fragmentiX Secret Sharing:

how 41 year old math

saves our …

Shamir’s Secret Sharing
and a few unpleasant truths

@CODE 2020
Europe’s Digital Sovereignty – Road to Success?
Nov 11th 2020

Werner Strasser, CEO fragmentiX
ws@fragmentix.com

This is what we do! Answers in 0,5 sec to 5 min

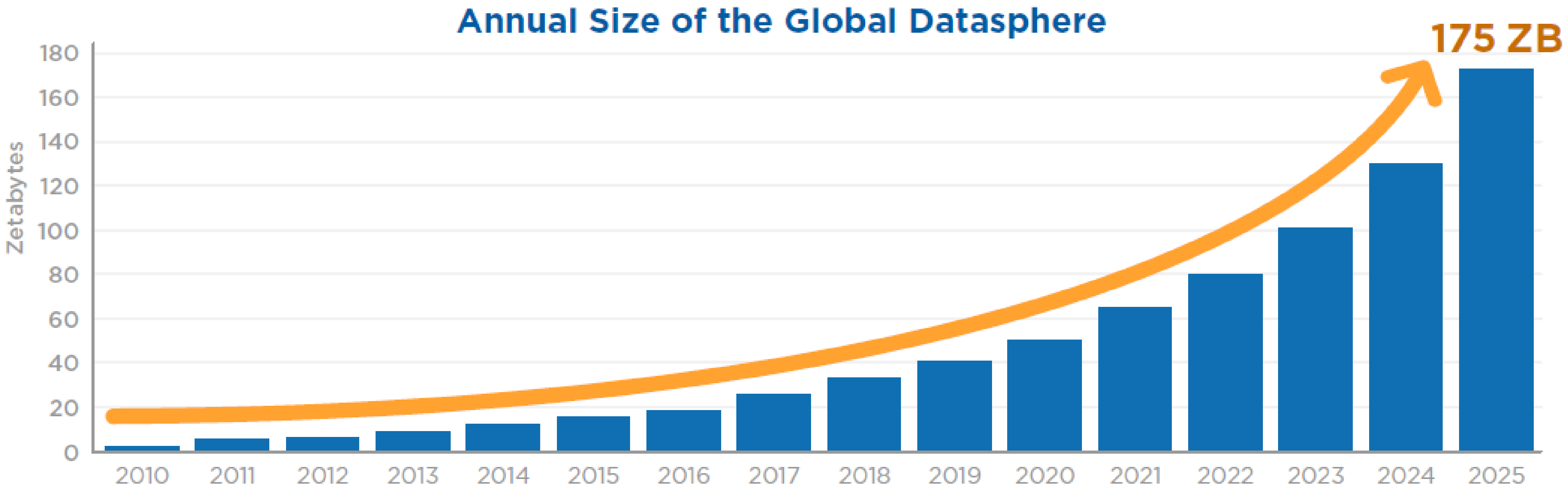
- Mine!
- Digital Sovereignty!
- Shamir’s Perfect Secret Sharing
- I act for and with Digital Sovereignty!
- We develop and produce Secret Sharing Storage Appliances!
- Everyone has the right to protect their own data in the cloud from being accessed by others

Werner STRASSER

- Werner Strasser (*1965) is an Austrian Entrepreneur
- Training Precision Engineering (today Mechatronics), Admin and repair of first Unix systems in Austria, Graphical / Departmental Supercomputing, Vector Processing (today HPC), Publishing and Document- Managementsystems, search technologies for government agencies (binary pattern recognition, semantic networks, ontologies), video conferencing solutions for companies and government agencies (including military applications).
- Since 1991 independent entrepreneur in different capacities for public authorities in Austria & EU, IT security related topics, protection of data against theft, sabotage etc.
- Foundation of fragmentiX GmbH in July 2018 - since September 2019 at IST Austria Technologiepark Klosterneuburg, fragmentiX Schweiz AG in the canton of Schwyz founded in Oct. 2020.
- Company vision: Empower everyone to control their privacy with focus on digital sovereignty
- Close cooperation with the AIT and Austrian ministries of Justice, Interior and Defense and authorities within the EU.
- Pro bono lecturer for cyber recruits in "Digital Forensics" at the LVAk of the Austrian Military.

amount of data that needs to be stored somewhere

fragmentiX®
QUANTUM SAFE STORAGE SOLUTIONS



… and 49% of data will be stored in public cloud environments by 2025.

source: *IDC whitepaper “DataAge 2025”*

Vision Statement

fragmentiX®
QUANTUM SAFE STORAGE SOLUTIONS

"We at fragmentiX are convinced that every individual human being, every company of any size as well as every state has the right to achieve Digital Sovereignty.

