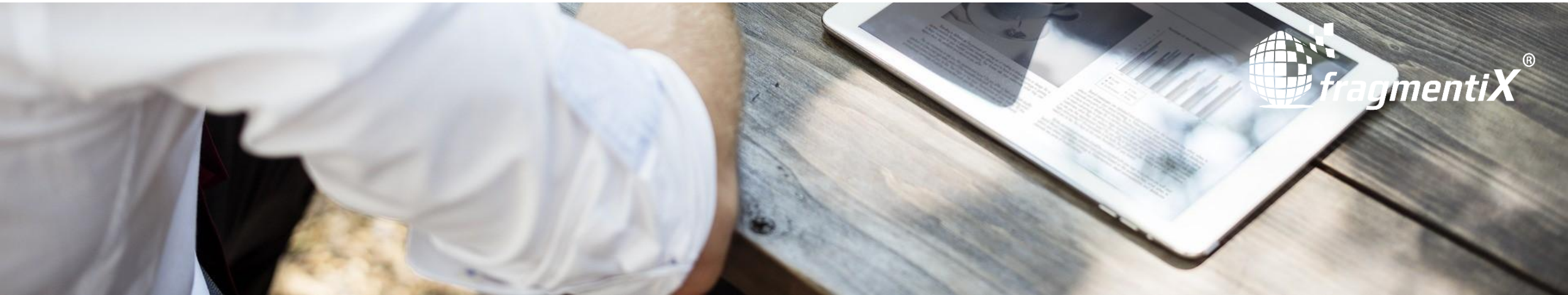
fragmentiX®

QUANTUM AGE CYBERSECURITY

Introducing fragmentiX data in transit, data at rest - Your Data Sovereignty -



Digital Sovereignty is our Vision, our Mission, our Passion

fragmentiX®
QUANTUM AGE CYBERSECURITY

fragmentiX empowers
every person, every company, every state
in effectively protecting their digital
knowledge and data assets
against asymmetric hybrid warfare,
data theft and industrial espionage.

Werner Strasser
Founder & CEO, fragmentiX

About fragmentiX

- Austrian cybersecurity company since 2018
- Cutting-edge technology „first of its kind“ globally
- Developer and producer of appliances for quantum-safe data sovereignty based on secret sharing

Digital Sovereignty is Our Vision, our Mission, our Passion

Fact sheet

fragmentiX®
QUANTUM AGE CYBERSECURITY

History

Austrian cybersecurity company since 2018

Project

biobanks

protected medical data exchange and safe backup in the clouds

Global Technology Partners

TOSHIBA
SEP The Data Protection Company
groq
CONNECT4VIDEO
MIRACL
MAXELER a groq company
Zatloukal Innovations
UNITED ACCESS anytime-anywhere
portal26
DELL Technologies

Research

OpenQKD project

Medizinische Universität Graz
TOSHIBA
IDQ

CVStar project

QUARTER project

CVStar
QUARTER

QCI-CAT project

ESA SAGA project

QCAT
SAGA-1G
esa

THE 'NEW' GLOBAL COMPETITIVE MODEL

ASYMMETRICAL HYBRID WARFARE

THE MODERN BATTLEFIELD IS EVERYWHERE

UNRESTRICTED WARFARE

NON-MILITARY	TRANS-MILITARY	MILITARY
Economic Warfare*	Espionage Warfare*	Biological Warfare
Financial Warfare*	Information Warfare*	Chemical Warfare
Transaction Warfare*	Intelligence Warfare*	Ecological Warfare
Trade Warfare*	Industrial Warfare*	Space Warfare & EMP
Resources Warfare*	Resources Warfare*	Electronic Warfare
Regulatory Warfare*	Pirating Warfare*	Guerrilla Warfare
Legal Warfare*	DarkNet Warfare*	Terrorist Warfare
Education Warfare*	Smuggling Warfare*	Conventional Warfare
Technological Warfare*	CYBER WARFARE**	Kinetic 'Smart' Warfare
Sanction Warfare	Drug Warfare*	Nuclear Warfare
Media Warfare	Infiltration Warfare*	
Propaganda Warfare	Deterrence Warfare*	
Culture Warfare	Psychological Warfare	
Ideological Warfare	Diplomatic Warfare	
Religious Warfare	Subversion Warfare	
Poisioning Warfare	Environmental Warfare	

"ANYTHING WARFARE" ABSENT OF ANY RULES

** Cyber Warfare functions as the key accelerator to all hybrid warfare methods

* Related to Economic and Transaction Warfare

BLACKOPS PARTNERS

SPECTRE®

Threats of Quantum Computer

fragmentiX®
QUANTUM AGE CYBERSECURITY

Today, even with supercomputers, it **takes too long** to crack asymmetric encryption!

which until today we consider it's safe

QUANTUM COMPUTERS = GAME CHANGER

Already available to governments worldwide and large internet corporations they will **only need a few seconds** for cracking "asymmetric encryption"

P W Shor "Polynomial Time Algorithms for prime Factorization and Discrete Logarithms on a Quantum Computer" SIAM Journal on Computing no 5 p. 1484

Threats of Quantum Computer

How long does it take to crack Asymmetric Encryption?

