EUROPE BIOBANK WEEK 2021

TRUSTED DATA ENVIRONMENT FOR BIOBANKS AND OTHER SHAREHOLDERS INCLUDING PATIENTS

W. STRASSER[1], C. PACHER[1], K. ZATLOUKAL[2], and T. LORÜNSER[3]

1. fragmentiX Storage Solutions GmbH, Klosterneuburg, Austria
2. Digital Pathology, Medical University Graz, Graz, Austria
3. Center for Digital Safety & Security, AIT Austrian Institute of Technology GmbH, Vienna, Austria

fragmentiX® QUANTUM SAFE STORAGE SOLUTIONS

INTRODUCTION

Medical imaging and genome sequencing produce huge amounts of sensitive medical data that must be shared among authorized stakeholders, e.g. research institutions, and at the same time protected against unauthorized abuse.

- To enable seamless integration this data must be easily accessible on demand.
- Furthermore, it must be secure on transit and on rest against current and future cyberattacks even by quantum computers.

AIM

The performance and privacy needs of modern biobanks and their stakeholders ask for a **state-of-the-art, cryptography based, quantum-safe IT solution that is compatible with GDPR and other legal requirements.**

- We present such a novel IT solution based on threshold cryptography (secret sharing), distributed cloud data storage, and optionally including quantum key distribution (QKD) and post-quantum cryptography (PQC).
- We also report on a field trial that demonstrated the feasibility of the approach.

METHOD

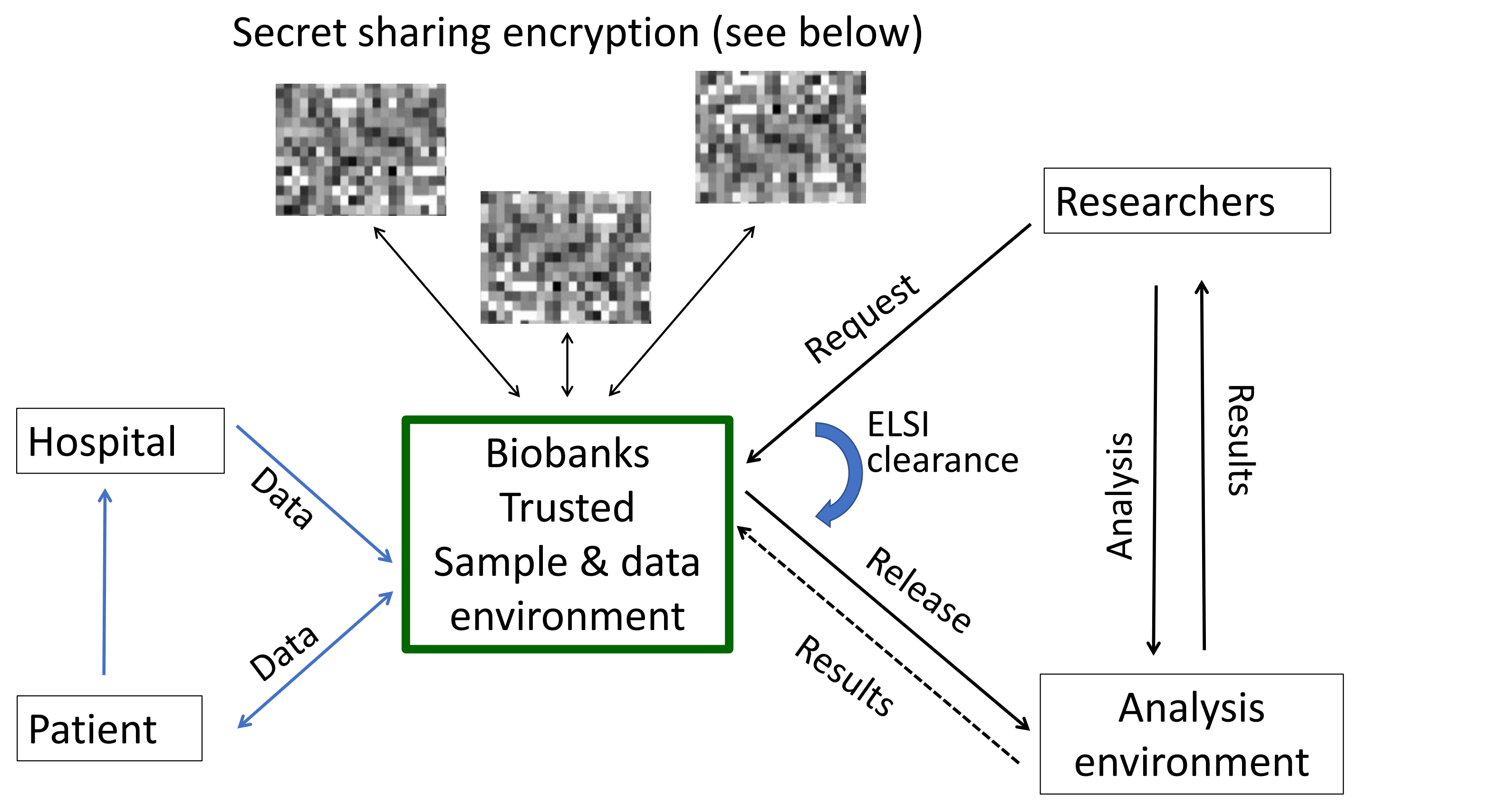
Secret sharing is about splitting data into "fragments" …