As an Austrian and European IT company, we want to ensure that every citizen and company can effectively protect their knowledge and data against the effects of asymmetric hybrid warfare, data theft and industrial espionage."

Werner Strasser, CEO of fragmentiX Storage Solutions

Shamir‘s Secret Sharing

Shamir‘s Secret Sharing is about splitting data into "fragments".

The special feature is that you can freely choose how many fragments are created in total, and also how many fragments are needed at least to recover the data. The ratio of required fragments to the total number of fragments created is called „**frx-ratio**“.

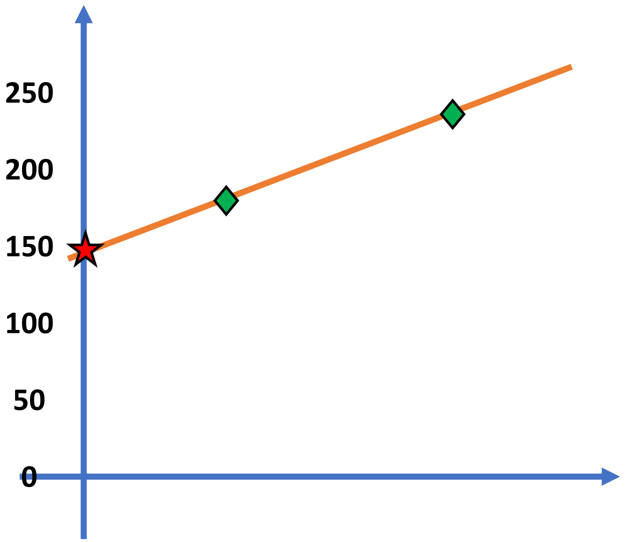
This is **Perfect Secret Sharing (PSS)**, which means that the *n* fragments created require a total of *n* times as much storage space as the original file. This increased storage space requirement can be seen as a disadvantage, but it is the only way to achieve **information-theoretical security (ITS)** , i.e. it is **guaranteed that no conclusions** about the content of the original data can be drawn from too few fragments.

Optionally, **PSS** can be combined with other cryptoalgorithms to reduce the memory requirements. This is then called **Computationally Secure Secret Sharing (CSS)**.

Shamir‘s Secret Sharing

Beispiel: We want to fragment a byte with the value **148** and a frx-ratio of 2/3. A property of a straight line is that you need at least 2 points to define it. We use this property because we also want to have at least 2 fragments to recover our data.

So let's imagine the fragmentation of **148** simply as a straight line through two points that intersects the secret value on the y-axis.



Line equation: $y = k \cdot x + d$
k … random value
d … Value of the secret byte

★ Secret data, e.g. a byte with the value **148**

— A straight line with random gradient intersecting the value **148** on the Y axis

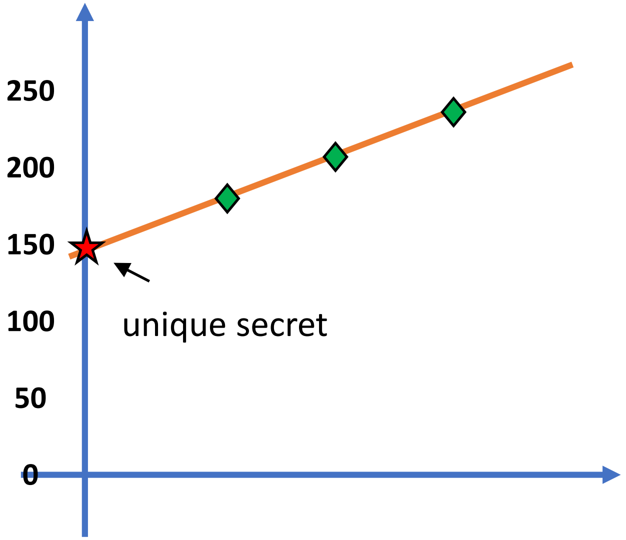
◆ points ("fragments") that lie on the random straight line

