Cloud Security in a box!

Digitale Souveränität
mit fragmentiX Storage Appliances

Oktober 2018

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Warum QSSS?

Wie funktioniert das?

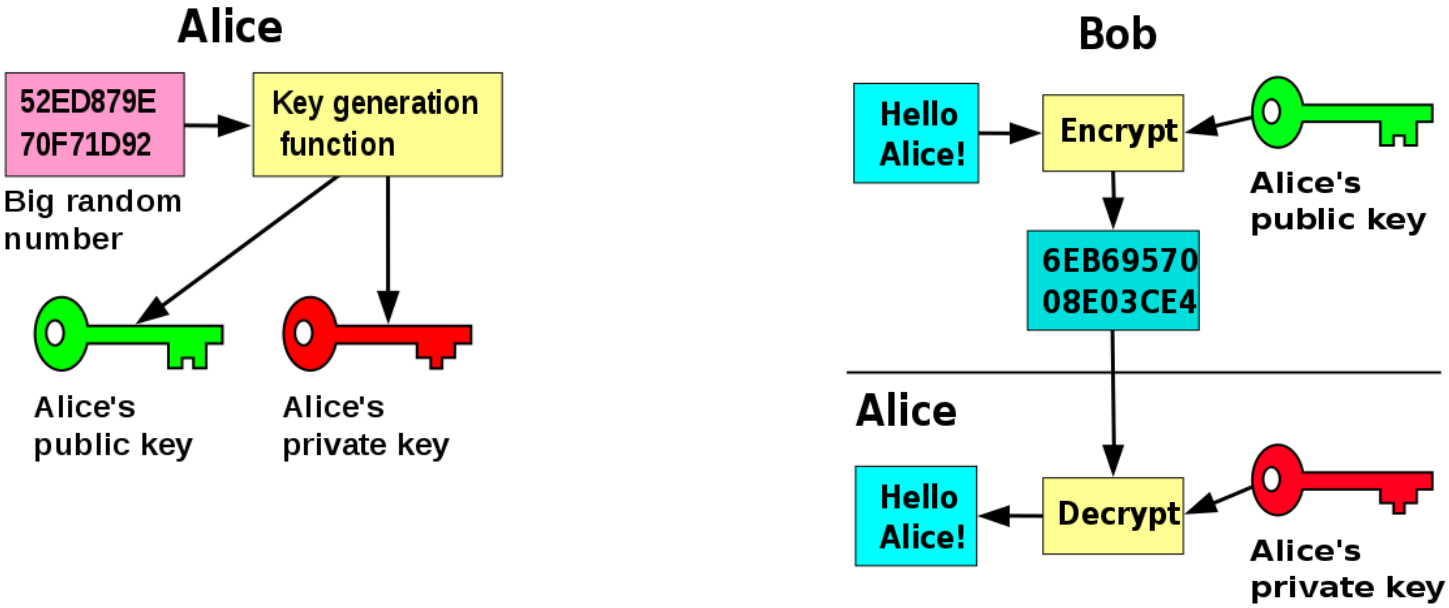
Wen betrifft das?

Digitale Souveränität?

Gibt es dazu **eine Lösung?**

Warum ?

Die wesentlichen Sicherheitsmaßnahmen gegen Diebstahl und Spionage in Netzwerken und Daten-trägern hängen heute meist von der Verschlüsselung mit mathematischen Verfahren ab:



fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Warum ?

- Vereinfacht kann gesagt werden, dass die meisten asynchronen Verschlüsselungen mit **M = p * q** arbeiten.
- **M** ist dabei das Produkt zweier großer Primzahlen **p * q**
- Um **p** und **q** mit "brute force" zu berechnen fehlte bisher potentiellen Dieben/Spionen einfach die Zeit.
- Das „Knacken mit herkömmlichen Computern – selbst Supercomputern - dauert ohne zuvor mutwillig eingebaute backdoors sehr sehr sehr ... viele Jahre!

Das sind 21 Nullen und Jahre!

PC Stand heute **28.000.000.000.000.000.000.000 Jahre**

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

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Warum ?

- Die weltweit für Regierungen und Konzerne bereits verfügbaren Quantencomputer brauchen – sobald sie noch mehr „Qubit‘s“ bekommen - für das Knacken asymmetrischer Verschlüsselungen, die wir heute als „SICHER“ erachten:

Das sind 2 Nullen und Sekunden!

- **Quantencomputer** **sehr bald** **100 sec**

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

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Warum ?

Also last month, China announced that it would build the world's biggest quantum research facility, a $10 billion center in Hefei, capital of Anhui province, with the aim of building a working quantum computer that could break most any encryption within seconds.

China already has the world's fastest supercomputer, the Sunway TaihuLight, which captured the title in the 2016 and 2017 at a competition in Frankfurt, Germany.

Monroe, the Maryland physicist, said China had set a goal of fully constructing the quantum research center within two years.

"If it costs $10 billion, China will just do it without asking, and they'll put an army together to do it," Monroe said. "I don't think any other government in the world is able to throw together something (so) fast."

Google, IBM and Microsoft all see huge opportunity in quantum computing and fund research labs. Commercial applications may include determining how polymers go together, mapping the genome, finding oil in complex geology, detecting cancer and handling air traffic.

From http://www.mcclatchydc.com/news/nation-world/national/national-security/article179971861.html

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Warum ?

Was bedeutet das für mich?

- Bald wird es nicht mehr genügen Daten „nur“ noch zu verschlüsseln!

- Jede “nur“ verschlüsselte Datei, die heute gestohlen oder am Transportweg “aufgenommen” wird, kann sehr bald vom Dieb/Spion gelesen und genutzt werden.

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Warum ?

Digitale Souveränität – eine Meinung:

- Jeder Mensch und jedes Land für sich hat das Recht auf Digitale Souveränität – die alleinige Hoheit über die eigenen Daten - und damit das eigene Wissen.
- Nicht nur landeseigene und fremde staatliche Institutionen können zukünftig praktisch alle digitalen Daten lesen und u.U. auch missbrauchen – auch kriminelle Akteure werden weltweit noch stärker in der Lage sein alle gewünschten Daten zu knacken und für deren Zwecke einzusetzen.

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Warum ?

Digitale Souveränität – ein Beitrag:

- fragmentiX ist als ein Mittel zur Selbstverteidigung und Erlangung Digitaler Souveränität geplant und entwickelt worden.
- Durch den Einsatz von fragmentiX kann wesentlichen Forderungen der DSGVO entsprochen werden und dadurch immer vorhandenes Risiko verringert werden.

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Wer steht dahinter?

- In intensiver Kooperation der ProCom-Strasser GmbH mit dem AIT - dem Austrian Institute of Technology wurde fragmentiX zu einem marktreifen Produkt entwickelt.
- Im Juli 2018 wurde die fragmentiX Storage Solutions GmbH gegründet.

