

PRESS RELEASE

Klosterneuburg/Austria, December 10, 2020

MEDICAL DATA SUCCESSFULLY PROTECTED BY QUANTUM-CRYPTOGRAPHY IN GRAZ

Sharing sensitive medical data between doctors at different hospitals is essential to improve the quality of diagnosis and treatment and demands special efforts to protect patients' rights and privacy. Within the framework of the EU project 'OpenQKD', the technical implementation and usability of such a cooperation was proven in the use case 'Medical Data Protection Graz'. By combining the two state of the art technologies fragmentiX CLUSTER and QKD equipment, the setup in Graz provides the highest level of security for the data while maintaining ease of use. *Information theoretic security (ITS)* for data at rest – stored in fragments – is provided by the fragmentiX Secret Sharing implementation, while the use of quantum key distribution (QKD) is protecting the data fragments with quantum safe symmetric encryption during transmission between the hospitals and the external S3 storage locations. Within the EU project OpenQKD, fragmentiX Storage Solutions GmbH cooperates with 37 partners, in order to move closer towards a pan-European quantum-safe digital infrastructure.

Klosterneuburg/Austria, December 10, 2020 (fragmentiX) – The use case 'Medical Data Protection Graz' for quantum key distribution (QKD) in the framework of the EU-project OpenQKD is successfully proving the highest possible protection of the most sensitive data imaginable, medical records. Together with the Medical University Graz, the Hospital (Landeskrankenhaus) Graz II, fragmentiX and its partners managed to successfully set up the QKD and encryption hardware.

Pathologists from both institutions were enabled to exchange (mutually upload and retrieve) medical records and images securely. In each of the two connected institutions the data is split by a fragmentiX CLUSTER node into three fragments. Two of them are transmitted securely to different datacenters, run by Citycom Graz, protected by QKD. The third fragment is sent to a traditionally https-protected storage – simulating a commercial public S3 storage – located at Medical University Graz but reachable from both institutions. ITS is achieved by fragmentiX Secret Sharing, which renders a single fragment useless and protecting the transmission of two (out of three) fragments, using QKD.

This use case demonstrates secure data sharing of digital histological slides (up to 10 GB/image; big amounts of data), supplied by the Biobank Graz, linked with clinical and genetic data (highly sensitive data) between Medical University Graz and Hospital (Landeskrankenhaus) Graz II. The data sharing will enable harmonization and quality control of advanced diagnostics in context of personalized medicine and promote medical research.

“For fragmentiX - as the developer of quantum safe storage solutions - the fusion of security measures like quantum key distribution and fragmentiX Quantum Safe Storage Appliances is a perfect fit. While QKD protects the transfer of crucial information (data in transit), the fragmentiX products 'CLUSTER' and 'box' offer information theoretic security for data storage (data at rest)”, states fragmentiX CEO, Werner Strasser.

EU-Project OpenQKD

The ambition of the EU project OpenQKD, which is coordinated by AIT Austrian Institute of Technology, is to reinforce Europe's global position at the forefront of quantum communication capabilities. It aims

at demonstrating the transparent integration of quantum-safe solutions broadly across the European digital landscape cases to potential end-users and relevant stakeholders. The work in the OpenQKD project lays the foundations for rolling out a pan-European quantum-safe digital infrastructure, with a solid basis to educate and lead a quantum-aware workforce with engaged European research, SMEs and industry leaders. For fragmentiX OpenQKD is a perfect platform to foster its support for *digital sovereignty*.

What is quantum key distribution?

Quantum key distribution (QKD) provides a constant flow of secret digital cryptographic keys between two locations in a computer network. The security of QKD is based on single photons and their properties, which are transmitted using regular and existing optical fibers. The quantum nature of the photons themselves ensures that each attempt to intercept a QKD protected datalink – e.g. by reading or copying - changes their state and is therefore immediately detectable. This makes it impossible to compromise the key exchange without destroying the information for the intended receiver. For this reason, QKD is superior compared to other existing security solutions, especially in the view of future developments in quantum computing. As QKD is a very potent safety measure for data in transit, it is the perfect fit for fragmentiX Storage Appliances that provide *information theoretic security* for data storage in public or hybrid S3 buckets. Due to the still very high costs and limited physical distances between two points of a QKD connection, this technology has so far only been used to protect highly sensitive data in critical industries such as finance, critical infrastructure, defense and now beginning in healthcare.

Project partners for the realization of the use case

As official coordinator for this use case within OpenQKD, fragmentiX provided the Medical University Graz and the Hospital (Landeskrankenhaus) Graz II each with a fragmentiX CLUSTER system. The pathologists' workstations were setup to the specific needs for diagnosing with high resolution images and were provided by Medical University Graz for the experts in both institutions. Both institutions have fiber optic connections to two datacenters owned by the City of Graz's own ICT provider Citycom. Racks in both of those datacenters were equipped with 10 GB Cisco switches and Dell S3 storage units, both provided by fragmentiX.

With the help of experts from AIT Austrian Institute of Technology, the QKD and encryption hardware – provided by ID Quantique and ADVA – was assembled at fragmentiX headquarters at IST Austria Technology Park in Klosterneuburg. In early October, the setup was put in place to protect the connection between the institutions and Citycom's data centers in Graz. In the latter stages of the project, we are pleased to get the opportunity to use Toshiba's QKD components as well. The hardware provided by ID Quantique, Toshiba UK and ADVA, together with the fragmentiX Storage Appliances, meets the high security and privacy standards for medical data as well as GDPR requirements, while maintaining very high performance.

About fragmentiX

fragmentiX Storage Solutions GmbH is a privately owned Austrian IT Security company – with Digital Sovereignty as its passion. The headquarter is located in Klosterneuburg, 10 km outside of Vienna, Austria. With software, partially licensed from AIT Austrian Institute of Technology, fragmentiX is developing and producing Quantum Safe Storage Appliances to protect sensitive datasets in hybrid cloud storage environments for the global IT market. As DELL Technologies OEM partner fragmentiX can support its products around the globe. The main focus is to help customers protect their sensitive data in critical sectors such as medical, financial, and governmental. The in September 2020 founded subsidiary in Switzerland will mainly focus on new products for the personal/individual market.

Further inquiry notes:

Nadine Wallner

fragmentiX Storage Solutions GmbH
Digital Marketing & Sales Support
Phone: +43 2243 24203 110
nadine.wallner@fragmentix.com

www.fragmentix.com

Twitter: [@fragmentix](https://twitter.com/fragmentix)

LinkedIn: [fragmentiX Storage Solutions GmbH](#)

Links, pictures and further information:

OpenQKD image & document collection | <https://www.fragmentix.com/pressrelease/openqkd/downloads>

fragmentiX logo | http://erp.fragmentix.com/downloads/fragmentiX_logo.jpg

Partners

fragmentiX Storage Solutions GmbH: <https://www.fragmentix.com/>

AIT Austrian Institute of Technology: <https://www.ait.ac.at/>

EU-project OpenQKD: <https://openqkd.eu/>

Medical University Graz: <https://www.medunigraz.at/>

Hospital (Landeskrankenhaus) Graz II: <https://www.lkh-graz2.at/>

Citycom: <https://www.citycom-austria.com/>

ID Quantique: <https://www.idquantique.com/>

ADVA: <https://www.adva.com>

Toshiba: <https://www.toshiba.co.jp/qkd/en>