Shamir‘s Secret Sharing

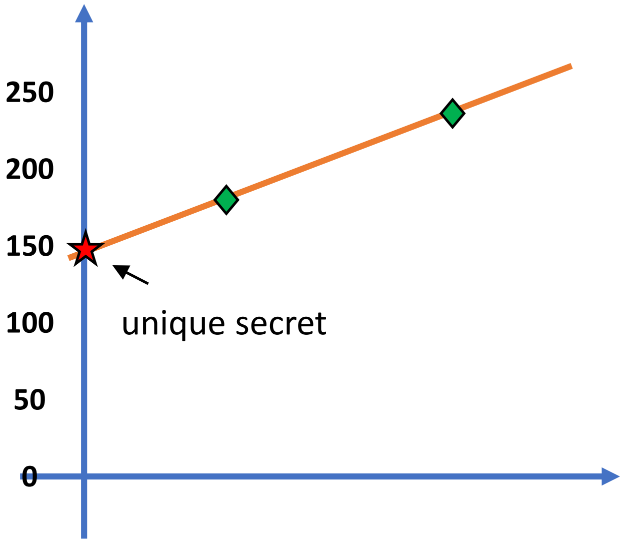
We can randomly select any number of points on the straight line, depending on how many fragments are to be created. The condition that we need any two points on the straight line to reconstruct the secret byte is always kept.

But as soon as there is only 1 point (i.e. 1 fragment), the secret byte could take any value.

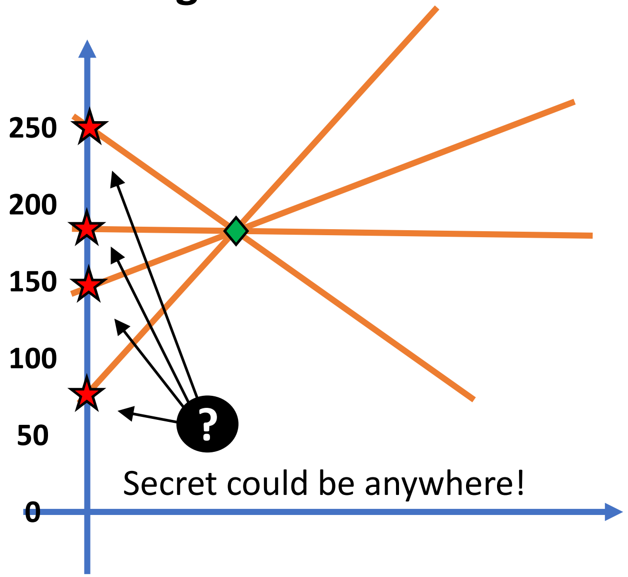
3 Fragments:



2 Fragments:



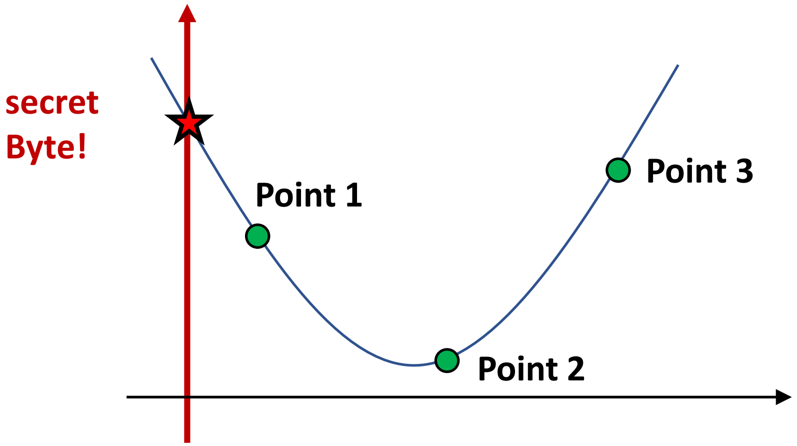
1 Fragment:

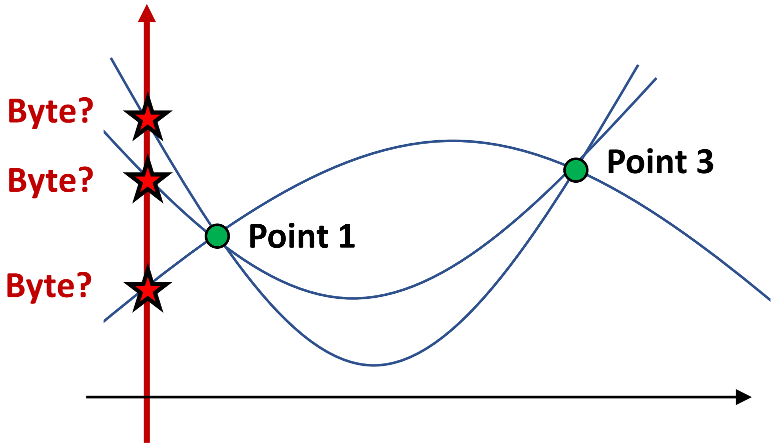


Shamir‘s Secret Sharing

You need two points to define a line. But if for example 3 points are needed, then we use a parabola.

The following applies: you need 3 points to define the parabola unambiguously. With 2 or less points the "secret byte" can take any value:





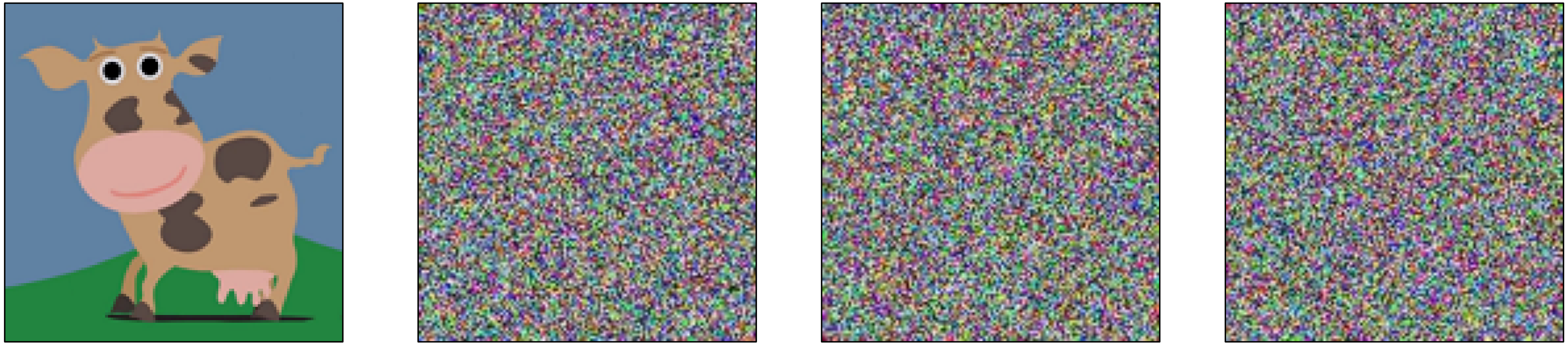
If more than 3 points (fragments) are needed, a polynomial function of higher degree must be used.

This can be extended at will.

Shamir‘s Secret Sharing

A separate random polynomial function is generated for each byte to be encrypted.

Here you can see how an image file would look like if its pixel color values were "fragmented" according to Shamir's Secret Sharing algorithm.