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

ProCom Strasser
www.procom-strasser.com

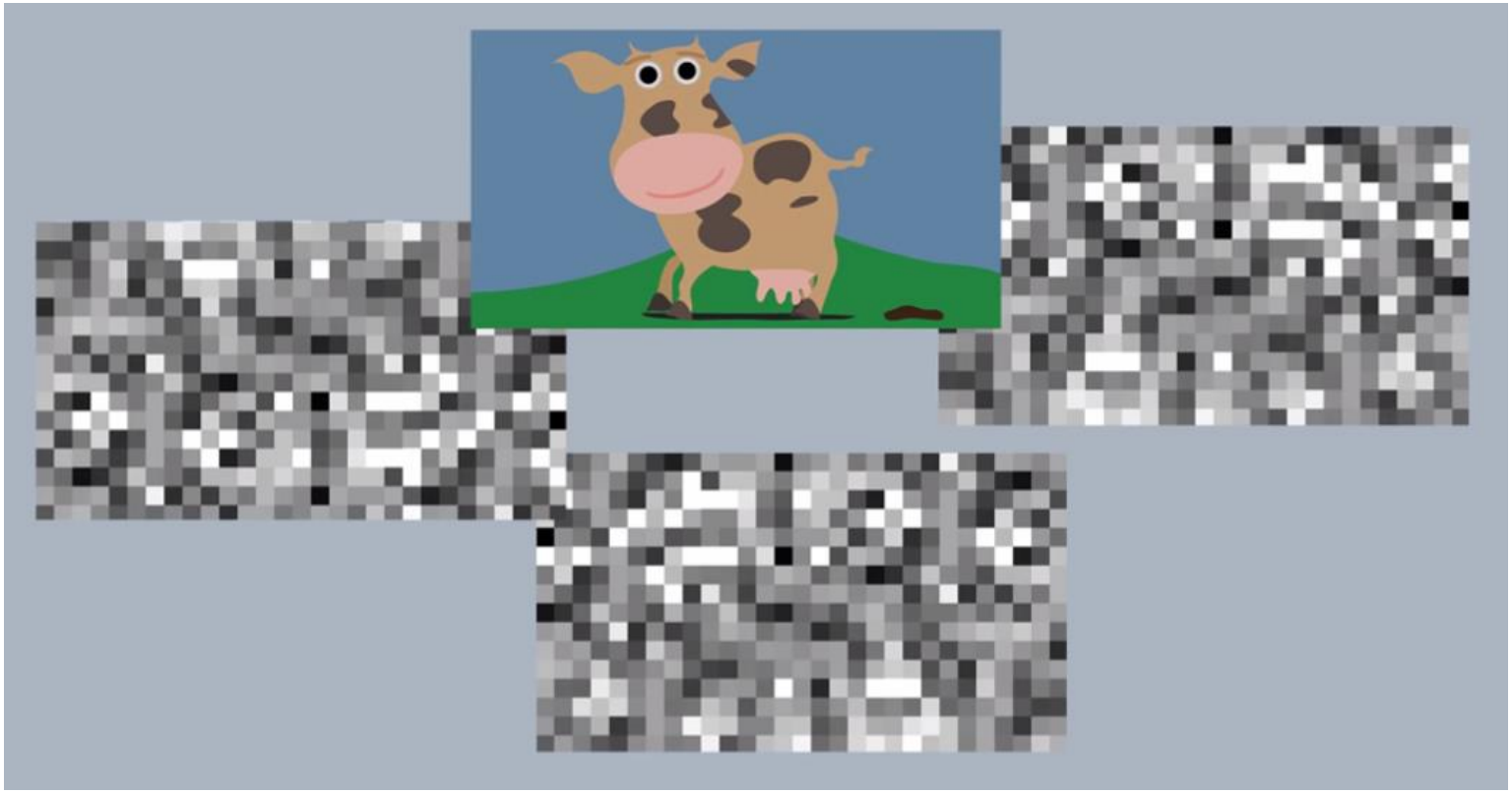
fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Wie?
Ein Beispiel:

Dieses Bild soll geschützt werden:

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

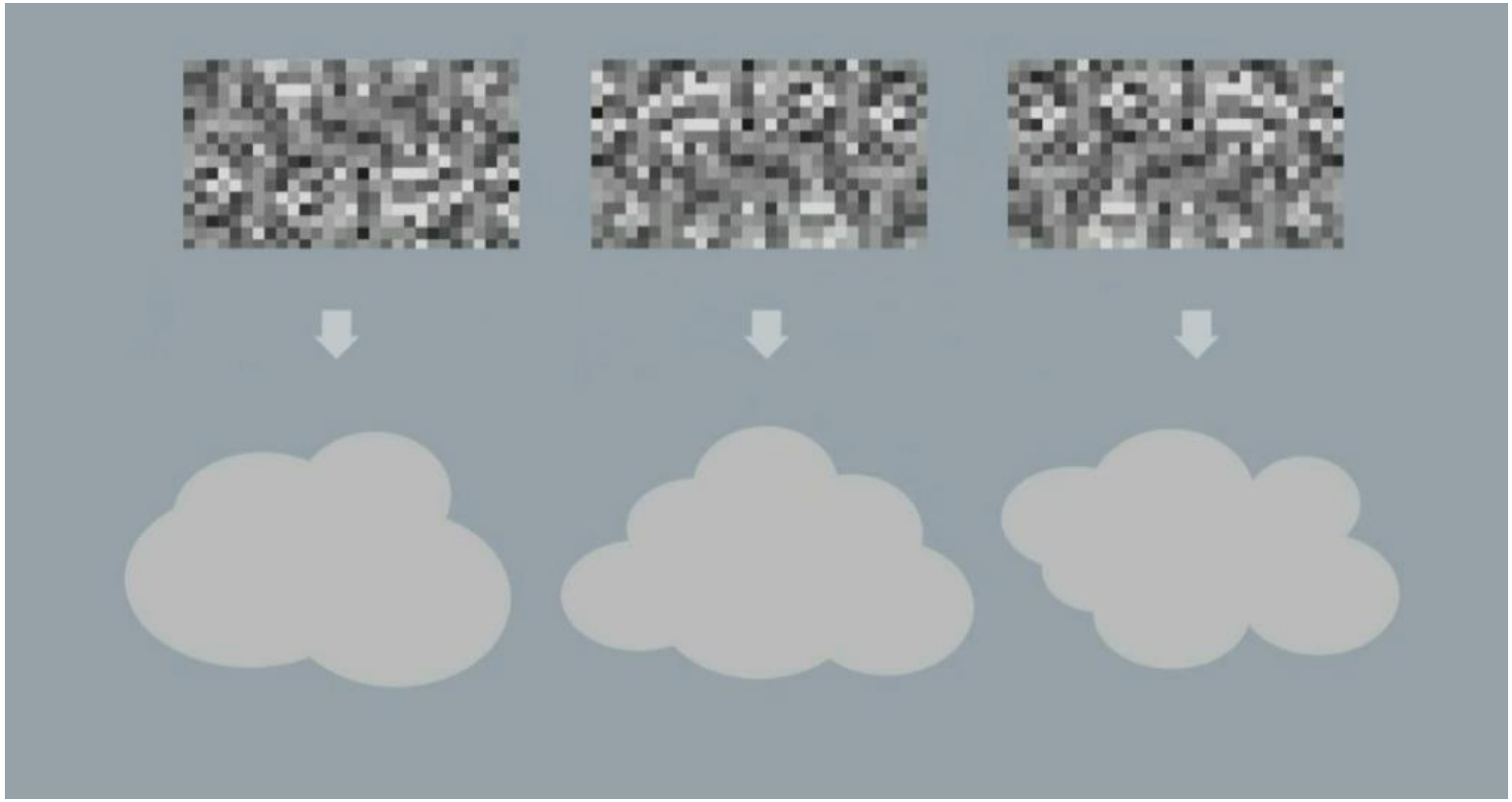
Wie ?



