

fragmentiX CLUSTER II[®] ... to use cloud storage without risks

fragmentiX CLUSTER II[®] is the **QRNG enabled** high-performance model of the fragmentiX storage appliance product family for GDPR-compliance, privacy protection, and data loss protection enabling real digital sovereignty. The highly efficient and redundant design of the cluster hardware is perfectly suited for use in datacenters of enterprises, service providers, and governments.

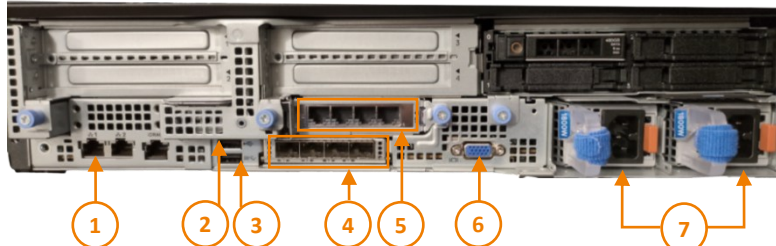
First and only world-wide commercially available quantum resistant appliance to use standard cloud storage

- Secret-sharing algorithm (ISO/IEC 19592, BSI TR-02102-1)
- PQC for TLS and code signatures
- Quantum random number generator (QRNG) as entropy source
- Highest protection against many traditional cyber risks and all quantum computer attacks
- High availability of data and strong resilience against data loss
- Compatible with all relevant cloud storages
- Compatible with 19" telecom racks
- 5 years mission-critical hardware support & repair within 4 hours worldwide – performed by DELL
- Fault-tolerant industrial grade hardware cluster nodes which act as a load balancing and 'failover system'
- Hardened frXOS operating system
- NATO TEMPEST (SDIP) on demand

fragmentiX CLUSTER II[®] consisting of two nodes



Interfaces of a fragmentiX CLUSTER II[®] node



- | | |
|-----------------------------|-----------------------------|
| 1 1 x 1 Gbit/s CONFIG NET | 4 4 x 25 Gbit/s SFP28 |
| 2 1 x USB CONFIG STORE | 5 4 x 10 Gbit/s RJ45 |
| 3 1 x USB CONFIG ENABLE | 6 1 x VGA |
| | 7 2 x 1800 W power supply |

Technical specification of a single fragmentiX CLUSTER II[®] NODE

Application environments	Datacenters	Network interfaces	4 x 10 Gbit/s RJ45
Max. storage LOCATIONS	26		4 x 25 Gbit/s SFP28
QRNG	Certified, rate up to 1Gbit/s	Power consumption	Typical 500 W
frXOS firmware/OS updates	1 year included	AC input	100-230 V AC, 50/60 Hz
HW mission critical support	5 years included	Weight	ca. 21 kg
Configuration options	Rear access available	Size (rear access)	19" width, 2U, max depth: 496.3 mm
	Front access available	Size (front access)	19" width, 2U, max depth: 572 mm

Privacy by design: Information-Theoretic Security with Secret Sharing

Secret sharing algorithms (ISO/IEC 19592, BSI TR-02102-1) guarantee information-theoretic security (ITS) for data stored with the fragmentiX CLUSTER II[®]. The data - no matter what files or directory structures - are divided into a number of fragments and each of them is stored on a different storage LOCATION. No user data remains locally on the fragmentiX CLUSTER II[®].

Any single fragment does not contain any information about the original data. Not even a small number of stolen / hacked fragments means a threat to your data's privacy - only a sufficient number of fragments allows the data to be restored. Choosing and combining up to 26 LOCATIONS allows to achieve better security than any other single storage solution can offer.

PQC for TLS and code signatures

TLS 1.3 data connections between the user (client) and the CLUSTER II[®], and between the CLUSTER II[®] and the storage LOCATIONS are protected by hybrid Post-Quantum Cryptography using X25519MLKEM768 (combining X25519 ECDH with ML-KEM-768 according to FIPS 203) for key establishment. Software updates are protected with PQC signatures.