Computers today: 8.000.000.000.000.000.000.000 years

Quantum Computers: 100 seconds

P W Shor “Polynomial Time Algorithms for prime Factorization and Discrete Logarithms on a Quantum Computer” SIAM Journal on Computing no 5 p. 1484

Current Risks and Average Costs per Cyber Incident

fragmentiX®
QUANTUM AGE CYBERSECURITY

RISKS	PROBABILITY	AVG COSTS
1. Data Breach	27.9% - 34.5%	$3.86 million
2. Ransomware	22.1% - 28.4%	$11.5 million
3. Insider Threat	18.2% - 24.5%	$11.45 million
4. Phishing	32.1% - 43.8%	$3.86 million
5. DoS/DDoS	14.5% - 20.6 %	$2.5 million

Source: Multiple Leading Industry Reports 2020-2024

Cloud storage risks – Governments

fragmentiX®
QUANTUM AGE CYBERSECURITY

The USA Clarifying Lawful Overseas Use of Data Act (US CLOUD Act, 2018)

The USA CLOUD Act (2018) has significant implications for cloud data security. It allows country-specific governments to access data stored by US-based cloud providers.

The CLOUD Act primarily amends the Stored Communications Act (SCA) of 1986 to allow federal law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil.

Cloud storage risks – Governments

1.4 Data Privacy. You may specify the AWS regions in which Your Content will be stored. You consent to the storage of Your Content in, and transfer of Your Content into, the AWS regions you select. We will not access or use Your Content except as necessary to maintain or provide the Services, **or as necessary to comply with the law or a binding order of a governmental body.** We will not (a) disclose Your Content to any government or third party or (b) move Your Content from the AWS regions selected by you; **except in each case as necessary to comply with the law or a binding order of a governmental body. Unless it would violate the law or a binding order of a governmental body**, we will give you notice of any legal requirement or order referred to in this Section 1.4. We will only use your Account Information in accordance with the Privacy Notice, and you consent to such usage. The Privacy Notice does not apply to Your Content. **Extract from: AWS, Customer Agreement 2025**

In clear:

You will never know, when, how often, and who is / will be abusing your data on the cloud, which includes, but is not limited to:

Intellectual property (IP), tenders, patents, trade secrets, personal medical records, financial assets, board meeting protocols, …

heise online

Ex-CIA-Direktor bestätigt Wirtschaftsspionage mittels Echelon

12.03.2000 21:40 Uhr Florian Rötzer

Gegenüber europäischen Vorwürfen führte James Woolsey als Rechtfertigung an, Europe habe eine "Kultur der Bestechung".

Der ehemalige CIA-Direktor James Woolsey sagt, die Wirtschaftsspionage der USA würde auf "Bestechungsaktionen der Europäer " zielen. Bei einer Pressekonferenz vor ausländischen Journalisten in Washington rechtfertigte der ehemalige CIA-Direktor US-Aufklärung "mit Spionage, durch Abhören, durch Aufklärungssatelliten" damit, dass Europa eine "Kultur der Bestechung" habe, wenn es darum gehe, internationale Großaufträge zu erhalten.

Er bezog sich auf den kürzlich dem Europaparlement vorgestellten Bericht "Interception Capabilities 2000", der unter anderem Informationen über angebliche US-Wirtschaftsspionage mittels des Satellitenüberwachungssystems Echelon enthält. Er bescheinigte dem Bericht "intellektuelle Aufrichtigkeit", behauptete aber, bei den zwei im Bericht zitierten Fällen sei es um Bestechung gegangen. Seiner Meinung nach sei das aber keine Wirtschaftsspionage. "Ich reserviere den Begriff Wirtschaftsspionage dafür, wenn einer Industrie direkte Vorteile verschafft werden sollen. Ich nenne es nicht Wirtschaftsspionage, wenn die USA ein europäisches Unternehmen ausspionieren, um herauszufinden, ob es durch Bestechung Aufträge in Asien oder Lateinamerika zu erhalten versucht, die es auf ehrlichem Weg nicht gewinnen würde", sagte Woolsey.

Die USA hätten wenig Bedarf an High-Tech-Spionage , da "die amerikanische Industrie in vielen Bereichen technologisch weltführend ist". Doch die "Kultur der Bestechung", die es in Europa gäbe, und die Hilfe, die europäische Unternehmen von ihren Regierungen erhalten, legitimieren laut Woolsey die US-amerikanischen Spionageaktivitäten.