ES WIRD IN 3 FRAGMENTE ZERTEILT

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

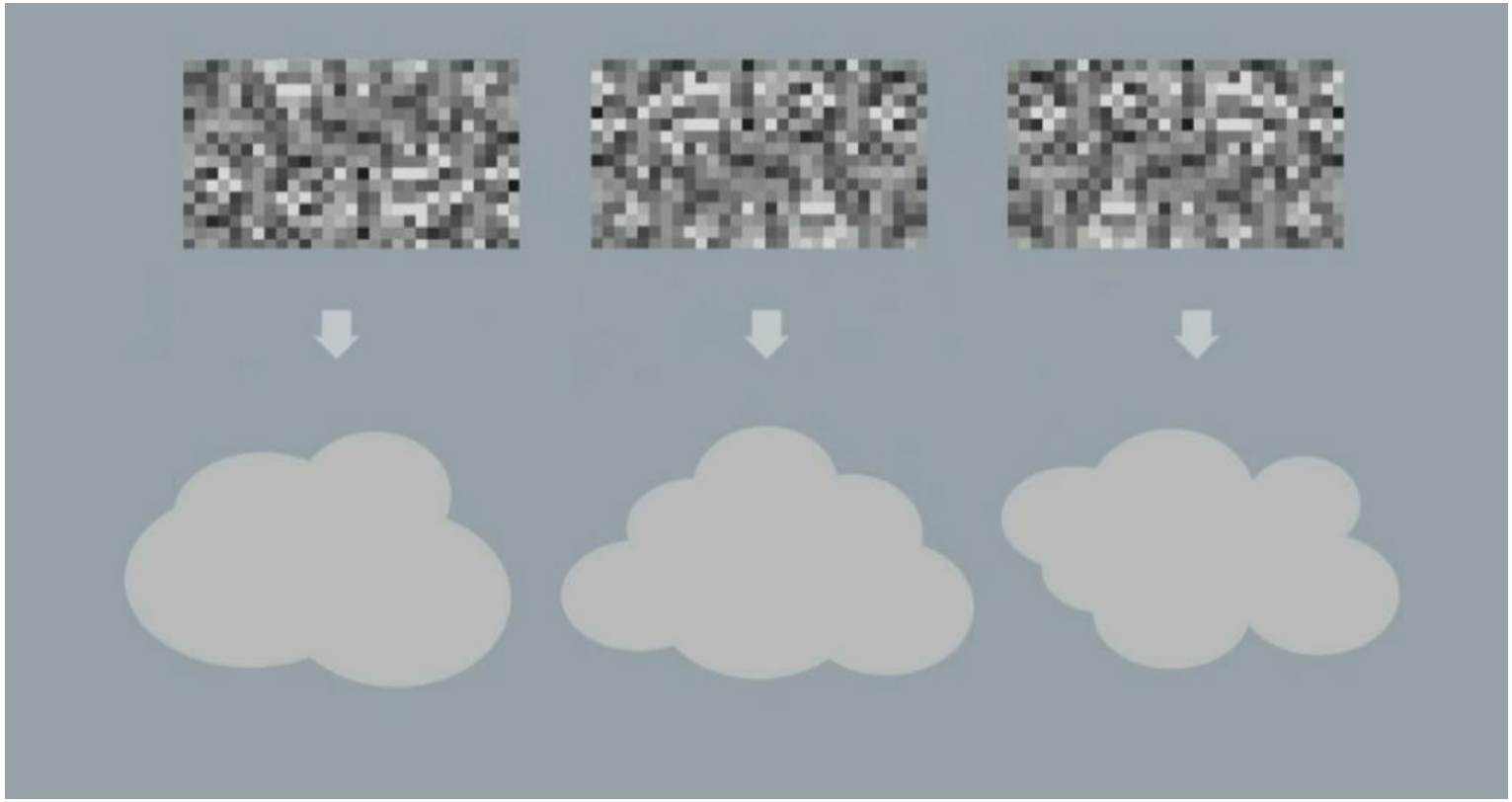
Wie ?



KEINES DIESER 3 FRAGMENTE ALLEIN ENTHÄLT NUTZBARE INFORMATION

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

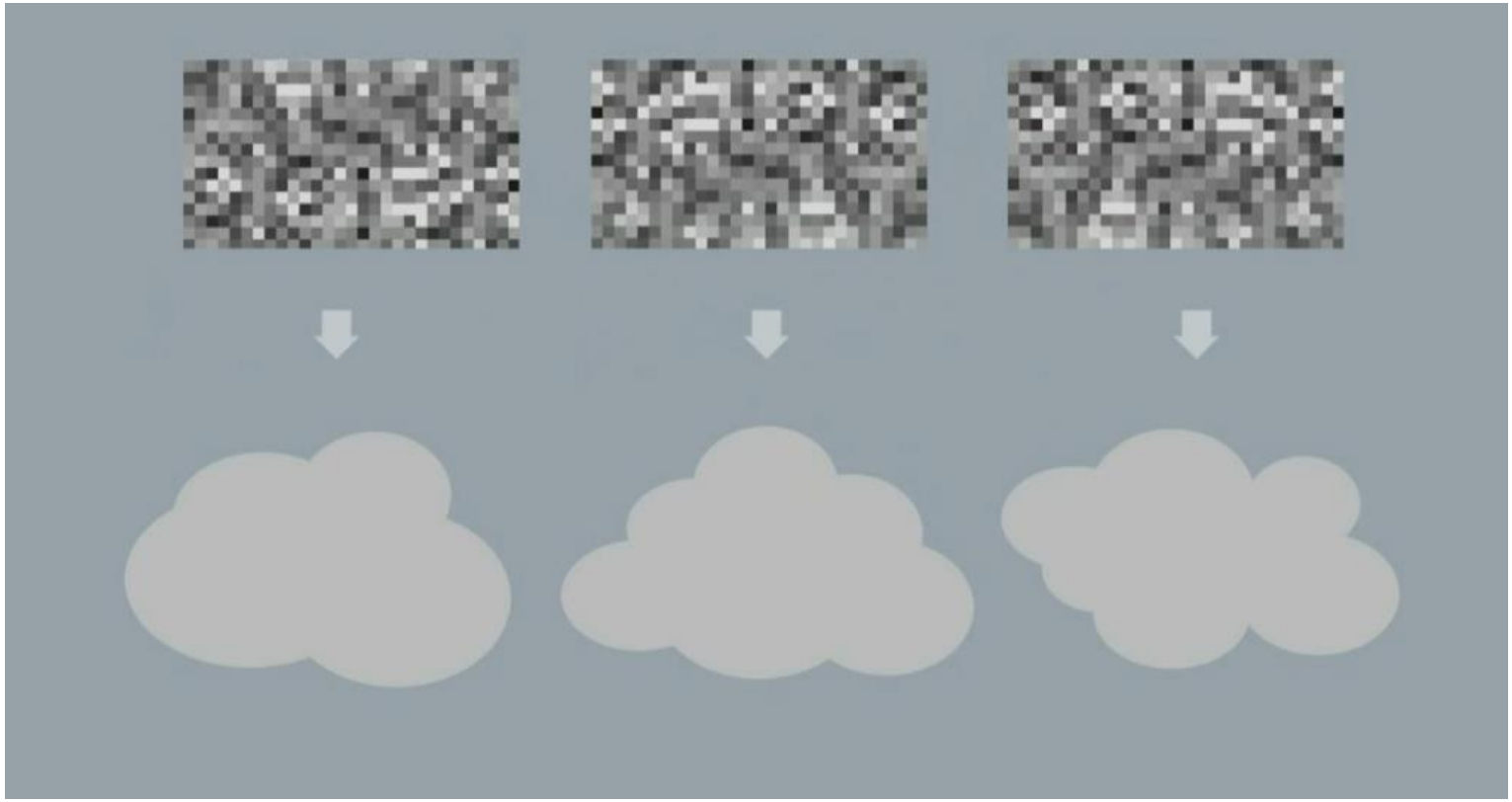
Wie ?