- The user chooses how many fragments are created in total and the minimum number of fragments needed to recover the data.
- Shamir's secret sharing algorithm [1] guarantees that
  - Any set of less than the minimum number of fragments contains no information on the data
  - Any set of at least the minimum number of fragments contains the full information

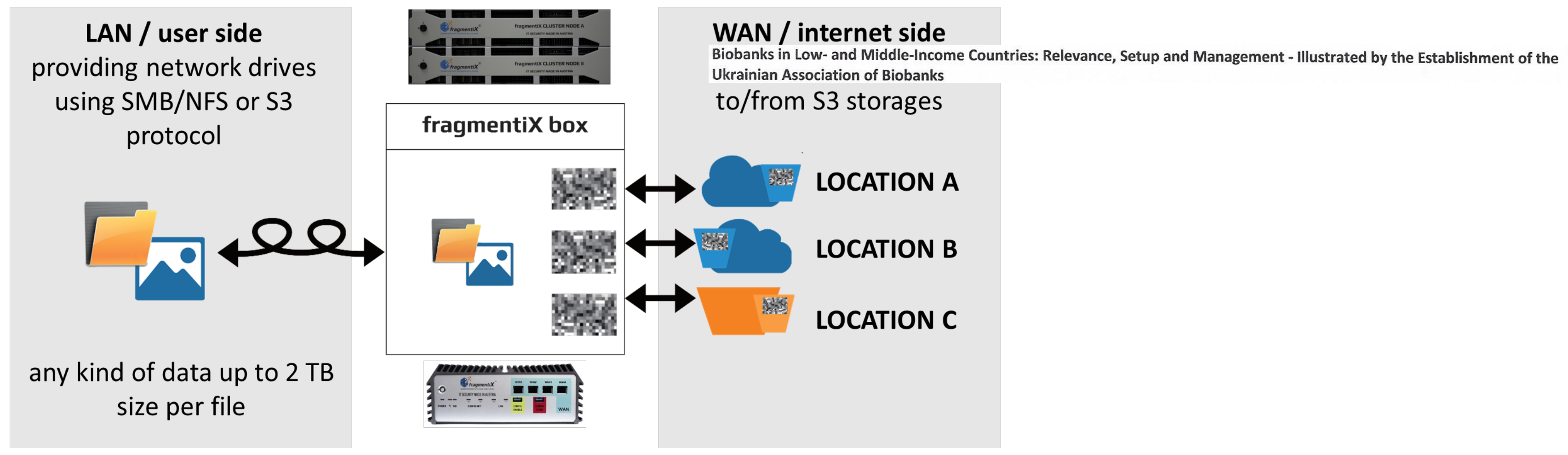
Distributed and/or federated storage…

- By distributing fragments to different public/private/hybrid cloud storage locations fragmentiX® CLUSTER guarantees that the **data is protected from data loss and data theft.**

RESULTS


Secret sharing encryption (see below)
Researchers
Request
ELSI clearance
Hospital
Data
Biobanks Trusted Sample & data environment
Analysis
Results
Release
Results
Data
Patient
Analysis environment
MPC, Federated machine learning

Schematic of future trusted medical data environment [3]


LAN / user side
providing network drives using SMB/NFS or S3 protocol
any kind of data up to 2 TB size per file
fragmentiX box
WAN / internet side
Biobanks in Low- and Middle-Income Countries: Relevance, Setup and Management - Illustrated by the Establishment of the Ukrainian Association of Biobanks
to/from S3 storages
LOCATION A
LOCATION B
LOCATION C

Schematic of fragmentiX secret sharing (see also METHOD box)

