France's industry, Quantum startups, academic and institutional players join forces to build the future of the French quantum Internet communication system.

- Supporting the EU's Cybersecurity Strategy.
- Securing communications and data for critical infrastructures and government institutions.

Brussels, Paris – 18 April 2023, Airbus, CNRS, Cryptonext Security, Direction Générale de l'Aviation Civile, Orange, Sorbonne Université, Telecom Paris, Thales, Thales Alenia Space, Université Côte d'Azur, Veriqloud and Welinq are pleased to announce the official launch of a programme in charge of deploying Quantum Communication Infrastructure (QCI) networks in France and perform experimentations with them. This FranceQCI project will span over 30 months

FranceQCI is part of the European Quantum Communication Infrastructure (EuroQCI) initiative launched by the European Union in 2019, under the helm of Thierry Breton, European Commissioner for Internal Markets, which aims at building a secure quantum communication network infrastructure that will span the whole European Union, including its overseas territories. As such, it is one of the main pillars of the EU's new Cybersecurity Strategy for the coming decades and aims at securing communications and data for critical infrastructures and government institutions.

As part of this program, 26 out of 27 member countries of the EU will have its own program to deploy its national QCI network. The European Commission has selected a consortium of thirteen (13) partners to deploy national QCI networks in France and perform experimentations.

FranceQCI is a project co-funded by the European Commission.

The project falls within the Digital Europe Programme; it is a significant contribution in France to the objective of deploying a secure quantum communication infrastructure for the EU (EuroQCI) and paves the way towards the future European Quantum Information Network (QIN).

In particular, FranceQCI's objective is to deploy advanced national quantum systems and networks to test quantum communication technologies and integrate them into existing communication networks in France. FranceQCI will capitalize on existing infrastructures in the Paris (ParisRegionQCI) and Nice (Quantum@UCA/Nice) areas to progress towards operational Quantum Key Distribution (so called QKD) services and contribute to the development of the European technological autonomy. A quantum network will also be implemented in Toulouse (in DGAC/DSNA/DTI lab) to test a real end-user service for the French Civil Aviation Authority. It will consist of exchanging simulated operational air traffic control data secured by QKD.

A strong consortium gathering key Quantum technology players and leading Academics

FranceQCI as a consortium includes stakeholders with diverse and complementary expertise and resources: large industries that are world leaders in their respective domains, small and medium enterprises

(SME/start-ups) with deep and unique expertise and academic institutions amongst the best in the world will participate in the effort.

FranceQCI is composed of Airbus Defense and Space, Orange, Thales, and Thales Alenia Space as leading industrial partners. Innovative key players in the field of Quantum Communication and post-quantum cryptography will support them: Cryptonext Security, VeriQloud, and WeLinQ.

The French civil aviation authority that provides air traffic control service (Direction des Services de la Navigation Aérienne - DSNA), joins the project as a public institution to allow the consortium to test realistic use-cases.

Leading research organization and academic institutions, namely the Centre National de la Recherche Scientifique (CNRS), Sorbonne University, Université Côte d'Azur and Télécom Paris and will bring the consortium their expertise and research capabilities. The strong presence of academic institutions will also allow the development of the educational purpose of the call and build a training environment for all stakeholders in France including research staff, engineers, end-users from public and private entities.

Orange has been appointed coordinator of FranceQCI consortium, as the only telco operator, essential for its expertise in network deployment and integration.

« The FranceQCI consortium's objective is to drive a significant impulse towards a European quantum communication infrastructure that will be able to safeguard sensitive data and critical communications for governmental institutions, data centers, hospitals, energy grids, and more. We are delighted to benefit from fundings from the European Union through the Digital Europe Program to contribute to one of the main pillars of the EU's cybersecurity strategy." says Michaël Trabbia, EVP, CEO Orange Wholesale, and interim Orange Group Chief Technology and Innovation Officer, representing all members of the France QCI consortium.

France QCI represents a first step towards a global European quantum communication infrastructure that could be implemented with crossborder links to connect similar networks in other countries, either through terrestrial fiber links or space connectivity.

About CryptoNext Security

CryptoNext was created in 2019, following more than twenty years of academic research in quantum-resistant cryptography by its founders. It offers its Quantum Safe Remediation software suite (C-QSR), which is natively agile and performance-optimized for a wide variety of CPU/OS platforms. C-QSR includes NIST standard Post-Quantum Cryptography (PQC) algorithms as well as the recommendations of the European National Security Agencies, and those related to protocol and certificate hybridization. C-QSR includes a complete set of integration tools and post-quantum application plugins for a broad range of uses such as business applications, secure messaging, HSM, VPN, PKI, Signature and Certificate Solutions, IoT, Blockchain and more.

Selected by the US National Cybersecurity Center of Excellence (NCCoE) for the "Migration to Post-Quantum Cryptography" work group, and named by Gartner as one of the Top 5 leaders in PQC, CryptoNext works with its customers to support them in their post-quantum migration roadmap for long-term efficiency.

Press contacts

CryptoNext: Christian d'Orival - christian.d-orival@cryptonext-security.com – +33 (0)6 03 00 26 31