MIT GEHÄRTETEN APPLIANCES UND GEEIGNETER IT-METHODIK WIRD

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

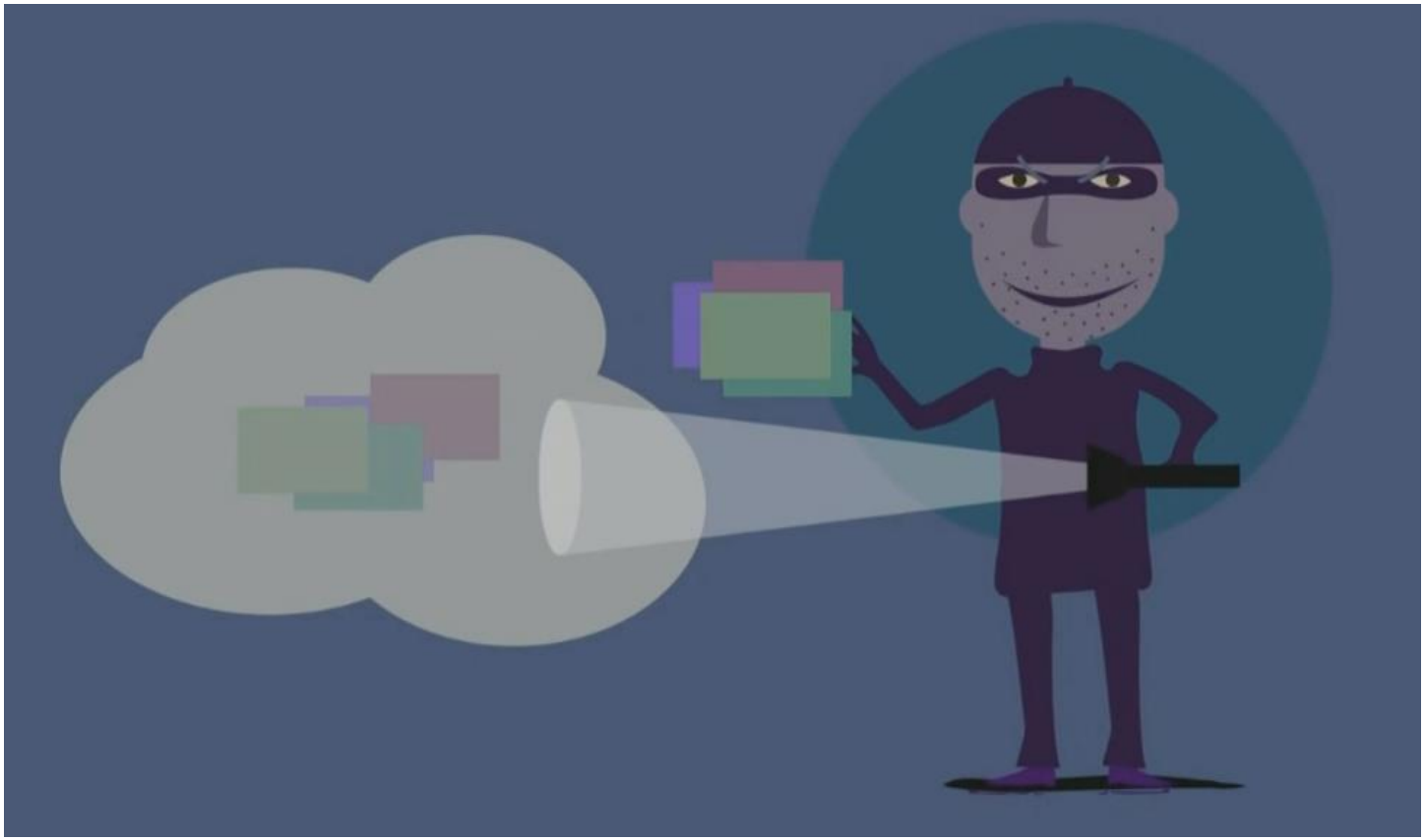
Wie ?



JEDES FRAGMENT AUF EINEN EIGENEN CLOUD- ODER LOKALEN STORAGE GELEGT

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Wie ?



WENN JETZT EINES DIESER FRAGMENTE AUS EINEM DER SPEICHER GESTOHLEN WIRD

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Wie ?

IST ES FÜR DEN DIEB ODER SPION VOLLKOMMEN NUTZLOS

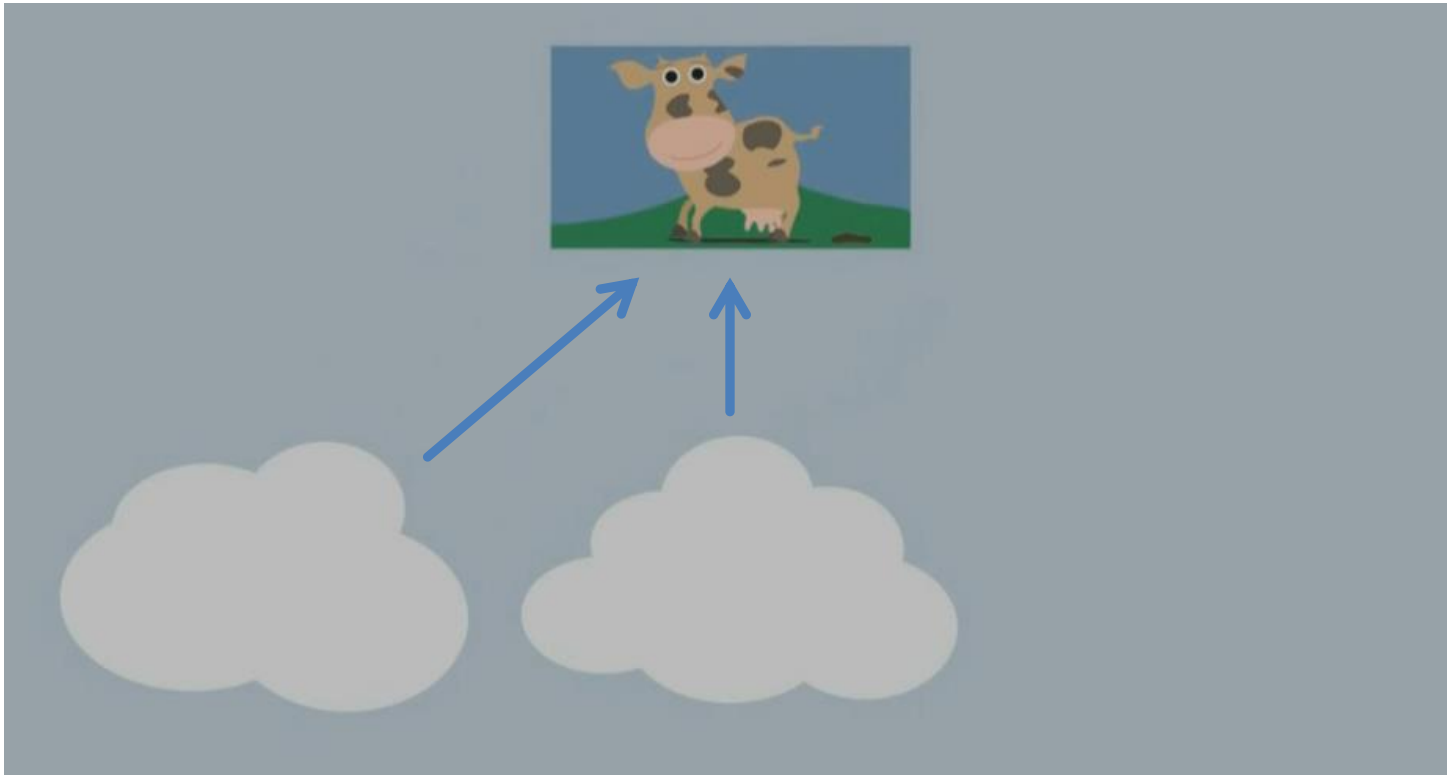
fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Wie ?

AUCH WENN EIN EINZELNES FRAGMENT VERSCHWINDET … ZWEI SIND GENUG

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Wie ?



UM DIE DATEI AUS DEN VERBLIEBENEN FRAGMENTEN WIEDER HERZUSTELLEN

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Wie ?