Mehr in Telepolis: **Spionieren gegen "Kultur der Bestechung"** [1]. (fr [2])

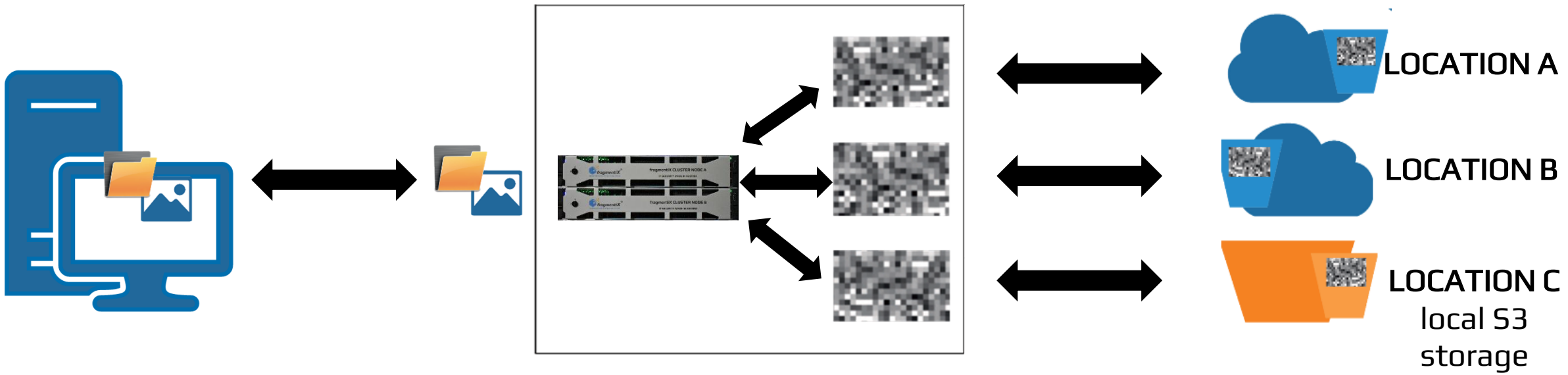
URL dieses Artikels:

`https://www.heise.de/-20861`

fragmentiX®
QUANTUM AGE CYBERSECURITY

Wird unter der DJT ....

frX Quantum-Safe Cybersecurity Technology Snapshot



fragmentiX Secret Sharing Technology – WRITE

fragmentiX®
QUANTUM AGE CYBERSECURITY

End-User side / LAN
Network drive
WebDAV
S3

fragmentiX Appliance
3 to 26 fragments
built-in local AES-256
optional encryption

fragmentiX CLUSTER

QKD
DSKE
PQC

fragments in transit

3-26 WAN/LAN Storages
S3 storages
NFS mounts
USB drives

fragments at rest

LOCATION A
LOCATION B
LOCATION C
local S3 storage

Data is written on network drive or object storage

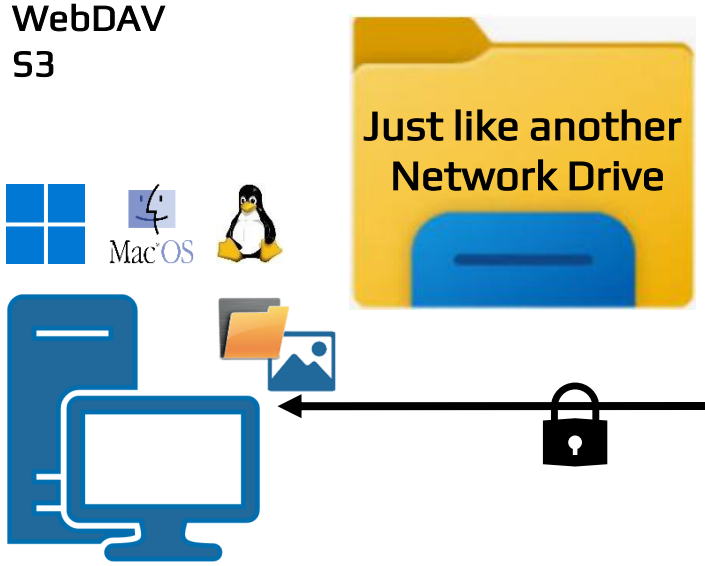
Data is cryptographically shredded in fragments