A single fragment does not allow **any conclusions to the content of the original file,**

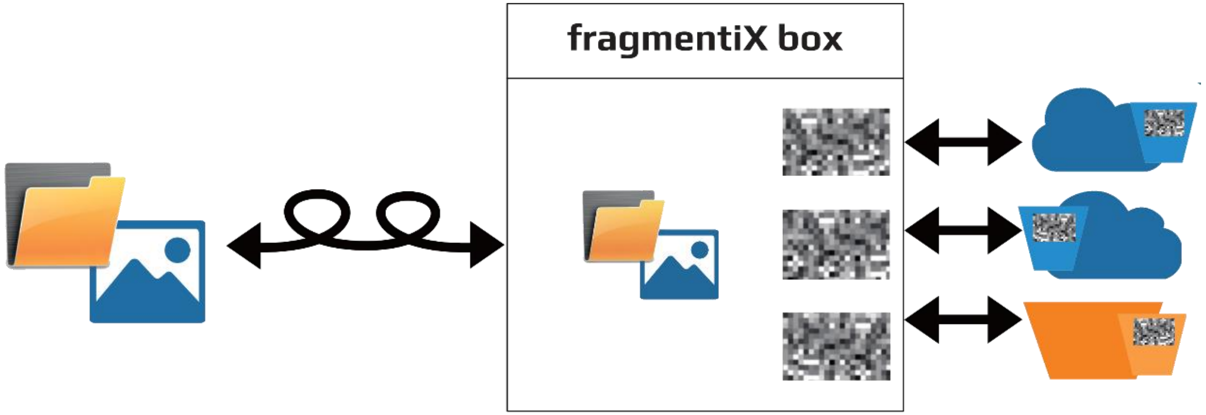
so → **information-theoretical security**!

fragmentiX Storage Appliances

fragmentiX® QUANTUM SAFE STORAGE SOLUTIONS

Demonstration of the functionality of a fragmentiX box

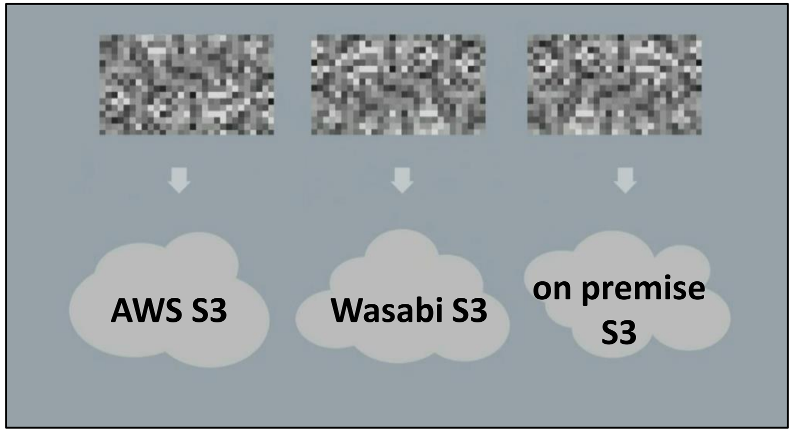
- Users save their files as usual on a network drive..
- The fragmentiX box uses Secret Sharing to split everything on the network drive into fragments.
- The number of created fragments and the storage locations of the fragments are defined by the owner / administrator.
- The fragmentiX box stores the fragments via one or more internet connections in the cloud or on local S3 buckets.



Example: reconstruction from 2 of 3 fragments

- If a frX-ratio 2/3 is chosen, 2 of 3 - no matter which 2 - fragments are sufficient for the fragmentiX box to reconstruct the original files.
- Even if one of the fragments is lost, all files can be completely reconstructed!

fragmentiX Storage Appliances



Each fragment is stored in its own cloud or local storage location **and only the owner** of the files knows where these locations are.

If one of the fragments is stolen, it is **absolutely useless** for the data thief or spy.

Product Roadmap

2019

fragmentiX box

for Companies

fragmentiX ONE
fragmentiX THREE
fragmentiX FOUR

2019

fragmentiX CLUSTER

for Datacenters & Corporations

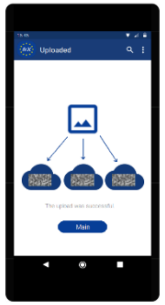
fragmentiX
fragmentiX CLUSTER NODE A
IT SECURITY MADE IN AUSTRIA
fragmentiX
fragmentiX CLUSTER NODE B
IT SECURITY MADE IN AUSTRIA

fragmentiX CLUSTER
fragmentiX half CLUSTER

2020

fragmentiX App

for Single-Users



for Android & iOS

2020/21

fragmentiX nano

for small Businesses

fragmentiX home

for families & private households

2021 ff.