- **fragmentiX teilt Ihr "Geheimnis" in bis zu 26 Fragmente auf – und jedes einzelne Fragment können Sie genau dort ablegen wo Sie es haben wollen:**

  - Public Cloud Storage: AWS, ACP Cloud …
  - Private Cloud Storage: freeNAS S3 …
  - Lokales USB Laufwerk / USB Stick

Wie?


DVI-I DISPLAY
LAN
CONFIG NET
fragmentiX THREE
DC IN 9V – 48V
USB Storage Ports
LAN Schnittstelle:
PCs, Linux und Macs sehen hier Netzlaufwerke.
Über SMB, NFS, etc. werden die Dateien hier her kopiert – und dann als frX Fragmente an die gewählten LOCATIONS und USB Platten/Sticks verteilt.
USB Storage Ports:
GANZ OHNE CLOUD oder GEMISCHT MIT LOCATIONS können die frX Fragmente auch auf USB-Platten oder USB-Sticks verteilt abgespeichert werden.
CONFIG NET:
NUR AN DIESEM PORT KANN der ADMIN die Konfiguration über das WEB GUI ändern.
fragmentiX
QUANTUM SAFE STORAGE SOLUTIONS

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Wie?

Wie ?

- **Sie selbst definieren die “frX ratio” für Ihre Anwendung:**

$$frX\ ratio = \frac{Notwendige\ Anzahl\ von\ Fragmenten\ zum\ Wiederherstellen}{Erstellte\ Anzahl\ an\ Fragmenten}$$

**Im KUH FOTO Beispiel wurde eine frX ratio von 2/3 verwendet,
3 Fragmente wurden erstellt und zur Wiederherstellung sind bereits 2 davon - egal welche 2 - ausreichend.**

- **Andere Beispiele könnten 5/8, 5/16 oder 17/26 sein:**

- **Die für eine Anwendung maximal nutzbare Anzahl von Fragmenten ist durch die Leistungsfähigkeit und damit die Anzahl an “locations” begrenzt die von der gewählten fragmentiX BOX benutzt werden kann: 6, 16 oder 26 bei aktueller fragmentiX Generation 1 Hardware.**

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Wie ?

- **Ein für einen Anwendungsfall geeigneter “frX ratio” hängt von der gewünschten Nutzungsgewichtung ab:**

  - Hochverfügbarkeit

  - Schnelligkeit

  - Langzeitsicherheit

  - Kostenoptimierung

Was will Ich erreichen?

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

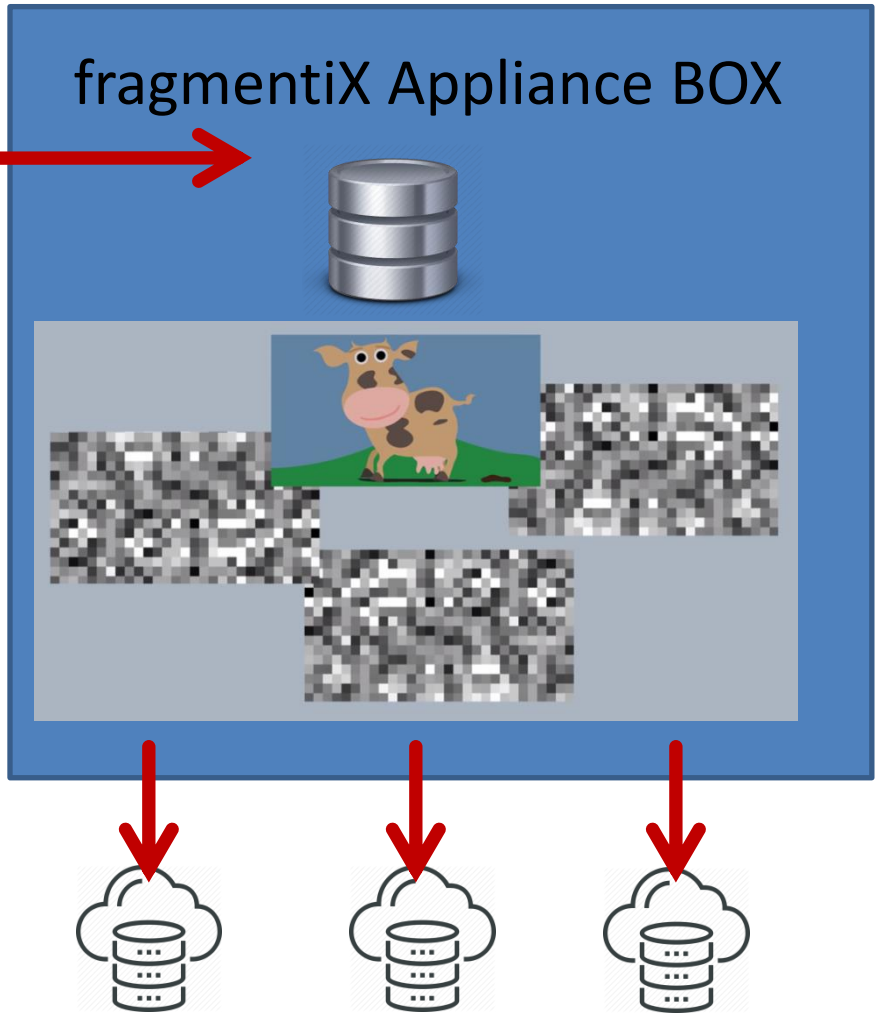
Warum ?

SIE MÜSSEN KEINEM EINZELNEN PROVIDER, ADMINISTRATOR ODER DIENSTLEISTER VERTRAUEN

SIE MÜSSEN AUCH fragmentiX - NICHT VERTRAUEN – NUR SIE ALLEINE LEGEN FEST WO IHRE FRAGMENTE GESPEICHERT WERDEN

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Wie ?



PUT DATA ?

IHRE SCHÜTZENSWERTEN DATEN

copy/move data to /frix directory

fragmentiX processing

Distribute parts to different ISPs using more than one NICs

Move to n (here 3) Storages

- location A
- location B
- location C

IHRE FRAGMENTIERTEN SCHÜTZENSWERTEN DATEN

GET DATA ?

IHRE SCHÜTZENSWERTEN DATEN

Request data using key-value to /frox directory

fragmentiX processing

Retrieve parts from different ISPs using more than one NICs

Move to n (here 3) Storages

- location A
- location B
- location C

IHRE FRAGMENTIERTEN SCHÜTZENSWERTEN DATEN

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

Generation 1 Produkte

Produkt	fragmentiX ONE	fragmentiX THREE	fragmentiX FOUR
Anwendungsfälle	Storage Appliance Box für kleinere Arbeitsgruppen oder Niederlassungen mit bis zu 10 Mitarbeitern und ein oder 2 Internetzugängen (z.B. ADSL und LTE Router)	Storage Appliance Box für Arbeitsgruppen oder Niederlassungen mit bis zu 30 Mitarbeitern und bis zu vier Internetzugängen (z.B. Standleitung, ADSL und 2 x LTE Router)	Storage Appliance Box für große Arbeitsgruppen oder Niederlassungen mit mehr als 30 Mitarbeitern und bis zu acht Internetzugängen (z.B. 2 Standleitungen, 2 ADSL und 4 x LTE Router)
Betriebssystem und CPU	Gehärtetes frxOS Betriebssystem auf Industrie-PC mit robuster Hardware, geschütztem BIOS und INTEL 4 Kerne CPU	Gehärtetes frxOS Betriebssystem auf Industrie-PC mit robuster Hardware, geschütztem BIOS und INTEL i5 CPU	Gehärtetes frxOS Betriebssystem auf Industrie-PC mit robuster Hardware, geschütztem BIOS und INTEL i7 CPU
Anzahl nutzbarere locations	8	16	26
NICs: LAN/WAN	2/2	2/4	2/8
Preis/Stück exkl. MwSt.	6.980 €	16.720 €	26.820 €
Wartung/Jahr	15%	15%	15%
Verfügbarkeit	jetzt	jetzt	jetzt