Fragments are stored in separate physical storage locations off/on cloud

fragmentiX Secret Sharing Technology - READ

End-User side / LAN

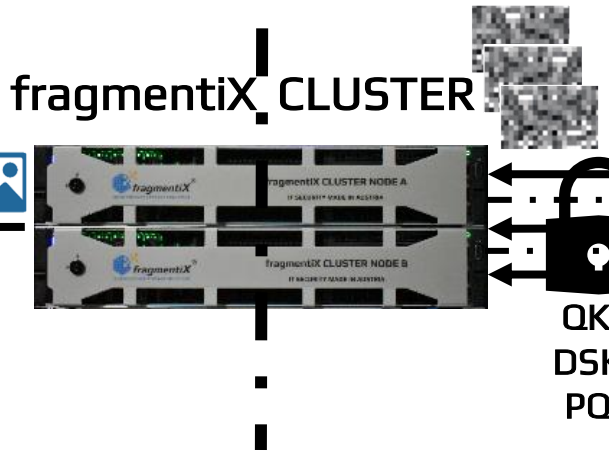
Network drive
WebDAV
S3



fragmentiX Appliance

3 to 26 fragments

built-in local AES-256 optional encryption

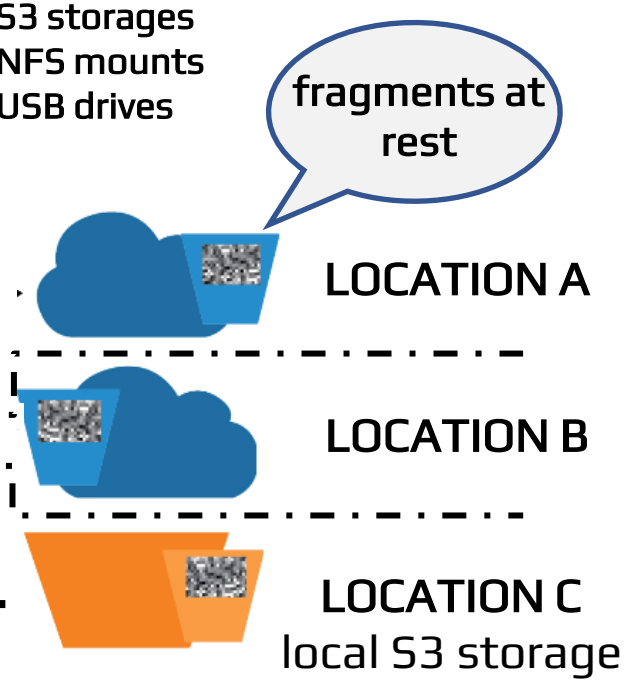


fragments in transit

QKD
DSKE
PQC

3-26 WAN/LAN Storages

S3 storages
NFS mounts
USB drives



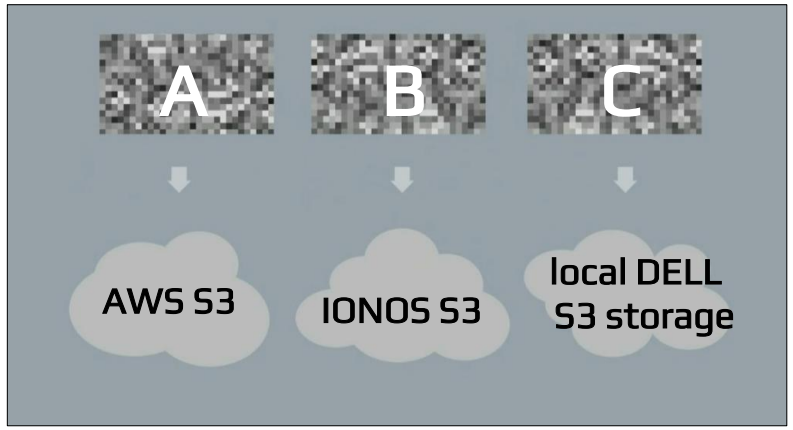
User reads data from network drive/virtual object storage

Data is re-assembled and combined from fragments

Fragments read at separate physical storage locations

fragmentiX Quantum Safe Sovereignty – ITS !

LOCATIONs



Each fragment is stored in its own public cloud or local S3/Azure/NFS/USB storage location.

Only the owner of the frX appliance knows where all the LOCATIONs are.

Should 1 fragment be stolen/hacked:
it is absolutely useless to the data thief/spy as fragmentiX Secret Sharing enables you to store data with ITS:
ITS – Information-Theoretical Security
Not even unlimited future quantum computing power has a chance to break it!

fragmentiX Quantum Safe Sovereignty – ITS !

fragmentiX®
QUANTUM AGE CYBERSECURITY

WIKIPEDIA
The Free Encyclopedia

Information-theoretic security | Search

Information-theoretic security

9 languages

Contents hide

(Top)
Overview
Physical layer encryption
Technical limitations
Secret key agreement
See also
References

Article Talk | Read Edit View history Tools

From Wikipedia, the free encyclopedia

A cryptosystem is considered to have **information-theoretic security** (also called **unconditional security**[1]) if the system is secure against adversaries with unlimited computing resources and time. In contrast, a system which depends on the computational cost of cryptanalysis to be secure (and thus can be broken by an attack with unlimited computation) is called computationally secure or conditionally secure.[2]

Overview [edit]

An encryption protocol with information-theoretic security is impossible to break even with infinite computational power. Protocols proven to be information-theoretically secure are resistant to future developments in computing. The concept of information-theoretically secure communication was introduced in 1949 by American mathematician Claude Shannon, one of the founders of classical information theory, who used it to prove the one-time pad system was secure.[3] Information-theoretically secure cryptosystems have been used for the most sensitive governmental communications, such as diplomatic cables and high-level military communications.[*citation needed*]

Strategic cooperations – DELL OEM Hardware

fragmentiX CLUSTERs are built by DELL under a global OEM partnership to frX specs within the EU (Poland). This provides for 5 years of worldwide mission critical support on customers' premises:

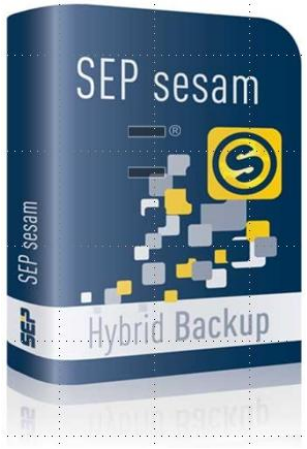
- Every frX CLUSTER customer is under a four (4) hours around the globe hardware repair / replacement response time.
- Sensitive CLUSTER parts, like SSDs, always stay at the customer premises.
- All security-related components and the frXOS operating system are installed by frX, DELL has no access to any IP held by frX.

Strategic cooperations – secunet

As a trusted partner of Germany-based secunet, fragmentiX provides customers:

- EGovernment-grade network encryption and ultra-secure clients
- More than 250,000 installations in 25 countries worldwide
- Approved by German BSI, EU and NATO for classified communication up to SECRET
- Designed for complex national and international infrastructures
- Central security and network management

Strategic cooperations – Backup & Disaster Recovery



As a worldwide partner of Germany-based SEP, fragmentiX provides customers:

- An enterprise approach to fully automated backups & recovery on all platforms
- SEP sesam is fully compatible and certified with all frX Quantum Safe Sovereignty Technology Appliances
- sesam's servers can run on Windows & Linux
- frX customers interested in SEP sesam, qualify for special deployment conditions

Usecase- Regional SME Cyber-Security Support

fragmentiX®
QUANTUM AGE CYBERSECURITY

Existing customer network	New hardware at the customer	Cloud infrastructure

Server 1 SEP

PC 1 SEP

PC 2 SEP

... SEP

PC 10 SEP

DELL T40 Microserver
at customer site with
60 TB harddrive and
SEP sesam backup software

SEP

fragmentiX®
QUANTUM AGE CYBERSECURITY

fragmentiX ONE Appliance

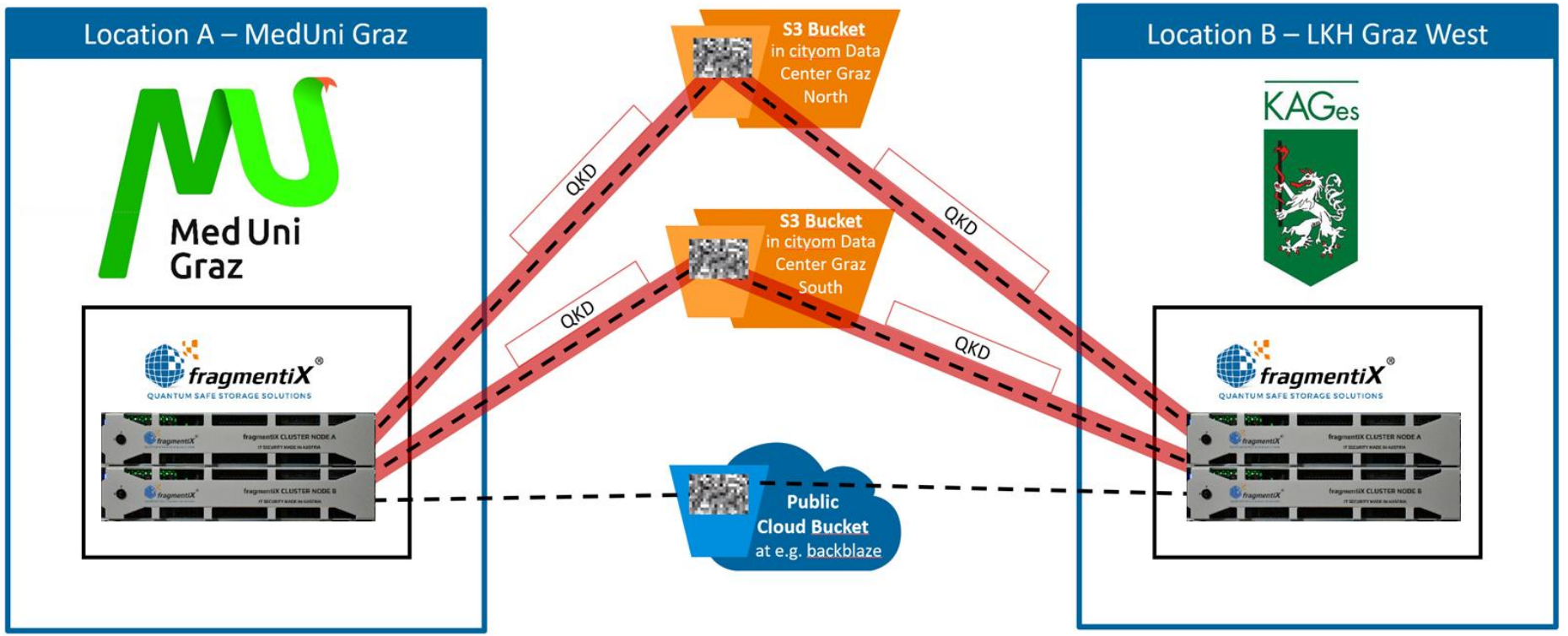
S3 Bucket at **storage provider 1**

S3 Bucket at **storage provider 2**

S3 Bucket at **storage provider 3**

IMMUTABLE TREE storage LOCATIONS
* Regional cloud storage providers should be selected individually, taking into account local initiatives to strengthen SME data protection & cybersecurity. Local value creation, paid fees should stay in the region where possible.

