Be Digital. Be Secure

Sicher in Public Clouds mit Securosys

Robert Rogenmoser
CEO Securosys SA

securosys

20/11/2023

Securing Digital Services and Cloud Systems

”Business interactions are built on trust”

In the digital world Encryption & Digital Signatures provide this trust

Encryption and digital signature are only as good as the KEYS used:

- How were the KEYS generated?
- Where are the KEYS stored?
- Who can access the KEYS?

Hardware Security Modules (HSM) protect your Keys

If I have your KEYS:

- I can sign for you – I can impersonate you
- I can spend your money
- I can read and modify your documents

© Securosys – Data Sovereignty and Privacy in Public Clouds

Keep your Keys separate from Public Cloud Providers

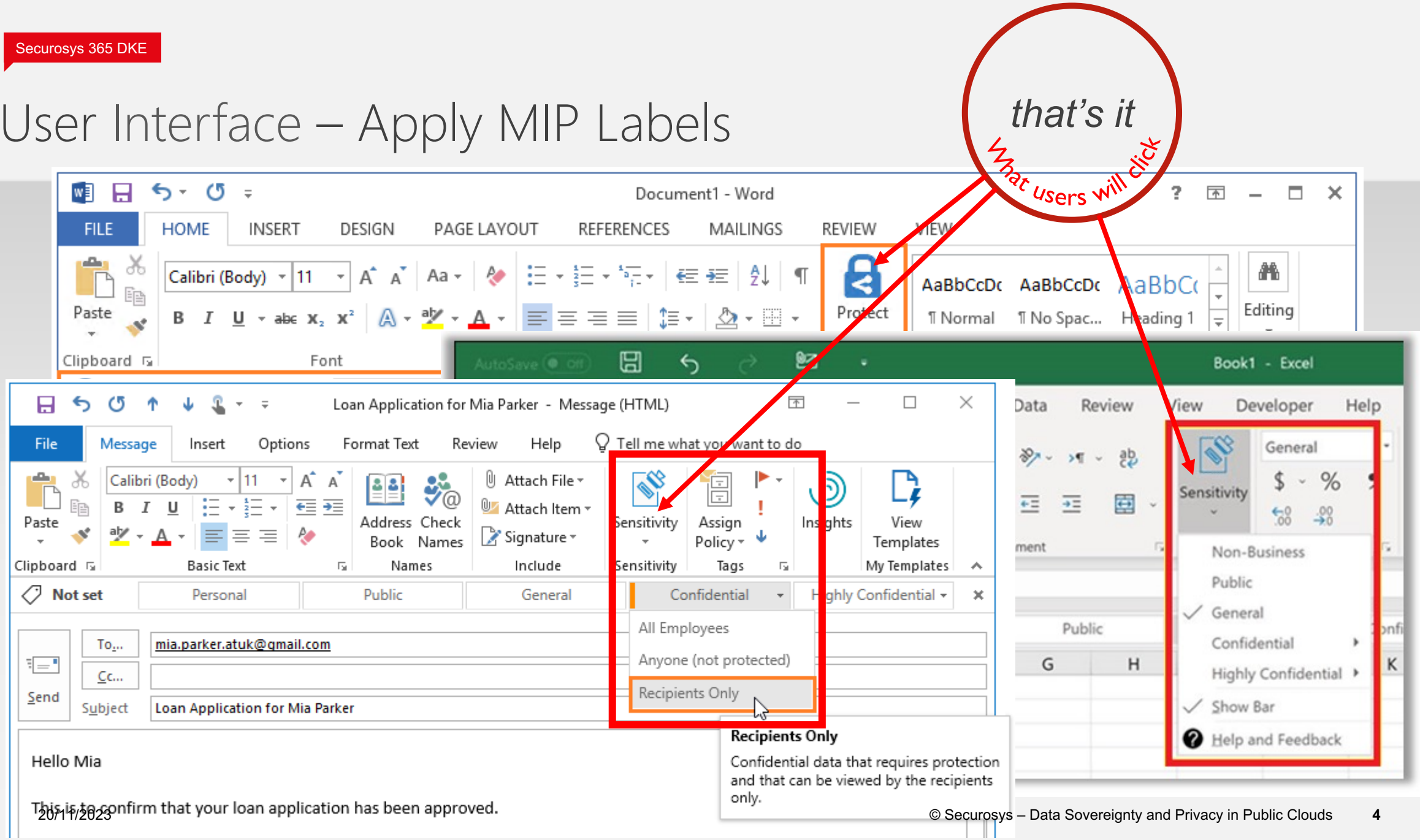
Securosys 365 DKE for Microsoft 365
(DKE: Double Key Encryption
HSM: Hardware Security Module)

