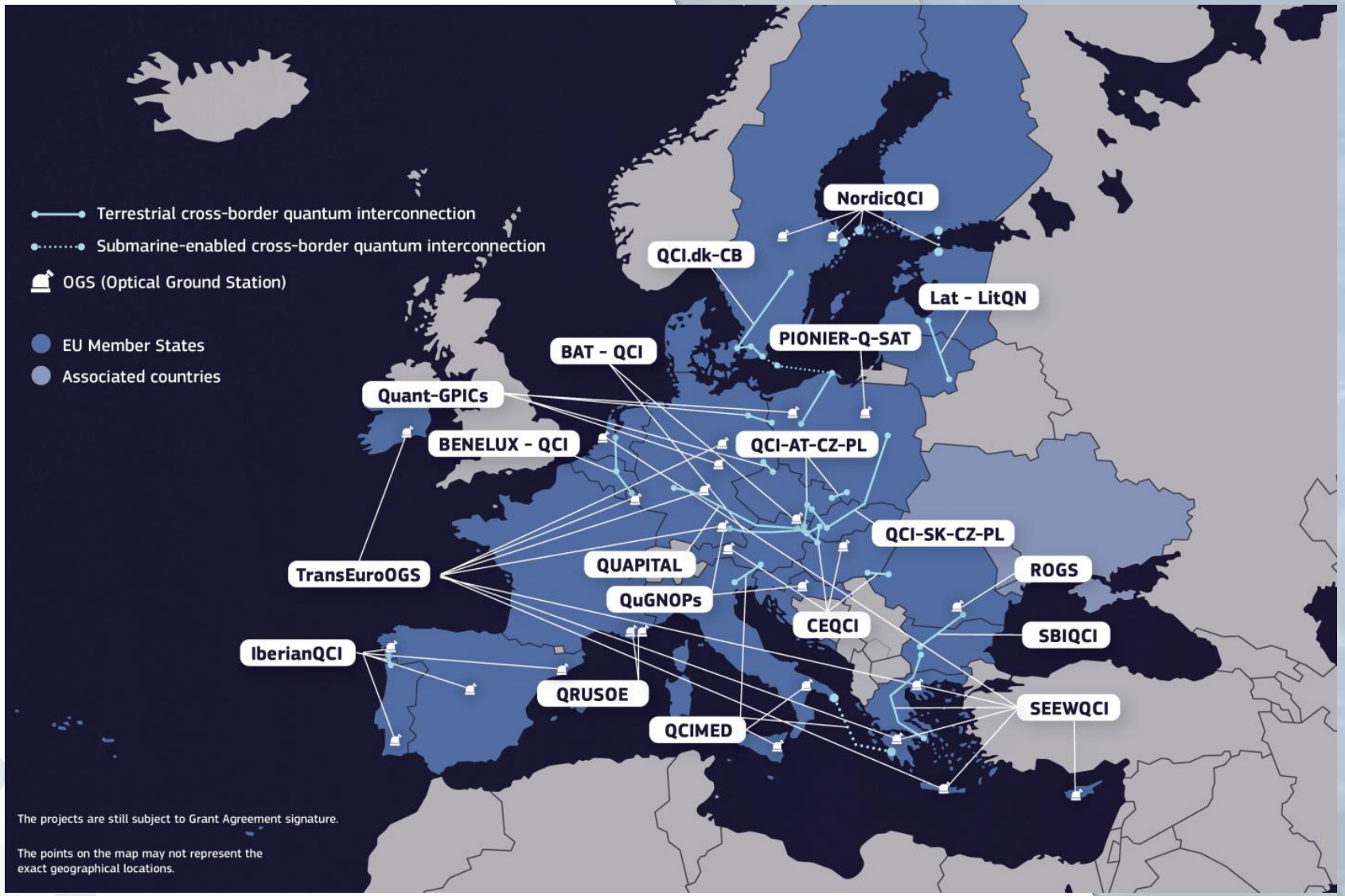
Fondo Europeo de Desarrollo Regional "Una manera de hacer Europa"