Usecase- Protecting the Most Sensitive Medical Data



OPEN QKD

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

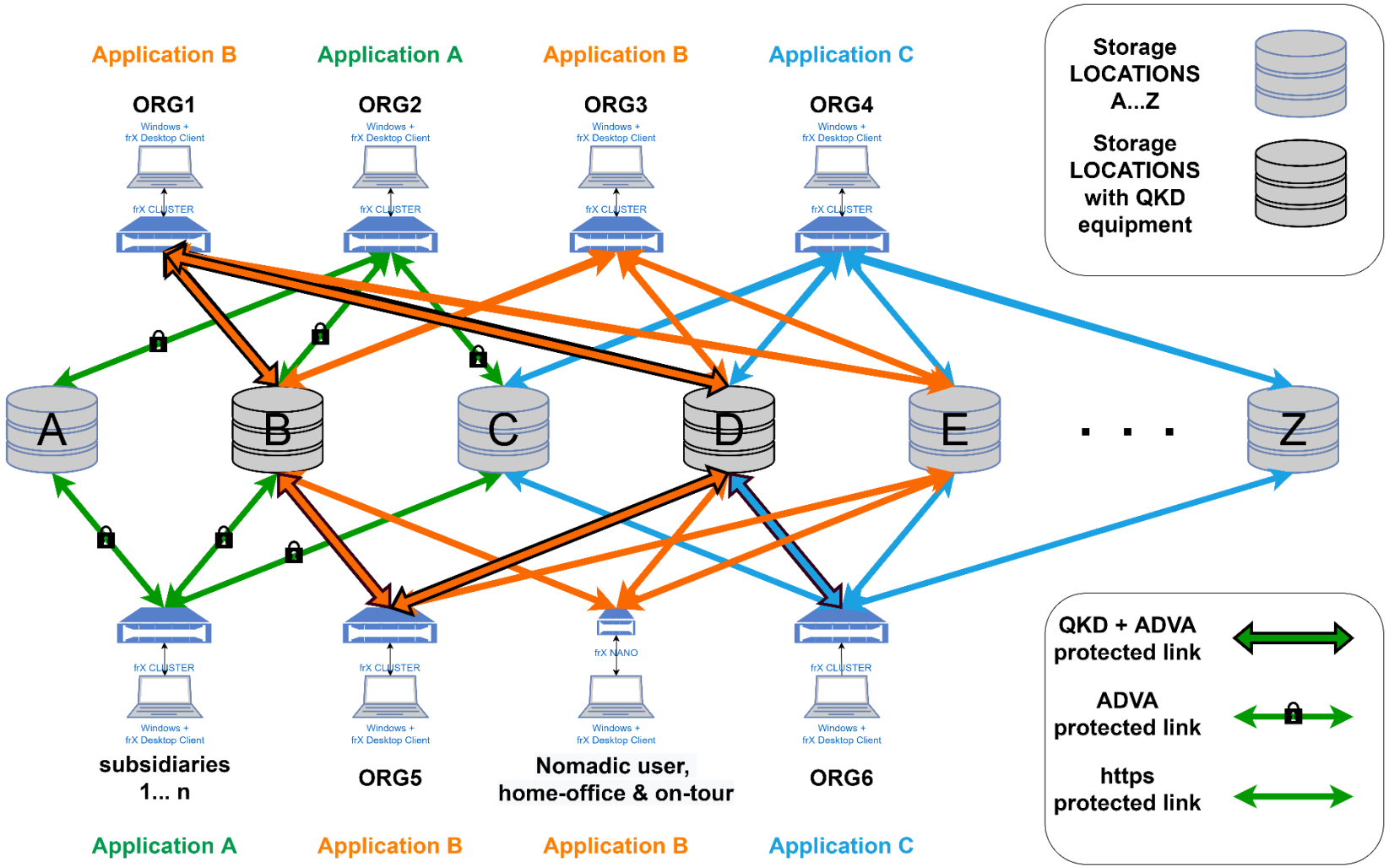
Usecase- fragmentiX and QKD for Fortune 500 / Gov / Mil