- 16 Jul 2020: Court of Justice of the EU (CJEU):
  - "US cloud services are incapable of complying with the GDPR and EU privacy laws"
- Oct 2020: BSI (German Ministry for Security and IT)
  - "Cloud administrators cannot have access to customer keys." in guidelines for Cloud Providers
- 12 Mar 2021: French Conseil d'Etat on data on AWS
  - "Encryption is a sufficient safeguard, especially regarding the "triangular scheme" implemented: the encryption key is held exclusively by a trusted third party."
- Swiss Federal and Cantonal Data Protection Officers: "Behörden haben nach wie vor die vollständige Verantwortung für ihre Daten und dürfen betroffene Personen nicht schlechter stellen, als wenn das Amt die Daten selbst verarbeitet – etwa weil diese einem Land mit nicht angemessenem Datenschutz zufallen könnten."

  "der juristische Weg in die Cloud lässt sich nicht abkürzen"

© Securosys – Data Sovereignty and Privacy in Public Clouds

User Interface – Apply MIP Labels



© Securosys – Data Sovereignty and Privacy in Public Clouds

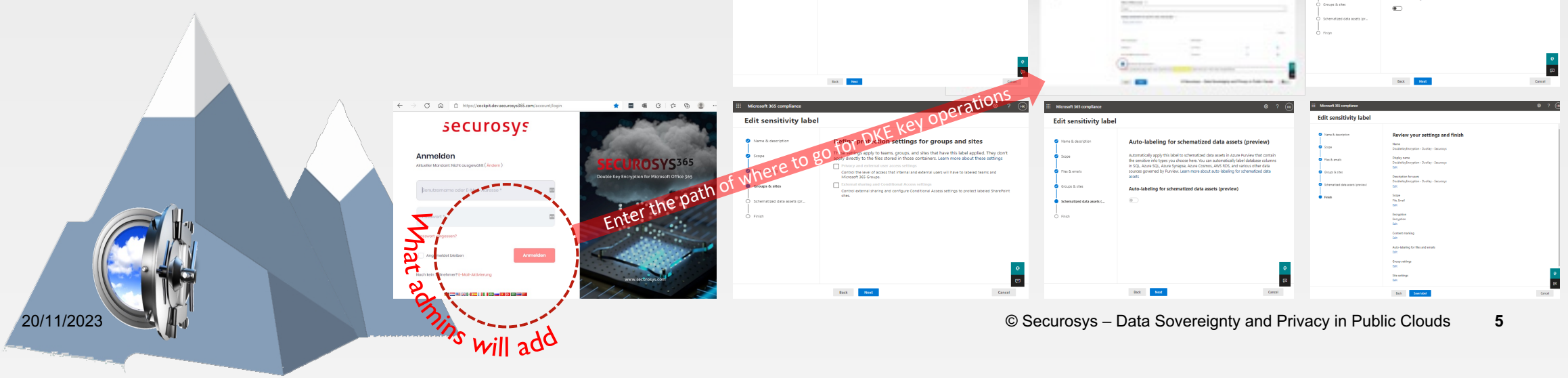
Administrator GUIs – Add a Securosys DKE key URL

Provided for *Microsoft Information Protection*

The one *missing link* Microsoft **cannot** provide for DKE customers – by design.

