Quantum Key Distribution

Quantum key distribution for tap-proof communication

The rapid development of quantum computers is fundamentally reshaping the foundations of cybersecurity. As traditional encryption methods such as RSA will soon become easily vulnerable, quantum physics opens new ways to make data connections virtually impenetrable. Quantum Key Distribution (QKD) uses the laws of quantum mechanics—particularly the phenomenon of entangled photons—to transmit symmetric keys in a way that makes any interception attempt immediately detectable. Austria, with decades of pioneering research, holds a leading international position in this field. The AIT Austrian Institute of Technology has consolidated this expertise and played a decisive role in major European quantum communication initiatives.

Quick Facts

- Solution area: **Organisations, Processes, Technological innovation**
- Administrative level: **State, Federation**
- Solution process: **Digitization and technology, Public service, Science and research, Security and defense**
- Technology: **Information technology, Networks**

How it works

QKD enables the generation and transmission of cryptographic keys via optical fibers or, in the future, via satellites—protected by fundamental physical principles. If a photon is intercepted or manipulated during transmission, its quantum state changes instantly. This makes attacks measurable and prevents undetected eavesdropping. The keys are then used for symmetric data encryption, while the key exchange itself remains perfectly secure. AIT plays a central role in this development. The institute participated in the early experiments of Nobel Prize laureate Anton Zeilinger, whose groundbreaking 2004 demonstration of QKD between a Viennese bank and City Hall laid the foundation for today's advances. Building on this legacy, AIT accumulated extensive scientific expertise and assumed leading roles in European flagship projects such as OpenQKD, UNIQORN, CiViQ, and QUARTZ. While OpenQKD created a Europe-wide testbed for quantum communication, UNIQORN succeeded in miniaturizing a fully functional QKD transmitter onto a 2×4 mm photonic chip—an essential step toward widespread commercial adoption. In the coming years, hardware-based QKD protocols will operate in parallel with software-driven post-quantum cryptography until a complete end-to-end quantum communication infrastructure (EuroQCI) is deployed across Europe. Austria is already a frontrunner: Through national KIRAS projects like QKD4GOV and QCI-CAT, the first operational quantum networks for highly secure authorities and healthcare communication are taking shape. AIT's participation in the QUARTZ project also enables the extension of terrestrial QKD through satellite-based links, ensuring global reach beyond current fiber limitations.

The Big Picture

QKD represents a strategic paradigm shift—from purely mathematical cryptography to security guaranteed by the laws of physics. For governments, critical infrastructure operators, network providers, cloud platforms, research institutions, and enterprises, this creates an entirely new level of protection. Europe thus strengthens its digital sovereignty in a future where quantum computers can break established encryption methods. Through close collaboration between research, industry, and public administration, Europe has accelerated knowledge transfer, standardisation, interoperability, and the development of new production capabilities. Austria and its European partners can now build ultra-secure governmental networks while also pioneering cost-effective miniaturised QKD components for future mass-market applications. From secure

health data to interconnected public-sector processes and global communication systems, new ecosystems, skills, and technology-driven jobs are emerging along the entire value chain. QKD is therefore much more than a security solution: It is a European technology catalyst—linking scientific excellence, industrial innovation, and governmental sovereignty—positioning Europe at the forefront of the global quantum communication race.

aed – Agency for Economic Cooperation and Development
Ferdinandstraße 4,
1020 Vienna, Austria

+43 (1) 448 00 55 10
platform@bestpracticeaustria.at