fragmentiX®
QUANTUM AGE CYBERSECURITY

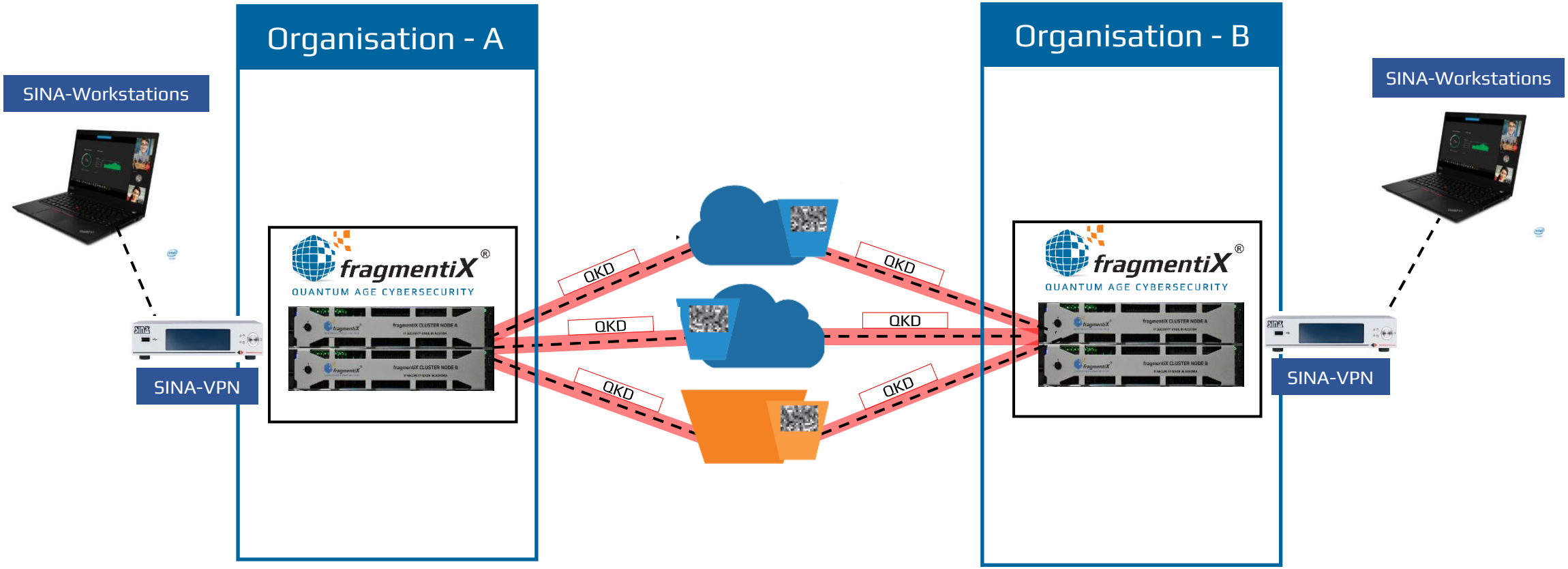
Application A:
data protection at rest via fragmentiX,
data protection on transit via ADVA encryptors at ORG2 plus subsidiaries and storages A, B, C

Application B:
data protection at rest via fragmentiX,
data protection on transit partly via QKD

Application C:
data protection at rest via fragmentiX
https protected on transit, a single link QKD protected



SINA + fragmentiX + QKD for sharing data across organisations



Usecase- Long Distance QKD with frX Trusted Repeater Nodes

fragmentiX®
QUANTUM AGE CYBERSECURITY

Trusted QKD Nodes:
Tamperproof repeaters to allow QKD links over long distances

Selected fragmentiX Cutting-Edge Projects

fragmentiX®
QUANTUM AGE CYBERSECURITY

Government

Bundeskanzleramt

KIRAS Sicherheitsforschung

Federal Ministry
European and
International Affairs
Republic of Austria

Smart FOX

UNSER HEER

EU

OPEN QKD

Medizinische Universität Graz

QCI4EU QSAFE

QCAT

QUANTERA

esa

SAGA-1G

QUARTER

CVStar

Global

BBMRI-ERIC®

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

GEORGETOWN UNIVERSITY
School of Medicine

Innophore

TOSHIBA

Lend AI DC – Austrian/EU Sovereign AI data centre

- Austrian private consortia – led by fragmentiX
- Full control over technical stack using finest DELL
- hardware UNDER AUSTRIAN ONLY CONTROL
- Goal to foster sensible AI usage for all of Austria – and surrounding likeminded countries
- Less than 300 meters between 25 MW hydro-energy, cooling river and high security data center
- Buildings exist, POC with MoD running
- EU-RESTRICTED by design