fragmentiX TEMPEST

Mil. / EU / NATO Specifications

SMPC
für frXOS

Secure Multi Party Computing

QKD
EU27

Part of the EU27 initiative

Outlook

Infrastructure immune to quantum computers

- fragmentiX enables ITS for "Data on rest" today - no future quantum computer will be able to decode data from a stolen fragment.
- The combination with QKD (Quantum Key Distribution) as protection for "Data on Transit" allows fragmentiX to realize a complete ITS system for its customers.
- Future "post quantum" algorithms will be added to the fragmentiX portfolio.

Secure Multi Party Computing (SMPC)

- Today fragmentiX is the first "facilitator" to make public cloud storage usable even for owners of the most sensitive data sets.
- Founding member of www.mpcalliance.org
- To enable joint collaboration on sensitive data between two or more parties, SMPC allows the "use" of records without the need to "give" the data to other parties (e.g. to train AI algorithms for medical diagnosis and research).
- Brings the algorithms to the data - and not vice versa.

Dell Technologies OEM Solutions Partnership

- All fragmentiX CLUSTER systems are produced and delivered worldwide by Dell Technologies for fragmentiX and are serviced by Dell Technologies at the end customers site.

- This makes it possible to implement even critical applications worldwide with fast support from Dell EMC.

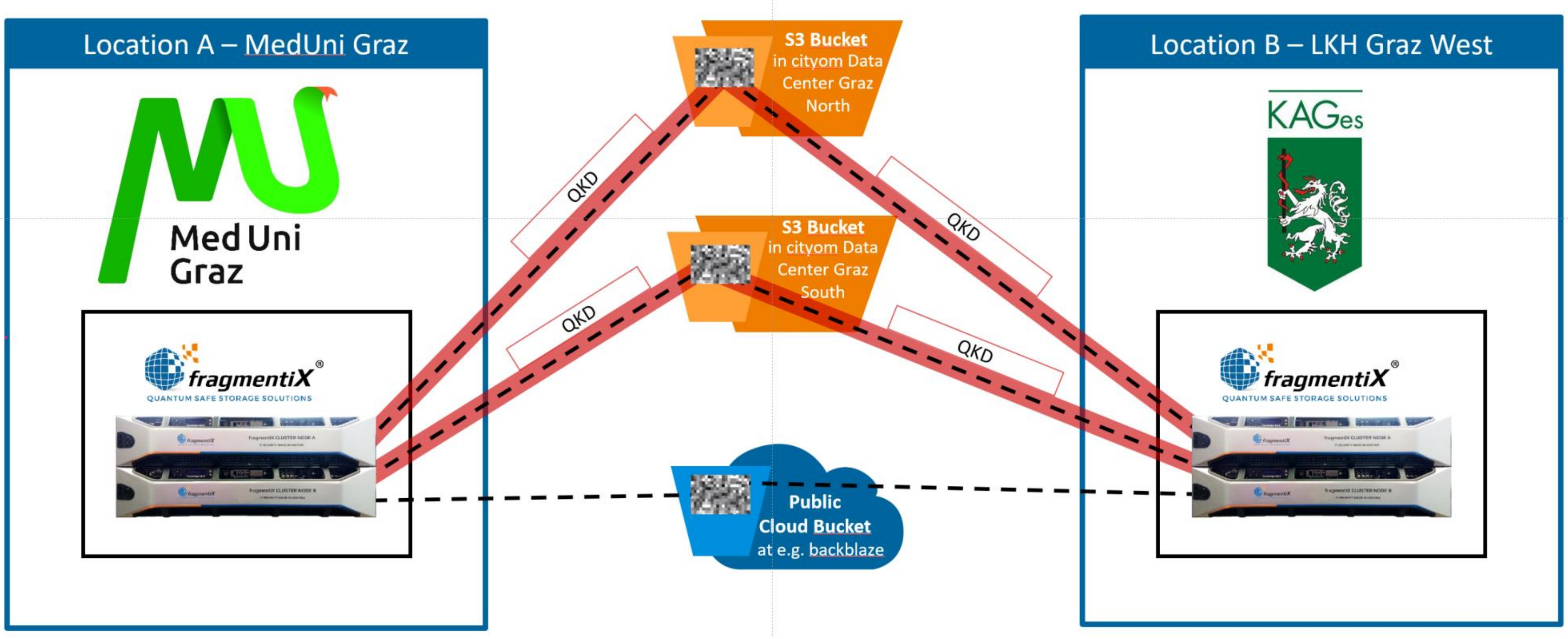
- Dell EMC ECS systems can be purchased directly through fragmentiX and maintained in a joint service contract with fragmentiX CLUSTER systems:

  standard: "next business day"
  expandable to “on-site service within 4 hours”

- fragmentiX is committed to support S3 storage from all major vendors equally.

OpenQKD EU Project UseCase Graz

fragmentiX®
QUANTUM SAFE STORAGE SOLUTIONS


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

fragmentiX Schweiz AG

“We are pleased to announce the foundation of **fragmentiX Schweiz AG** in Switzerland.

Since October we are registered as a company in the canton of Schwyz and therefore are able to react to changing EU regulations in a more flexible way.

We are already in negotiations with a number of distribution partners who are interested in supporting their end customers in Switzerland with fragmentiX products.

Swiss authorities and strategic partners and customers are now also directly supported by **fragmentiX Schweiz AG.**”

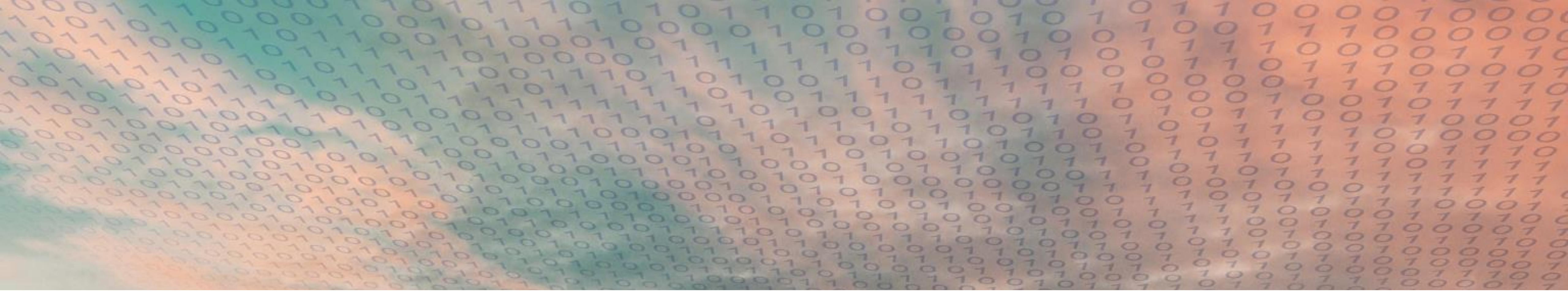
Recent presentations in German language

The following links enable you to download / stream recent slides and videos from:

“Information Security in Healthcare Conference *LUZERN / SWITZERLAND :”*

- **Warum uns 40 Jahre alte Mathematik dabei hilft, unsere Daten zu schützen** *Werner Strasser*
- Video: https://nc.fragmentix.com/nextcloud/index.php/s/DCaPztqAGonwn8G
- Slides: https://nc.fragmentix.com/nextcloud/index.php/s/JLJLdDK7McYx62S#pdfviewer

- **Eine zuverlässige und vertrauenswürdige Umgebung für Patientendaten bildet die Basis für Forschung und Entwicklung in der Medizin** *Kurt Zatloukal*
- Video: https://nc.fragmentix.com/nextcloud/index.php/s/2w24kCWXtMy4tDm
- Slides: https://nc.fragmentix.com/nextcloud/index.php/s/KdADJJQikKNLzkG#pdfviewer



contact us
» Werner Strasser +43 664 325 88 96
» ws@fragmentix.com
» sales@fragmentix.com
» www.fragmentix.com

head office
fragmentiX Storage Solutions GmbH
IST Technologie Park, Ploecking 1
3400 Klosterneuburg
Austria/Europe