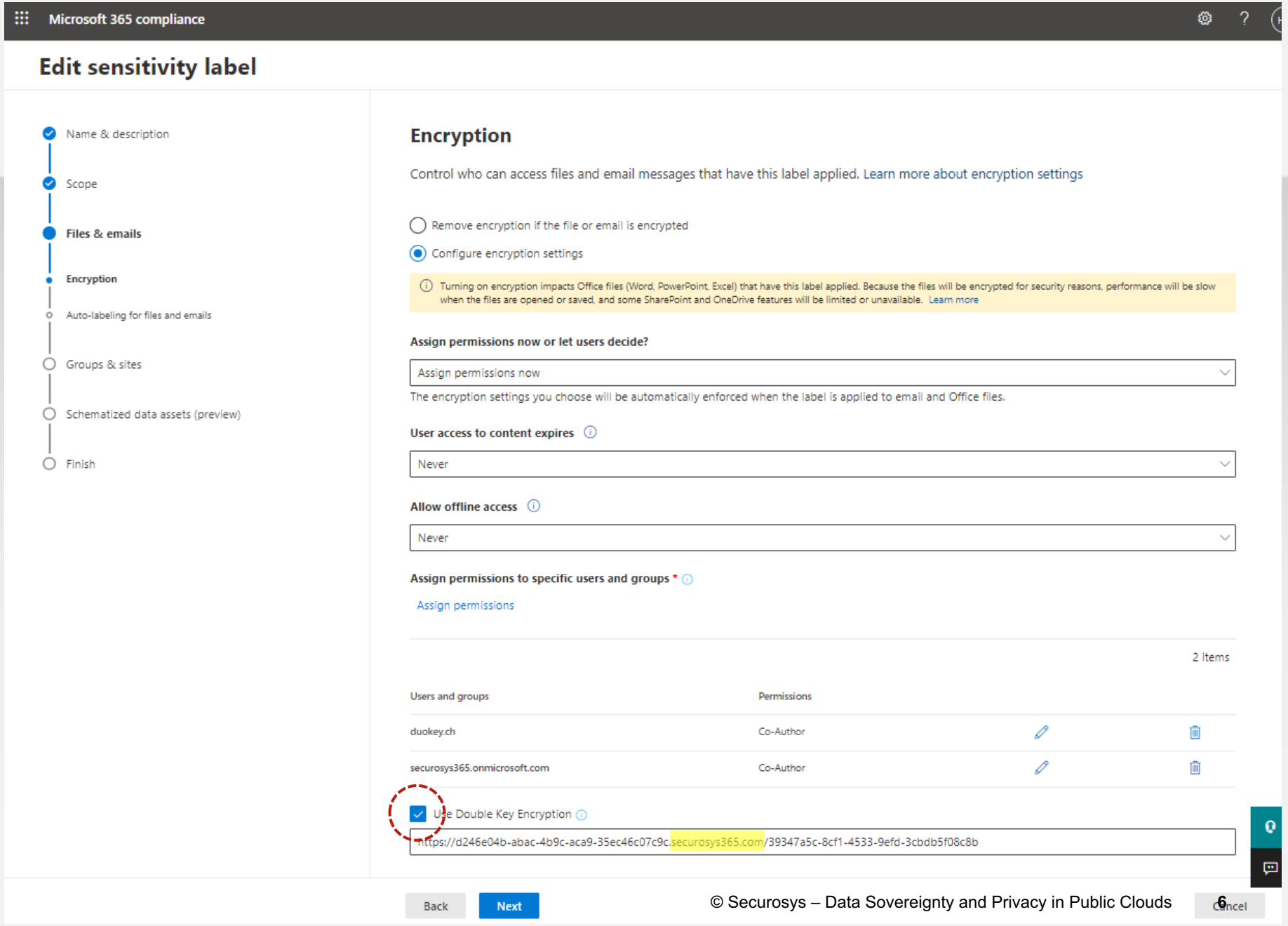
Microsoft Information Protection is powerful, elaborated and complete.

