

Moving quantum-secure communication from pilot to operational use



About QCFR

The Quantum Communication Fieldlab Rotterdam (QCFR) is a practical environment for testing, validating and operationalising quantum-secure communication in real-world infrastructure. It helps move quantum-secure communication from pilots and demonstrations towards trusted, everyday use, protecting critical and public infrastructure against current and future threats.

QCFR builds on proven results in the region: the 2024 Rotterdam port pilot, presented as the world's first scalable quantum internet connection, and the 2025 QUEST project, in which Quantum Key Distribution (QKD) is brought into operational use across two data centres in the Randstad. Together, the two initiatives accelerate the deployment and adoption of quantum-secure communication in the Netherlands.



What QCFR Does

QCFR brings technology, infrastructure and real networks together to answer one question: what does it take to run quantum-secure communication reliably in practice? It bridges the gap between demonstration and trusted operational use, focusing on validation, interoperability, operational readiness, integration with existing systems, and the governance and certification groundwork organisations need to adopt with confidence.



QCFR Focus Areas

- Quantum Key Distribution (QKD) in real infrastructure settings
- Advanced protocols such as measurement-device-independent QKD (MDI-QKD)
- Validation, interoperability and integration with existing networks
- Technical robustness and operational readiness
- Governance considerations and future certification and assurance approaches
- Capability development and knowledge transfer for participants



Founding Consortium Partners



QCFR manager. Leads project and fieldlab management, consortium coordination, project accountability, ecosystem development, and communication.



Quantum technology provider. Supplies QKD hardware, software and expertise, and drives the lab upgrade, R&D, use case development, technical validation and knowledge transfer.



Connectivity provider. Supplies the fibre and connectivity layer, the underlying technical environment, network connections and operational test conditions.



Network and security provider. Supplies network, routing and security technology, and handles integration with existing digital infrastructure and security architectures.



System integrator. Connects hardware, software, network and security components into one integrated, manageable and testable environment, and supports the move to operational use and market adoption.



Impact on Society

Quantum computers are expected, over time, to break parts of the encryption that currently protects digital communication. That's important not only for technology specialists, but for the everyday systems people rely on including banking, medical data, government communication, as well as the digital infrastructure behind ports, energy grids and other public and vital services.

This includes addressing the so-called 'harvest now, decrypt later' risk, where sensitive data intercepted today may become vulnerable in the future. Quantum Communication Fieldlab Rotterdam has been launched to help translate that future risk into practical action now, and strengthens Dutch and European digital resilience, trusted connectivity and strategic autonomy.



"With the QCFR fieldlab, our partners in Rotterdam and across Zuid-Holland are taking the next step in quantum-secure communication. Secure communication is a key issue not only for the vital operations in Europe's busiest port, but also for critical infrastructure and government organisations in our greater region. By rolling up their sleeves in collaboration, the QCFR consortium captures a great economic opportunity and is set to make an important contribution to Europe's security."

— Meindert Stolk, Regional Minister for Economy & Innovation of the Province of Zuid-Holland



How to Contribute

QCFR is built on collaboration and welcomes organisations that want to shape quantum-secure communication in practice. Organisations can get involved by bringing forward relevant use cases, exploring technology validation opportunities and exchanging knowledge with QCFR partners on implementation challenges around quantum-secure communication. Further information about participation, intake and contact points will be made available through www.qcfr.eu.



Strategic Partners



Contact

For questions, participation and further information, please contact:

Name: Arthur Dallau
Role: Fieldlab Manager, QCFR
Email: arthur@inspir8ion.nl
Website: www.qcfr.eu