ACHTUNG: Alle Angaben und Spezifikationen können ohne Vorankündigung geändert werden. Angaben ohne Gewähr

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

roadmap

Produkt	fragmentiX mobile APP	fragmentiX SHARE client	fragmentiX VM	fragmentiX CLUSTER	fragmentiX PARANOIA
Anwendungsfälle	IOS app & Android app	Software read only/ download only für Windows, Mac und Linux	Virtual frxOS Server für Testanwendungen und Pilotprojekte	Cluster für - Rechenzentrum - Unternehmens-zentralen - Dienstleister	Abstrahlungs-geschützte Hardware für sensible und mobile Anwendungen
Nutzen	Faßt drei Speicher zu einem secure - 2 aus 3- Speicher zusammen	Für “download only” von fragmentiX locations – nur verfügbar für fragmentiX Kunden	Günstige Produktvariante für private fragmentiX Anwendungen und Testbetriebe	frxOS on high performance cluster hardware	frxOS auf zonierter und zertifizierter Hardware
Number of storages	3 (Apple, Google, Microsoft)	Existing frxOS configs	3 bis 5	26	26
NICs: LAN/WAN	UMTS/LTE or WLAN	n.a.	1/1	8/8 10 Gbit NICs	1/1
Preis/Stück excl. MwSt. **Wartung/Jahr** **Verfügbarkeit**	1,99 € free Q4/2018	150 € n.a. Q4/2018	to be defined 15 % Q4/2018	62.200 € 15% Q1/2019	to be defined 15% Q1/2019

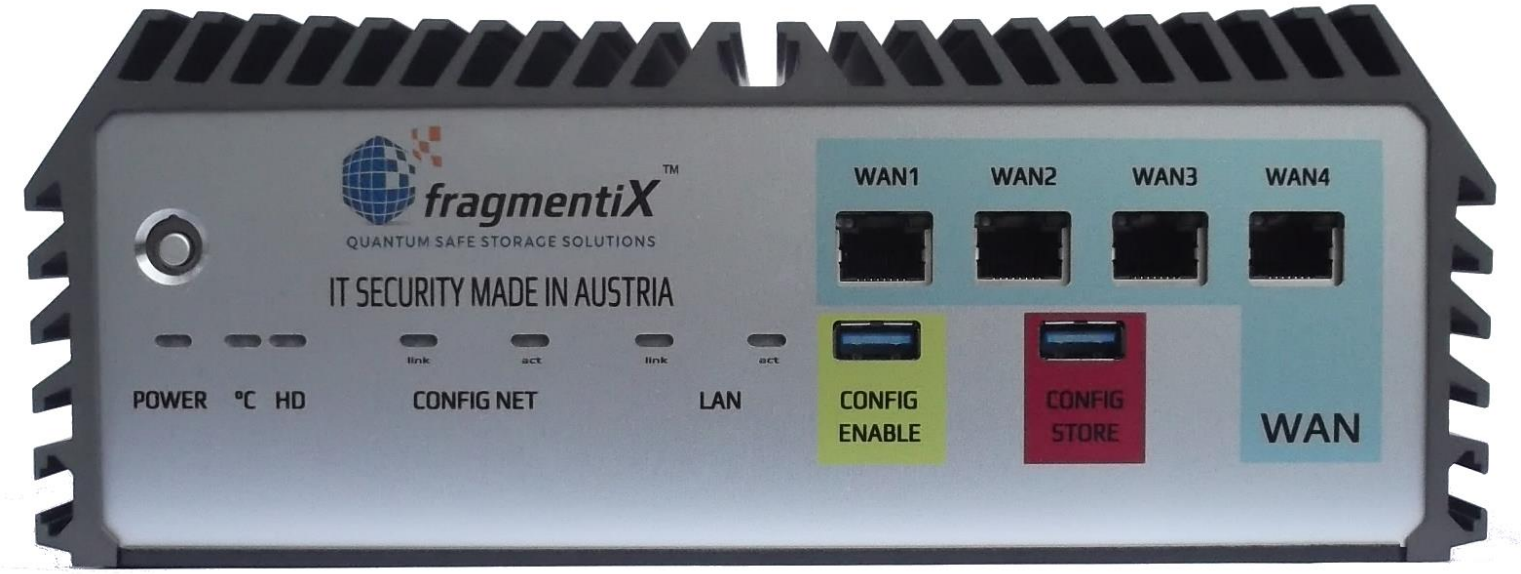
fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

fragmentiX ONE

2 x LAN Schnittstellen (1 x LAN als Netzlaufwerk, 1 x CONFIG ONLY)
2 x WAN Schnittstellen zur Nutzung multipler Internetzugänge
Bis zu 8 adressierbarer “locations” – Cloud S3 oder USB Disk / Stick
frxOS gehärtetes Betriebssystem

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

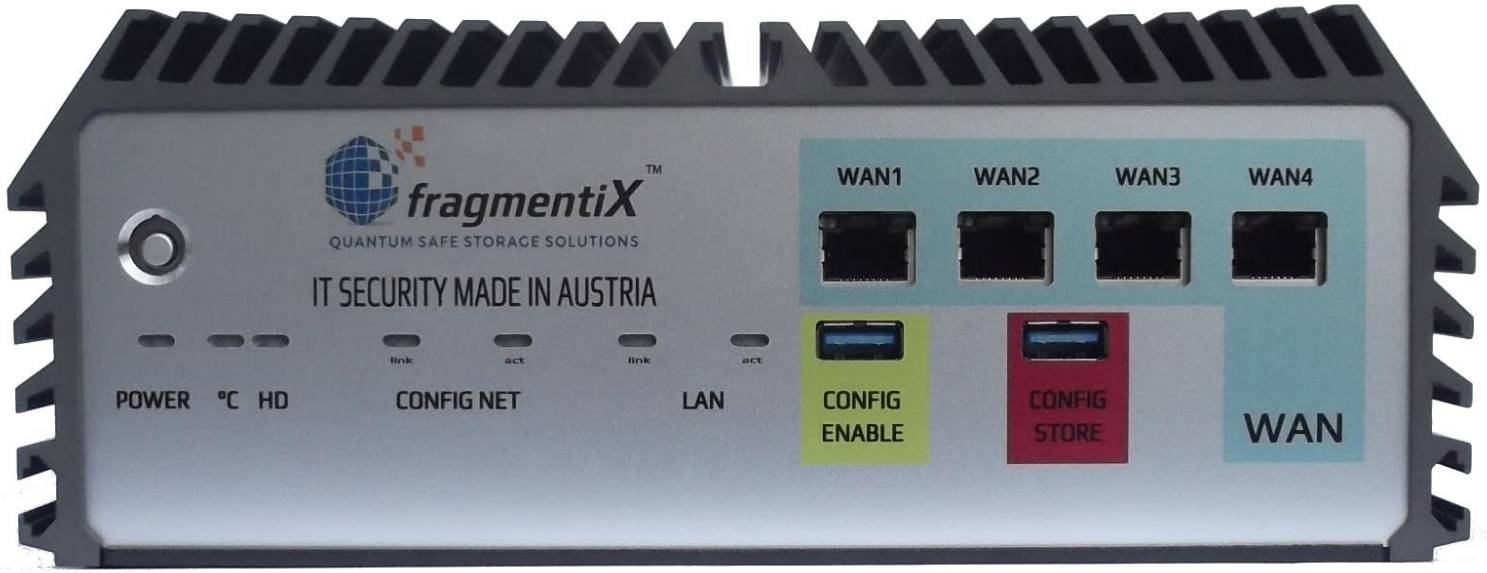
fragmentiX THREE



2 x LAN Schnittstellen (1 x LAN als Netzlaufwerk, 1 x CONFIG ONLY)
4 x WAN Schnittstellen zur Nutzung multipler Internetzugänge
Bis zu 16 adressierbarer “locations” – Cloud S3 oder USB Disk / Stick
frxOS gehärtetes Betriebssystem