Double Key Encryption adds tailor made privacy by checking a box and adding an URL

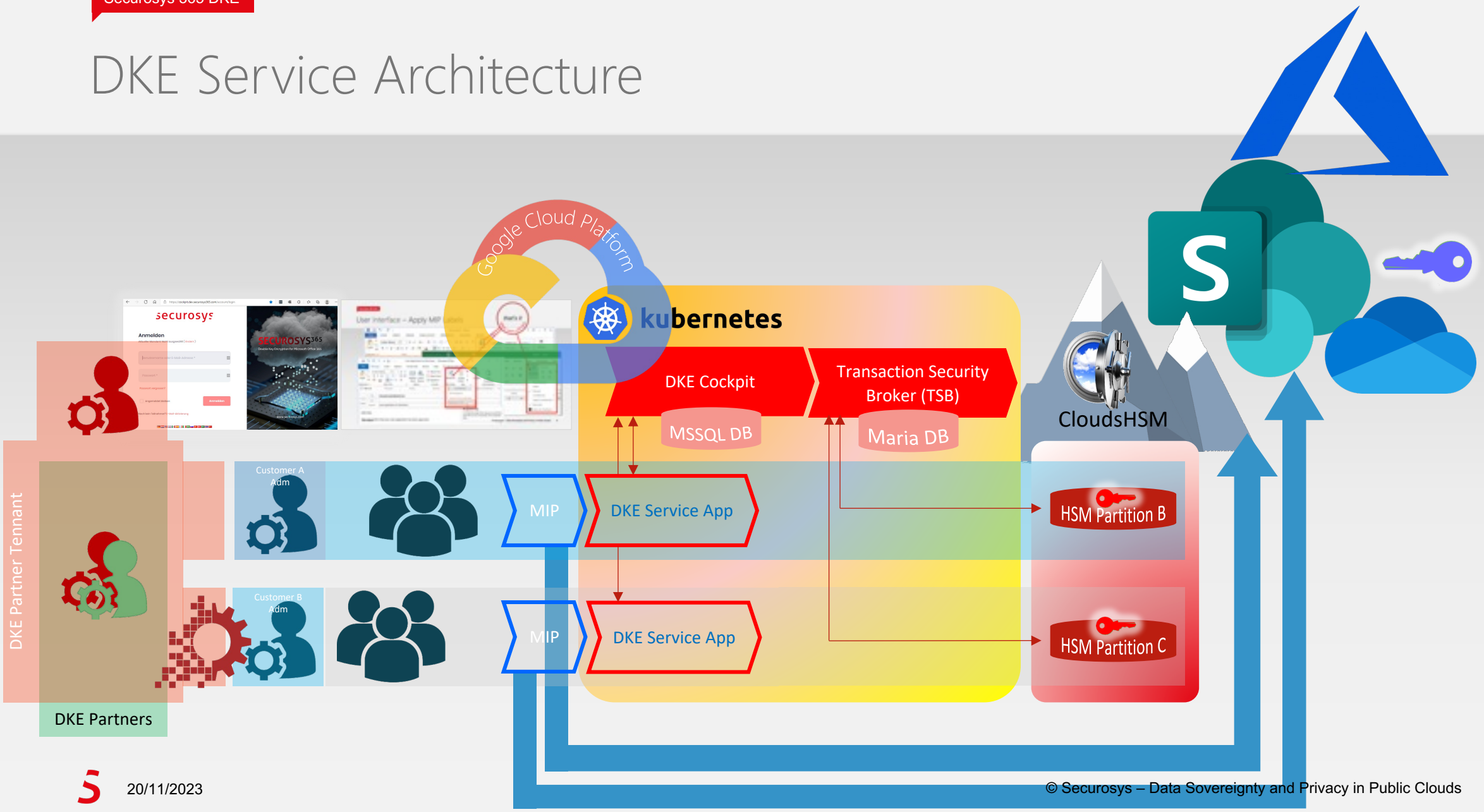


Securosys 365 DKE

The DKE Core



DKE Service Architecture

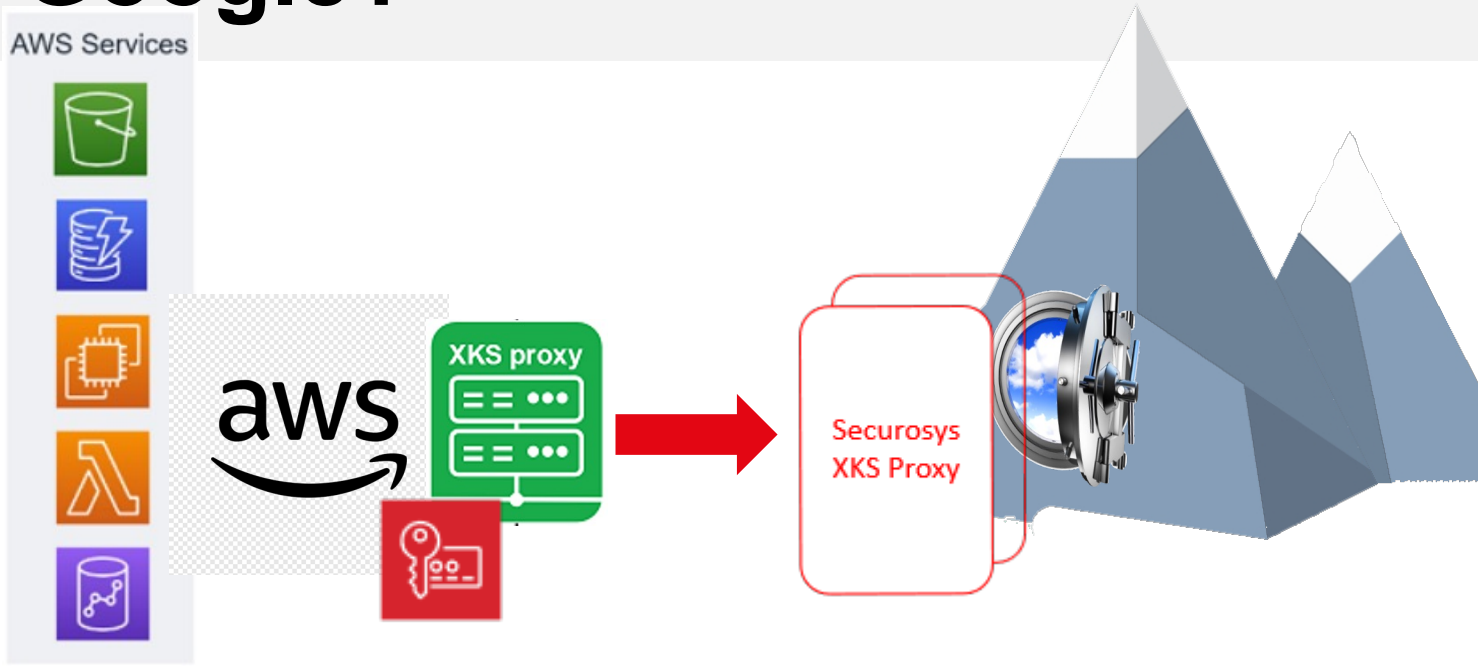


© Securosys – Data Sovereignty and Privacy in Public Clouds

How about AWS and Google?

AWS – Amazon Web Services

- AWS let's customers use an external keystore: XKS
  - Fully integrated with Securosys CloudsHSM



GCP – Google Cloud Platform

- Google Docs: CSE – Client Side Encryption: Similar solution to Microsoft DKE
  - Will be integrated with Securosys CloudsHSM Q1'2024
- Google Cloud: External Key Manager: EKM
  - Similar solution to AWS XKS
  - Securosys is looking for a GCP customer to engage for GCP-EKM

Challenges

Cloud Provider: Operations versus Compliance

- The operations teams wants no external dependencies – having signature and encryption keys offsite is a problem for them
- The compliance teams wants to offer solutions that conform to regulations such as GDPR

Customer: Additional Cost

- An external keystore is not free
- Microsoft requires a more expensive license for DKE (e5 instead of e3)