GOBIERNO DE ESPAÑA

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

RED ESPAÑOLA DE SUPERCOMPUTACIÓN

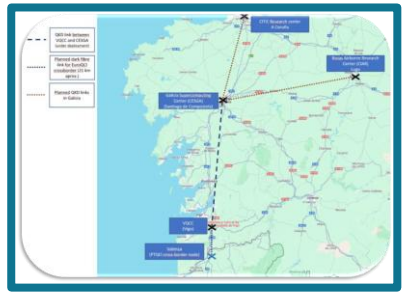
EuroQCI


Terrestrial cross-border quantum interconnection
Submarine-enabled cross-border quantum interconnection
OGS (Optical Ground Station)
EU Member States
Associated countries
NordicQCI
QCI.dk-CB
Lat - LitQN
PIONIER-Q-SAT
BAT - QCI
Quant-GPICs
BENELUX - QCI
QCI-AT-CZ-PL
QCI-SK-CZ-PL
TransEuroQGS
QUAPITAL
ROGS
QuGNOPs
CEQCI
SBIQCI
IberianQCI
QRUSOE
SEEWQCI
QCIMED
The projects are still subject to Grant Agreement signature.
The points on the map may not represent the exact geographical locations.

IBERIANQCI

BUILDING THE QUANTUM GATEWAY TO SOUTHERN WEST EUROPE

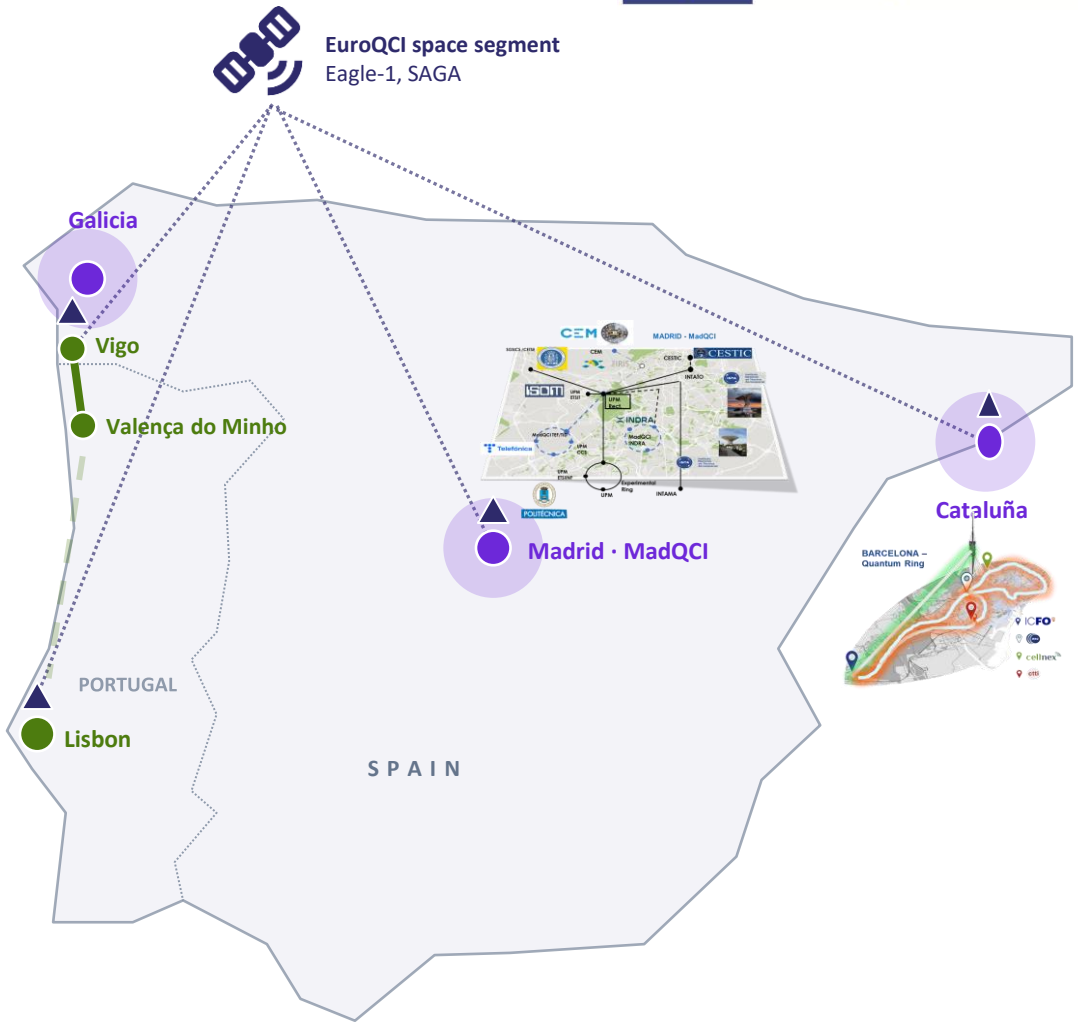
Co-funded by the European Union



CESGA GALICIA SUPERCOMPUTING CENTER

VQCC VIGO QUANTUM COMMUNICATION CENTER





Regional node / "island" — — Interconnection (next step) ▬ IberianQCI (fibre) ▲ Optical ground station (OGS)

Illustrative diagram; approximate positions.