fragmentiX™
QUANTUM SAFE STORAGE SOLUTIONS

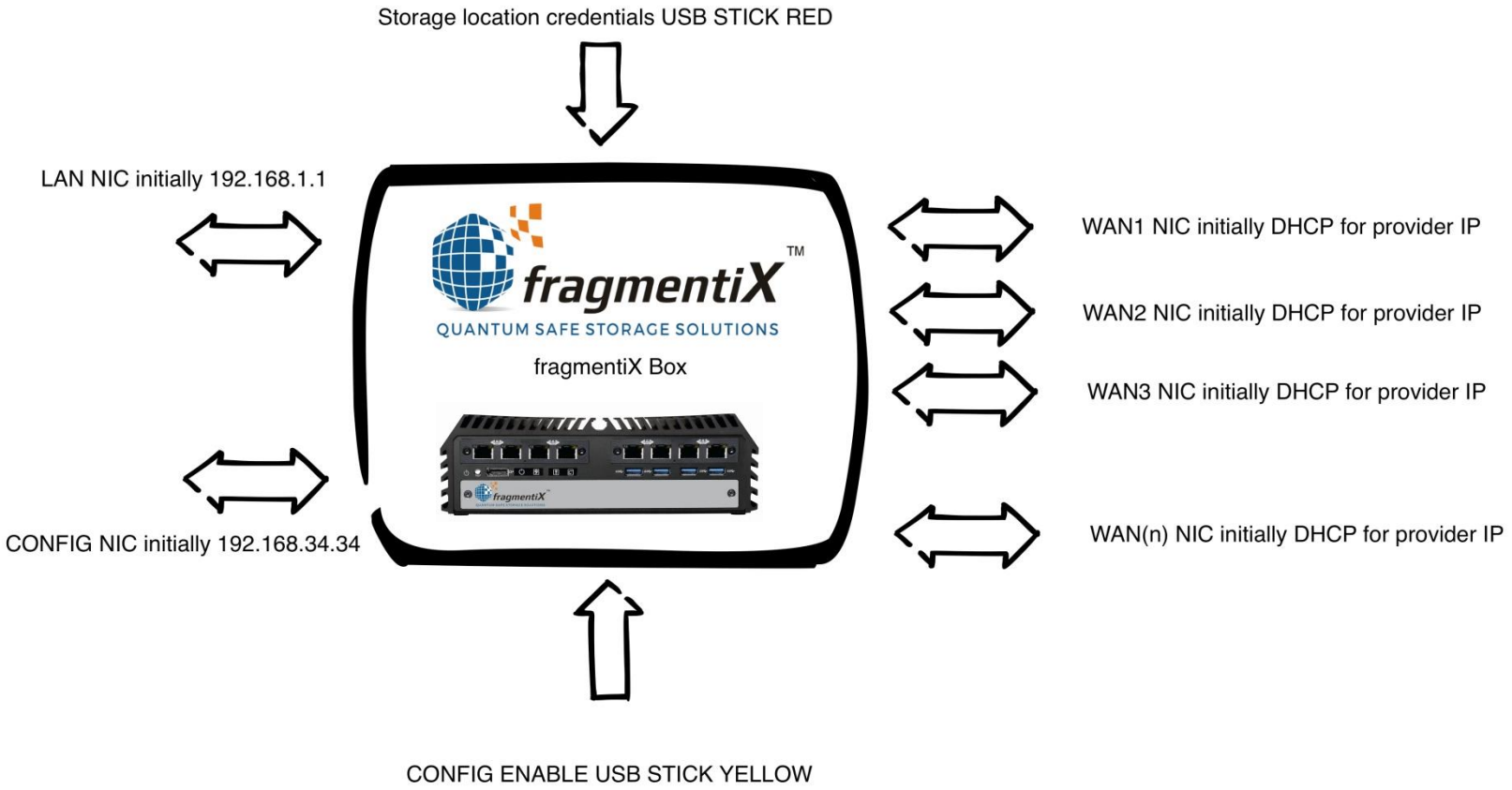
fragmentiX FOUR



2 x LAN Schnittstellen (1 x LAN als Netzlaufwerk, 1 x CONFIG ONLY)
8 x WAN Schnittstellen zur Nutzung multipler Internetzugänge
Bis zu 26 adressierbarer “locations” – Cloud S3 oder USB Disk / Stick
frxOS gehärtetes Betriebssystem mit optionaler IP Paketverschleierung

Wie ?

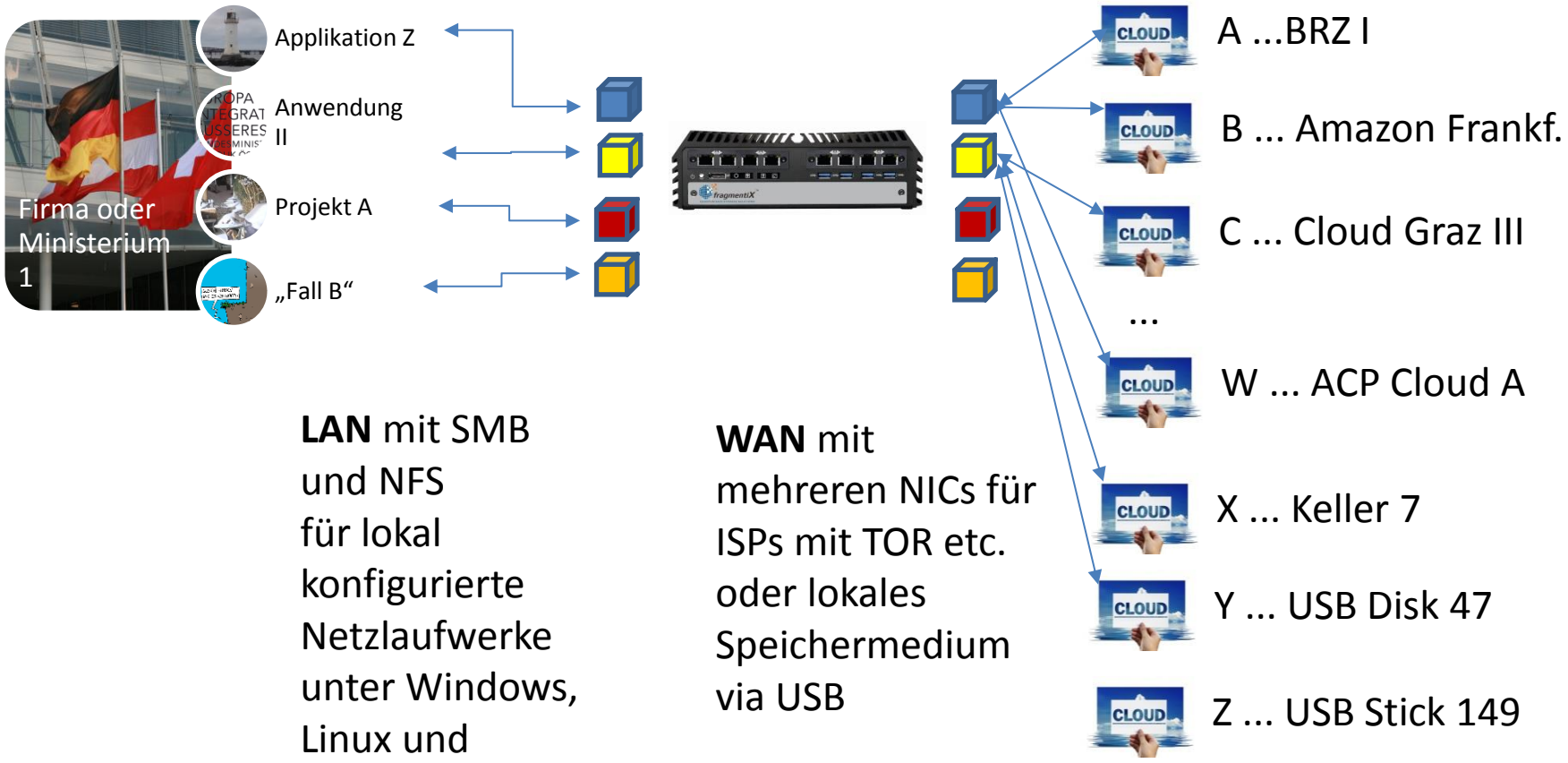
fragmentiX Anwendungsbeispiele



Wie ?