RESULTS

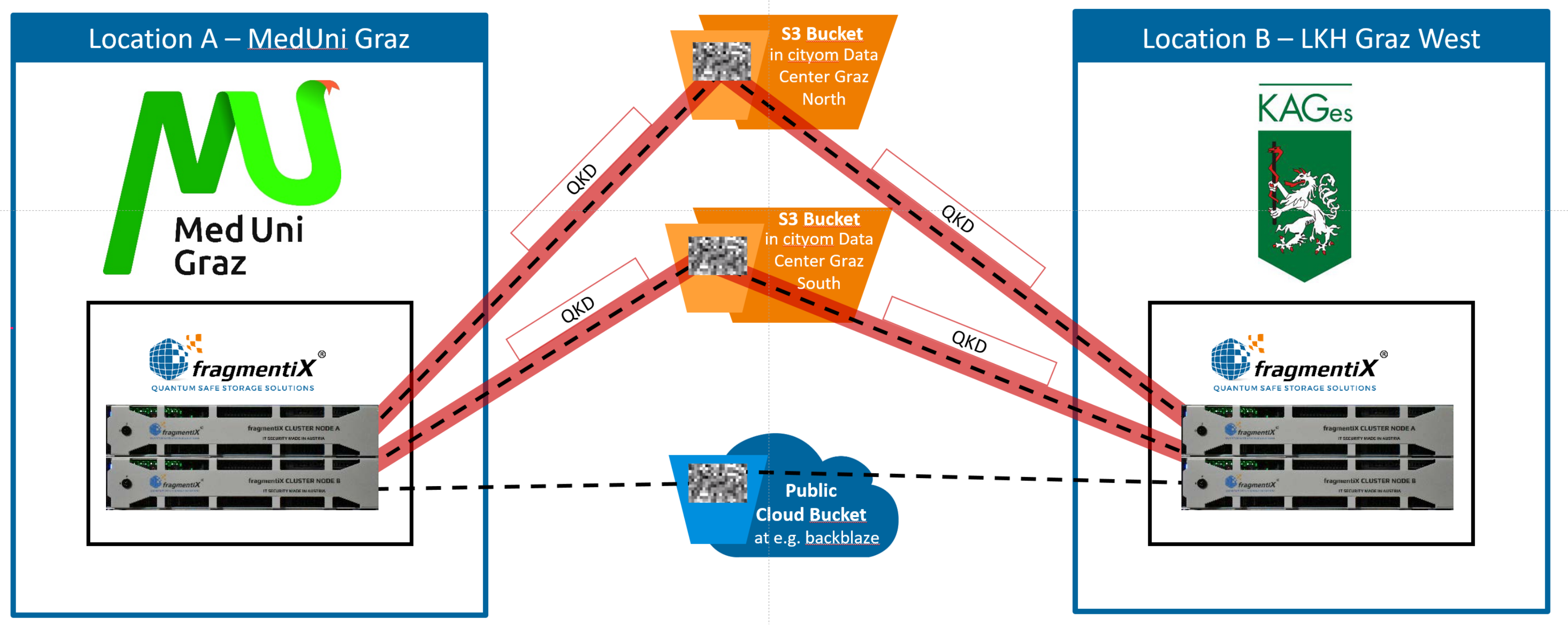
OpenQKD Medical Use-Case Graz:

In the framework of the EC funded project OpenQKD [2] a medical use-case was demonstrated in Graz during 2020/2021:

Pathologists from Medical University Graz and Hospital Graz West were enabled to exchange (mutually upload and retrieve) medical records and images securely.

Quantum-safe security (the system cannot be broken with future quantum computers) was achieved by

- fragmentiX secret sharing, which renders a single fragment useless
- protecting the transmission of two (out of three) fragments with QKD.


Location A – MedUni Graz
Med Uni Graz
fragmentiX®
QUANTUM SAFE STORAGE SOLUTIONS
S3 Bucket in cityom Data Center Graz North
S3 Bucket in cityom Data Center Graz South
QKD
QKD
QKD
QKD
Public Cloud Bucket at e.g. backblaze
Location B – LKH Graz West
KAGes
fragmentiX®
QUANTUM SAFE STORAGE SOLUTIONS

OpenQKD EU project UseCase Graz: Schematics of secure IT infrastructure.

CONCLUSIONS

Secret sharing can help biobanks to store sensitive data in public clouds:

- **Data loss protection** is ensured by the fact that not all shares are needed to fully recover the data.
- **Data theft protection** is ensured by the fact that too few shares contain zero information on the data. A breach in one cloud storage does not compromise the data at all.
- **Optimal user experience: Seamless integration** of fragmentiX Secret Sharing into Windows Explorer / macOS Finder.

Outlook: fragmentiX secure multi party computation (SMPC)

- will allow the in-depth processing of medical data sets owned by different parties with cryptographic guarantee for all parties that the own data is not disclosed to the other cooperating parties (e.g. to train AI algorithms in the fields of medical diagnosis and research)

REFERENCES

[1] Shamir, Adi (1979), "How to share a secret", Communications of the ACM, 22 (11): 612–613, doi:10.1145/359168.359176

[2] https://openqkd.eu

[3] Biobanks for enabling research and development by trusted patient data environment, Springer, 2021.

ACKNOWLEDGEMENTS

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857156 (OpenQKD).

CONTACT INFORMATION

Werner Strasser

CEO, fragmentiX Storage Solutions GmbH

+43 664 325 8896
ws@fragmentix.com
IST Park
Plöcking 1
3400 Klosterneuburg
Austria