Quantum random number generator (QRNG) as entropy source

The fragmentiX CLUSTER II[®] relies on true randomness generated by quantum effects. With the QRNG devices from our partners, we produce random numbers with rates up to 1 Gbit/s. These random numbers build the basis of the secret sharing algorithms.

Highest protection against many traditional cyber risks and all quantum computer attacks

The fragmentiX CLUSTER II[®] brings protection against storage related traditional cyber risks.

A data leak from your cloud provider or a misconfigured S3 bucket will not lead to disaster - because no provider or bucket alone contains abusable content. Typical insider and administrator threats can be largely mitigated by splitting responsibilities and using a fragmentiX central design principle: There is no longer a need to trust a single storage provider or your storage administrators. Data in each storage LOCATION is protected against malicious modifications by a cryptographic self-healing procedure.

The fragmentiX CLUSTER II[®] protects your sensitive data stored in cloud storages against the newly emerging cyber risks posed by large quantum computers: Several attackers are already collecting encrypted data streams on a large scale in order to be able to decrypt with quantum computers and abuse this stolen information later on.

fragmentiX products are the best way to increase the protection of sensitive data against traditional and quantum computer threats - today and tomorrow!

High availability of data and strong resilience against data loss

The connection of up to 26 regionally or globally distributed redundant storage LOCATIONS from different operators or own data centers to the fragmentiX CLUSTER II[®] increase the availability of data if individual parts of the internet or the company's own networks fail. The use of multiple redundant fragments provides a high level of robustness against data loss if individual fragments fail. Data in each storage LOCATION is protected against erroneous data corruption by a cryptographic self-healing procedure.

Easy-to-use directly as S3 proxy or with the fragmentiX WebDAV interface

In a typical scenario, the fragmentiX CLUSTER II[®] provides network drives to the existing desktop PCs and servers within the local network. These network drives are accessible through as S3 bucket or WebDAV share.

For heavy loads, the S3 interface excels with its robustness and reliability, while the WebDAV share is easily accessible even via modern Web-Browsers.

If your applications already use S3 storage you can simply add the fragmentiX CLUSTER II[®] as an S3 proxy without having to change your application and without any additional client software.

Multiple storage types reachable via separate connections

The following storage types can be used with fragmentiX CLUSTER II[®]:

- S3 and S3 compatible hybrid/multi cloud storage on the internet and/or intranet
- Microsoft Azure Blob storage
- NFS compatible storages

Four 10Gbit/s RJ45 and four 25Gbit/s SFP28 interfaces allow for maximal flexibility in different network scenarios.

Hardened operating system frXOS

frXOS - the fragmentiX CLUSTER II[®]'s hardened operating system - was developed by fragmentiX to make it both secure and easy to use for users and administrators. All functions are kept up to date through regular updates, which can be carried out locally by the administrator. A valid maintenance contract is required to receive the latest frXOS updates beyond the first year after delivery of your system.

Industrial grade hardware and advanced protection measures

All fragmentiX CLUSTER II[®] systems are prebuilt by DELL Technologies and the sensitive components and software are finished in Austria, to guarantee no backdoors or intended weaknesses are built into our products. State-of-the-art Crypto-Smartcards in USB smartcard readers ensures that all security-relevant data can only be read on the respective fragmentiX CLUSTER II[®] and modified by the authorized administrator. A fragmentiX CLUSTER II[®] system can be composed of one or more server nodes which can act in load balancing or failover mode and therefore provide hardware redundancy. Optionally, QKD devices and advanced link encryptors can be added.

For further information:

www.fragmentix.com | sales@fragmentix.com | +43 2243 24203

fragmentiX Storage Solutions GmbH

Wohllebengasse 10 Top 7
1040 Wien
Austria, Europe