Customer: Acceptance, missing processes

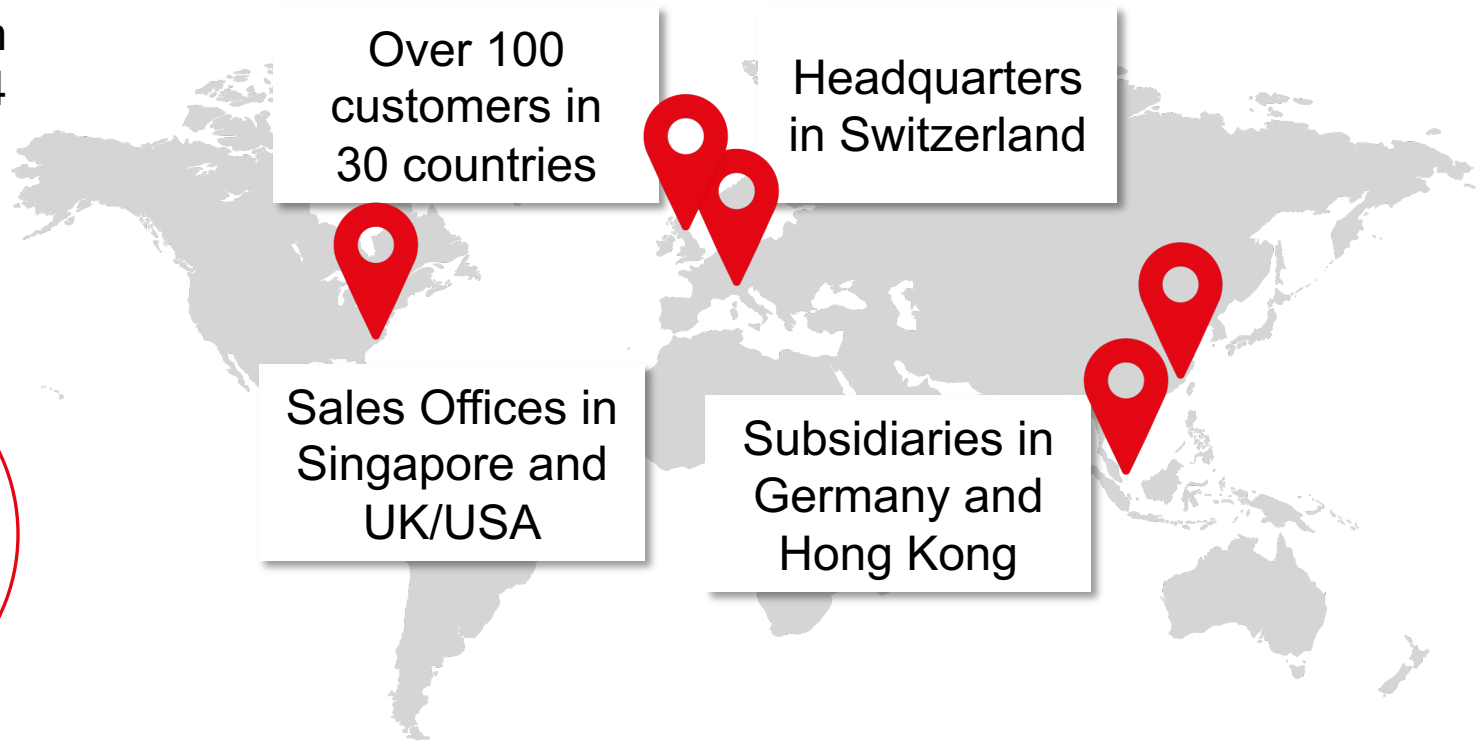
- Customers need to classify data
- Each employee who interacts with data has to be trained on classification and respective processes

We secure data and communications.