fragmentiX Anwendungsbeispiele

fragmentiX FOUR BOX mit 26 Stück S3 oder USB Speicher “locations”



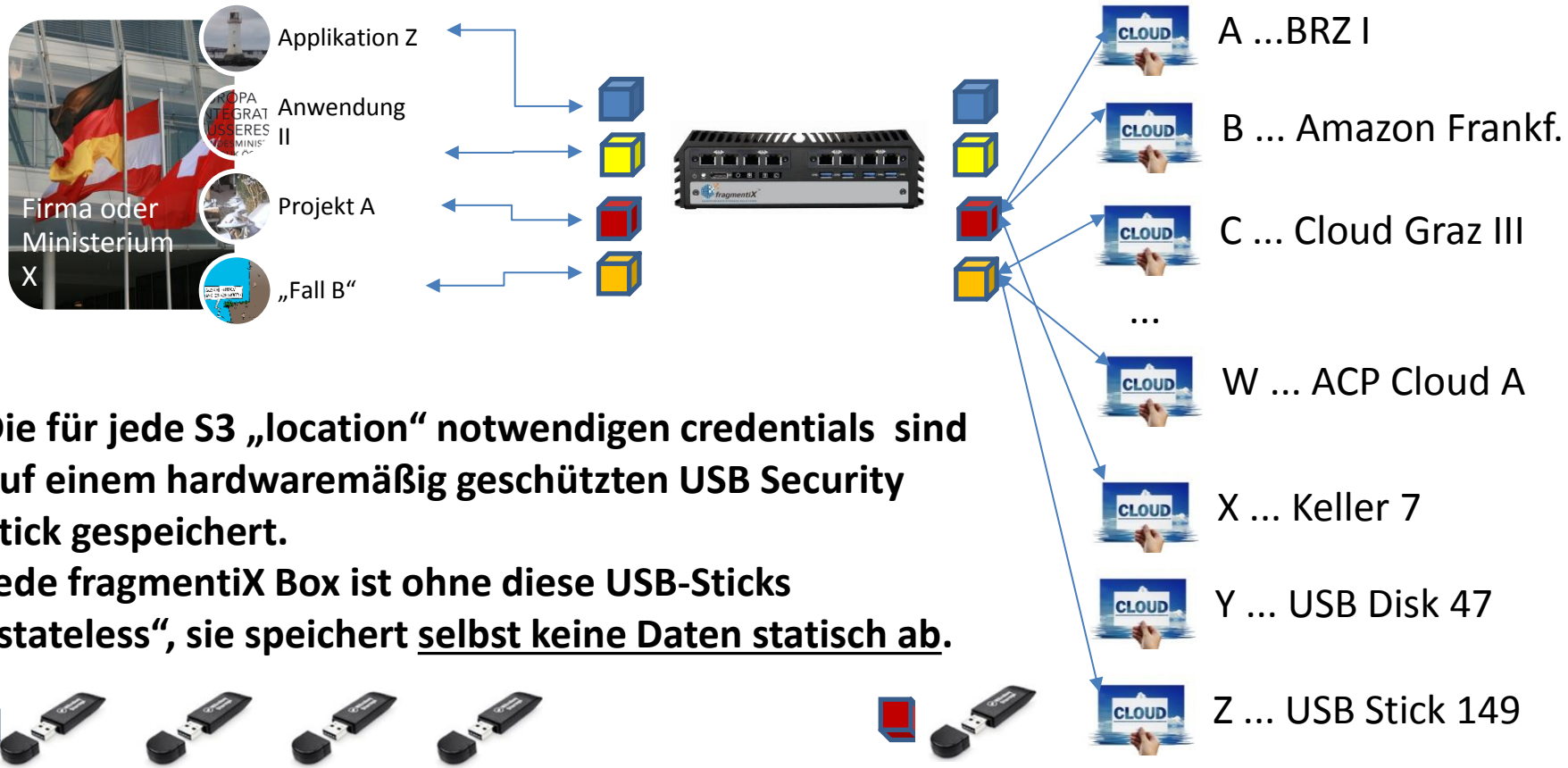
LAN mit SMB und NFS für lokal konfigurierte Netzlaufwerke unter Windows, Linux und MacOS

WAN mit mehreren NICs für ISPs mit TOR etc. oder lokales Speichermedium via USB

Wie ?

fragmentiX Anwendungsbeispiele

fragmentiX FOUR BOX mit 26 Stück S3 oder USB Speicher “locations”

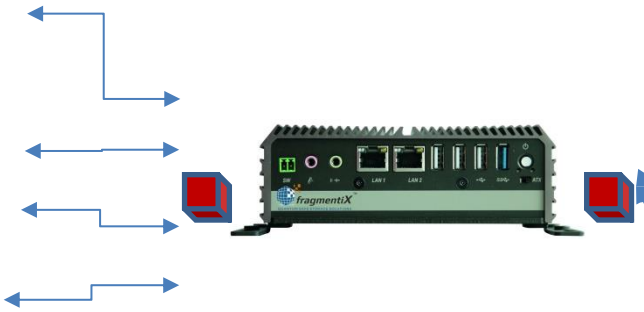


Die für jede S3 „location“ notwendigen credentials sind auf einem hardwaremäßig geschützten USB Security Stick gespeichert.
Jede fragmentiX Box ist ohne diese USB-Sticks „stateless“, sie speichert selbst keine Daten statisch ab.

Wie ?

fragmentiX Anwendungsbeispiele

fragmentiX ONE BOX mit bis zu 8 Speicher “locations” S3 oder USB



A ...BRZ I

B ... Amazon Frankf.

C ... Cloud Graz III

...

W ... ACP Cloud A

X ... Keller 7

Y ... USB Disk 47

Z ... USB Stick 149

Die für das Beispielprojekt A erforderlichen 4 Stück S3 credentials werden auf z.B. 5 ROTEN USB Security Sticks gespeichert und an 5 verschiedenen Orten mit fragmentiX ONE Boxen genutzt um jeweils auf die „Projekt A“ Daten zugreifen zu können ab.

Welche Leistungen bekommen fragmentiX Kunden?

- Die Softwareupdates und Security patches werden innerhalb der ersten 12 Monate ab Kaufdatum kostenlos zur Verfügung gestellt
- Danach steht für 15% des Produktpreise jährlich eine Update Service zur Verfügung
- Zusätzliche Maßnahmen zur Verbesserung und Erlangung weitest möglicher Digitaler Souveränität werden erklärt und empfohlen.

Wie ?

Zusätzliche Dienstleistungen

Eine große Anzahl von fragmentiX Anwendern wird gemeinsam einen sehr großen Bedarf an S3 kompatiblem Public Cloud Storage haben:

Durch ein von fragmentiX koordiniertes gemeinsames Einkaufen von Speicherkontingenten können für jeden Anwender deutlich günstigere Preise pro TB erzielt werden.

sales@fragmentix.com

oder

ws@fragmentix.com
+436643258896