About fragmentiX

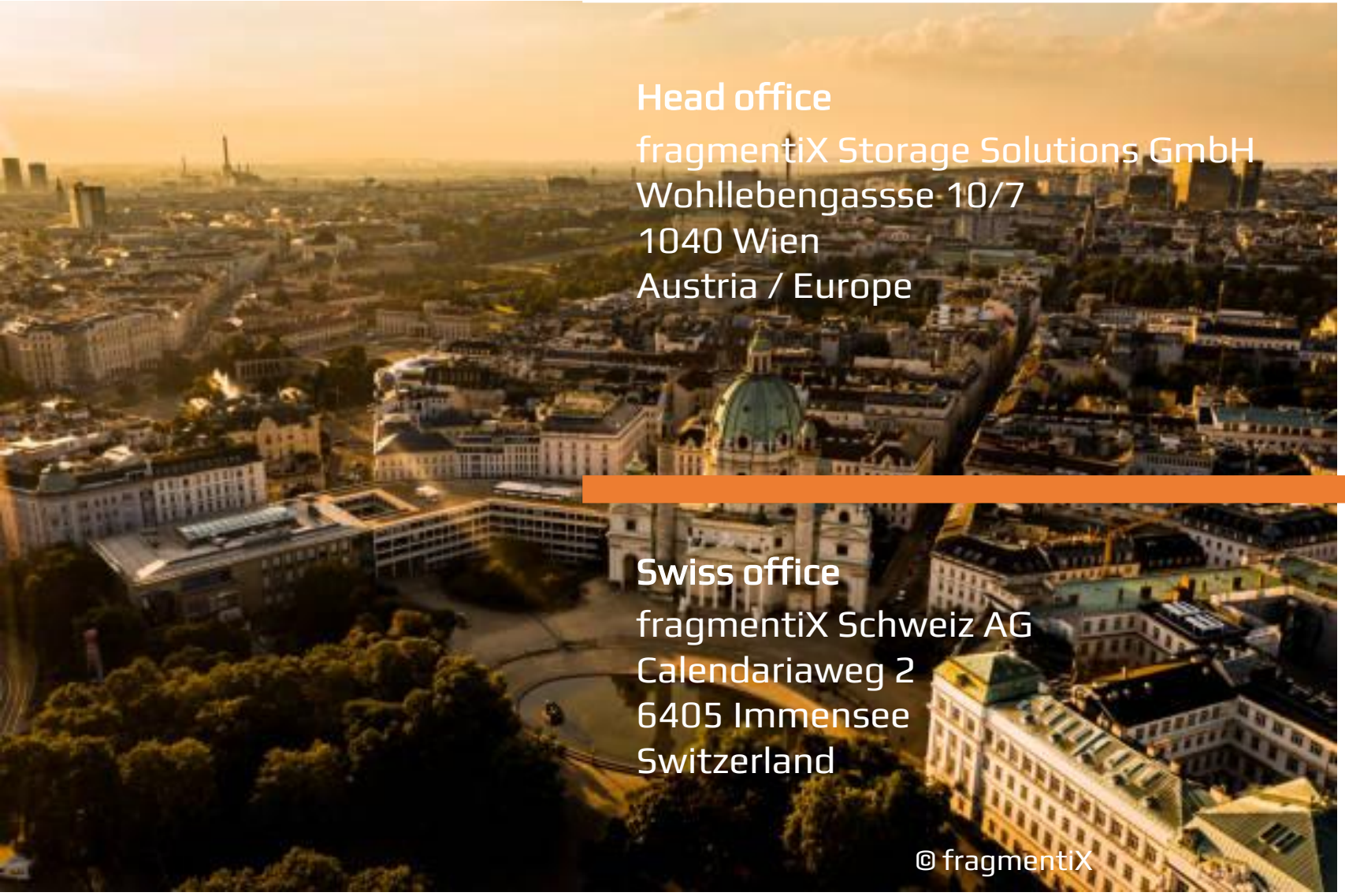
- Austrian cybersecurity company since 2018
- Cutting-edge technology „first of its kind“ globally
- Developer and producer of appliances for quantum-safe data sovereignty based on secret sharing

Digital Sovereignty is Our Vision, our Mission, our Passion

Lend AI DC – Austrian/EU Sovereign AI data centre

- Kooperationszusagen der Sicherheitsressorts
- Bundeskanzleramt: aktueller Stand wird laufend kommuniziert
- BRZ: Volle Kooperationszusage der Geschäftsführung
- BMLV: Audit der KI Nutzung der LVAk via frX@Lend, POC mit drei Abteilungen seit August 2025 sowie über bestehende Kooperationen mit fragmentiX und Zatloukal Innovations
- BMEIA: fragmentiX ist SINA Ausrüster des BMEIA
- BMI: Langjährige Tätigkeit von W. Strasser für EDOK, EBT und BK
- Betreibergesellschaft ist offen für PPP
- Schrittweiser Ausbau möglich – EU Fördermittel abholen, AED aktiv!

Headquarter & offices



Head office

fragmentiX Storage Solutions GmbH
Wohllebengassse 10/7
1040 Wien
Austria / Europe

Swiss office

fragmentiX Schweiz AG
Calendariaweg 2
6405 Immensee
Switzerland

Contact us

» Head Office
+43 664 325 8896
» sales@fragmentix.com
» www.fragmentix.com

Canada office

Cybersécurité Quantique
fragmentiX inc.
2800-630 Boul René-Lévesque O
Montreal/QC H3B 1S6
CANADA