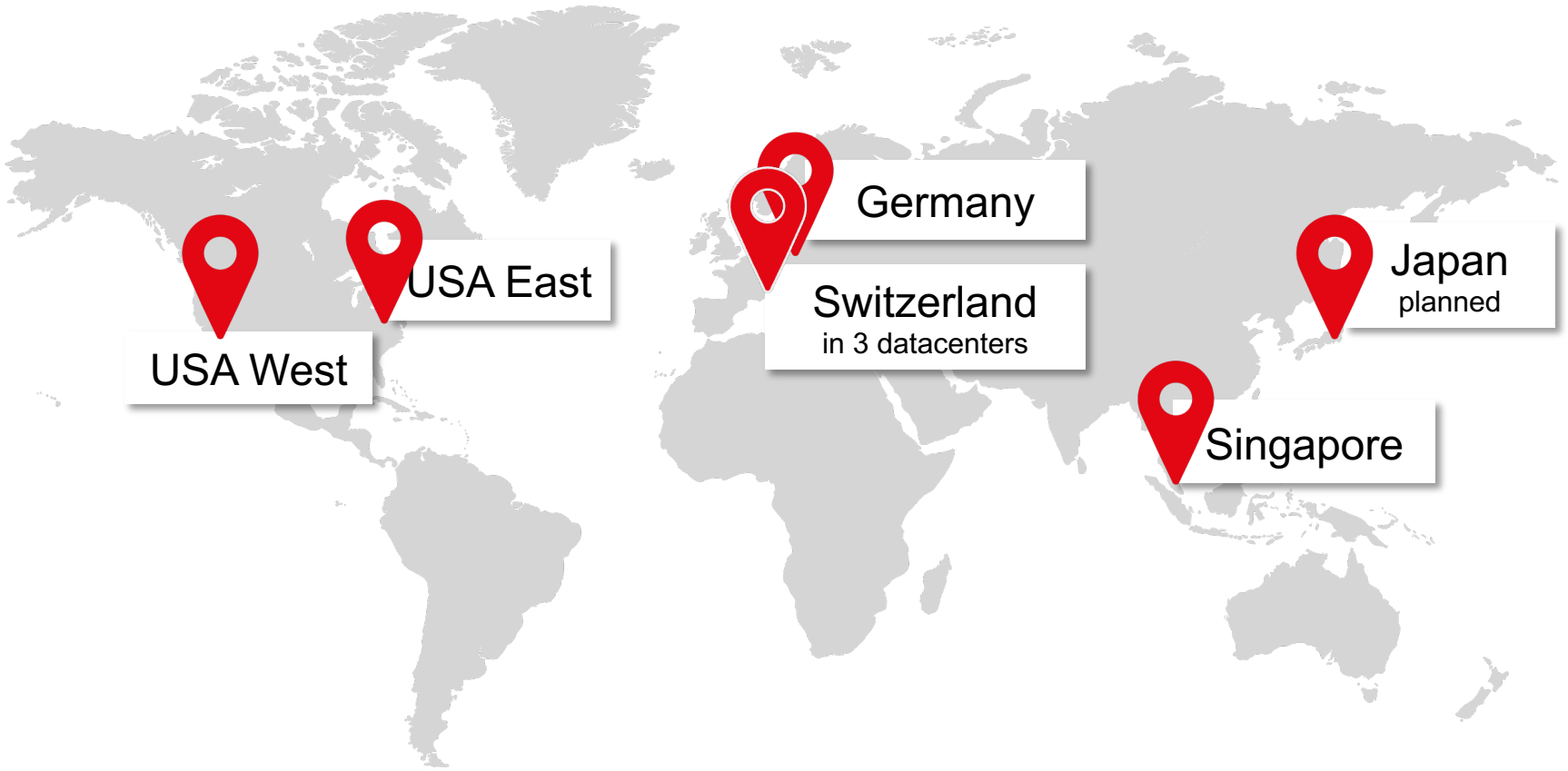
Founded in 2014

Owned by founders, employees, and Swiss private investors

Securing the Swiss Banking System (SIC) and Stock Market (SIX) with over CHF/USD/€100B in daily transactions



HSM as a Service.