NETWORK EVOLUTION

1 REGIONAL **Quantum "islands"**

National Complementary Plan for Quantum Comms: Galicia, Madrid, Catalonia, Basque Country and Castilla y León, among others. Next step: interconnecting them

3 CROSS-BORDER **IberianQCI**

Terrestrial link Vigo – Valença do Minho and OGSs in Vigo, Lisbon, Madrid and Barcelona

4 EUROPEAN **EuroQCI**

Terrestrial segment (fibre) + space segment (satellites). The 27 Member States, the European Commission and ESA

IBERIAN QCI

KO MEETING

14/05/2026







BUILDING THE QUANTUM GATEWAY TO SOUTHERN WEST EUROPE

INDRA · Infraestruturas de Portugal · IP Telecom · instituto de telecomunicações · altice labs · TÉCNICO LISBOA · ICFO · POLITÉCNICA · CSIC · Telefónica · VQCC VIGO QUANTUM COMMUNICATION CENTER · CESGA

Work packages

IBERIAN QCI

WP1 Coordination and Management
INDRA

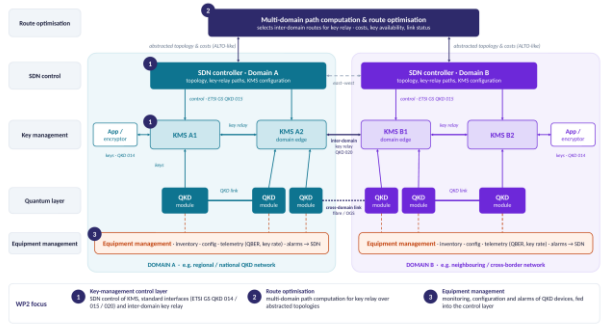
WP2: Network control and Crossborder Network Connectivity
POLITÉCNICA | UNIVERSIDAD POLITÉCNICA DE MADRID

WP3: Terrestrial Cross Border Implementation
CESGA

WP4: Space Cross Borders Implementation
INDRA

WP5: Use Cases and Europe-Wide Tests
ICFO | CSIC

WP2



CESGA
GALICIA SUPERCOMPUTING CENTER

WP3



POLITÉCNICA

WP4



indra

WP5



CSIC
CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS
ICFO

QUANTUM_IBER_IA · Quantum communications

Interreg VI-A Spain–Portugal (POCTEP) 2021–2027 · Dec 2025 – Dec 2028 · led by GAIN, with 17 Spanish and Portuguese partners

Project goal

To strengthen a cross-border ecosystem between Spain and Portugal in quantum technologies and artificial intelligence by fostering collaboration among centres and coordinating their capabilities to develop solutions that can be adopted by businesses and public administrations.

PROJECT CODE
0590_QUANTUM_IBER_IA_6_E

IMPLEMENTATION PERIOD
01/10/2025 – 31/12/2028

TOTAL FUNDING
€8,859,923.35

ERDF FUNDING
€6,644,942.51

Quantum-communications activity

Develop and validate a **key management system (KMS) for QKD networks** on a software-managed virtual infrastructure:

1. **Integrate nodes** (UVIGO-CESGA-Scayle) →
2. **Emulate devices & protocols** →
3. **Evaluate in ≥ 2 use cases**

Participants and infrastructure

Virtual KMS layer · software-managed infrastructure to be built by the project

UVigo	CESGA	SCAYLE
coordinates the QKD demonstrator	Santiago de Compostela	León
QKD equipment · local network	**QKD equipment · local network**	**QKD equipment · local network**

Today: separate local QKD networks, not interconnected.
UVigo also brings the VQCC / atlanTTic labs: fibre, free-space and satellite communications.

Also planned: U. Aveiro · U. Extremadura · U. Minho · COMPUTAEX — *QKD equipment not yet specified*

0590_QUANTUM_IBER_IA_6_E · Co-funded by the European Union through the Interreg VI-A Spain–Portugal Programme (POCTEP) 2021–2027.

Thank you!



XUNTA DE GALICIA

CSIC
Consejo Superior de Investigaciones Científicas

Visit: https://www.cesga.es