

QCI-CAT

QCI: Proof of Concept - Secure Connectivity Austria

Programm / Ausschreibung	Digital Europe (FZÖ), Digital Europe FZOE 2022 (Ver), Deploying advanced national QCI systems and networks	Status	laufend
Projektstart	01.01.2023	Projektende	31.03.2026
Zeitraum	2023 - 2026	Projektlaufzeit	39 Monate
Keywords	Quantum Technologies, Cybersecurity		

Projektbeschreibung

In Hinblick auf die Datenautonomie ist die Datensicherheit zu einem grundlegenden Kriterium geworden. Im öffentlichen Sektor und den kritischen Infrastrukturen sichert sie die wirtschaftliche Wettbewerbsfähigkeit und die nationale Sicherheit. Technologische Durchbrüche in der Quantenwelt bedrohen unsere derzeitigen Verschlüsselungsmethoden, weshalb die Entwicklung neuer „quantensicherer“ Verschlüsselungstechnologien und -systeme notwendig ist. Dessen Bedeutung wird durch das auf 10 Jahre angelegte Forschungs- und Innovationsprogramm Programm EuroQCI Quantum Communication Infrastructure unterstrichen. Aufbauend auf der langjährigen Forschungserfahrung österreichischer Institutionen im Gebiet der Quantentechnologien, zielt das Projekt QCI-CAT auf den Einsatz moderner Verschlüsselungstechnologie auf Basis von QKD (Quantum Key Distribution) für die quantensichere Kommunikation zwischen öffentlichen Stellen ab.

Zu diesem Zweck wird ein QKD-Demonstrationsnetz installiert, das das Bundeskanzleramt (BKA) als zentralen Knotenpunkt mit dem BMLV, BMEIA und BMK verbindet. Aufbauend auf einer engen Zusammenarbeit zwischen Forschungspartnern und Industrieunternehmen wird QCI-CAT neue Sicherheitsanwendungen für Behörden, wie z.B. Secret Sharing und Nachrichtenauthentifizierung, erforschen und verifizieren. Die enge Zusammenarbeit zwischen den Stakeholdern stellt sicher, dass die Entwicklung von QKD-basierter Sicherheitstechnologie aus der Sicht eines IT-Endanwenders vorangetrieben wird.

QCI-CAT wird neue technologische Ansätze, wie die Kombination der Post-Quantum Verschlüsselungstechnologie mit QKD, QKD über große Entfernungen mit gesicherten vertrauenswürdigen Knoten und Feldversuche mit Quanten-Repeatern, erforschen. Die Ergebnisse von QCI-CAT liefern die Basis für eine starke Positionierung Österreichs innerhalb der EuroQCI-Initiative. Die Erkenntnisse werden mit den Nachbarländern geteilt und mit grenzüberschreitenden Verbindungen wird ein EU-weites Quantenkommunikationsnetzwerk etabliert.

Abstract

As a cornerstone for data autonomy, data security has become a fundamental necessity. With regards to the public sector and critical infrastructures, it safeguards economic competitiveness and sustainable national security. Technological breakthroughs in the form of quantum computers threatens our current encryption methods, therefore, developments of novel encryption technologies and systems that are proven to be “quantum-safe” are necessary. The importance of

data security is underpinned by the 10-years research and innovation program “EuroQCI Quantum Communication Infrastructure”. Building on the long research experience of Austrian institutions in the field of quantum technologies, the project QCI-CAT aims at an adoption of modern encryption technology based on QKD (Quantum Key Distribution) for highly secure communication between public authorities. For this purpose, a QKD demonstration network will be installed in Vienna, which will connect the Federal Chancellery (BKA) as a central node with three other federal ministries BMLV, BMEIA and BMK. Building on a close cooperation between research partners and industrial companies, QCI-CAT will investigate and verify new security applications for public authorities, such as secret sharing and message authentication. Close cooperation between stakeholders ensures that the development of QKD-based security technology is driven from viewpoint of an IT end-user. QCI-CAT will also leverage a test and demonstration infrastructure to research new technological approaches such as the combination of post-quantum encryption technology with QKD, long-distance QKD with secured trusted nodes and field trials of quantum repeaters. Moreover, the results of QCI-CAT will constitute the basis for the strong positioning of Austria within the European EuroQCI initiative. The outcomes will also be shared with other neighboring countries and built upon with planning of cross-border links for a fully connected EuroQCI.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- CANCOM Austria AG
- dacoso GmbH
- fragmentiX Storage Solutions GmbH
- Medizinische Universität Graz Diagnostik- und Forschungsinstitut für Pathologie
- Quantum Technology Laboratories GmbH
- SBA Research gemeinnützige GmbH
- Technische Universität Graz Institute of Information Security (ISEC)
- Universität Innsbruck Institut für Experimentalphysik
- X-Net Services GmbH