Trusted Provider
Separation of duties

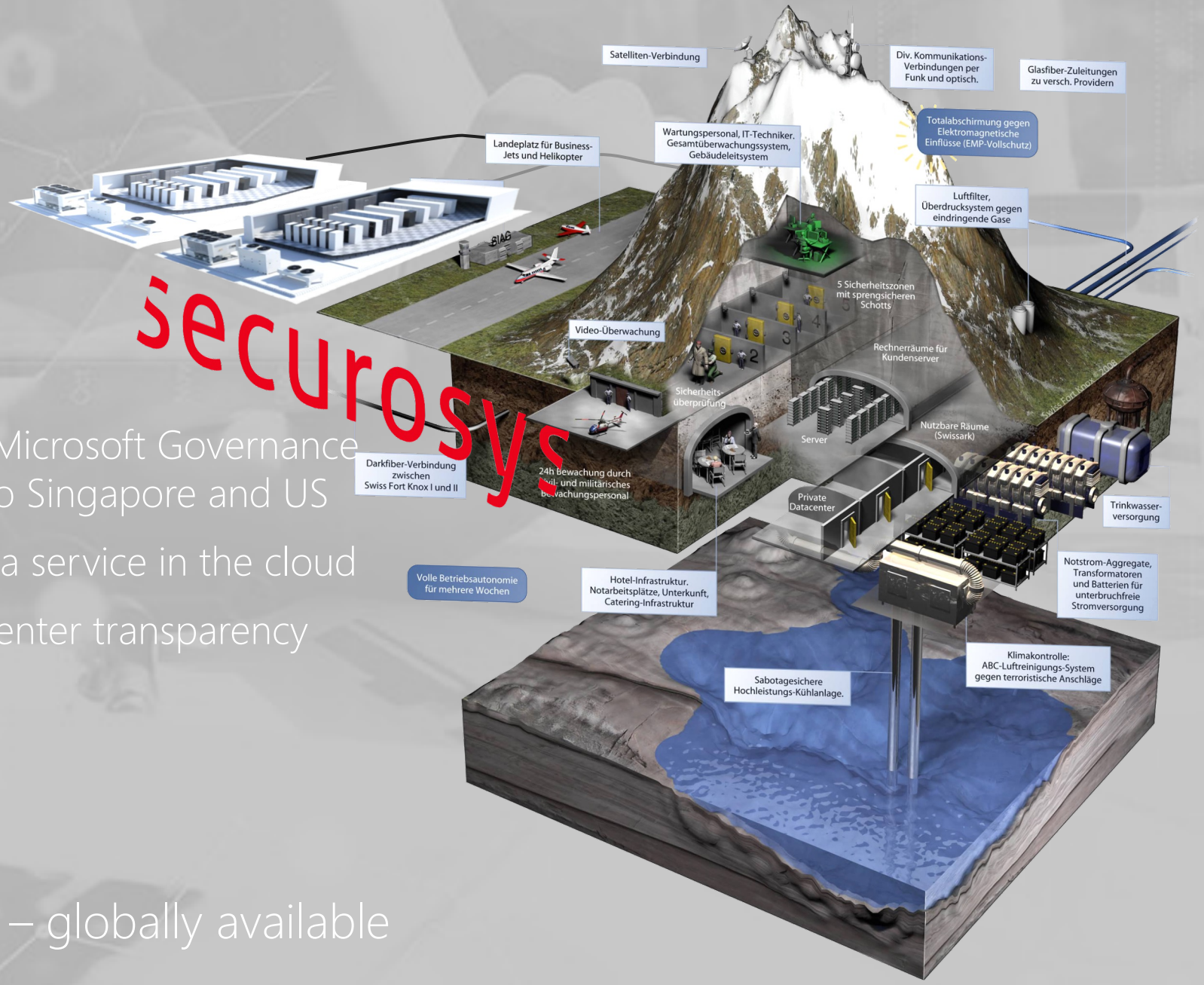
Certifications
ISO 27001, ISO 9001
FIPS 140-2 Level 3
Common Criteria EAL 4+

Redundant HSM Clusters:
Local, Regional, and Global

Securosys 365 DKE

We Do Cloud

- Adding Securosys encryption to Microsoft Governance *Keys as a Service* – from DACH to Singapore and US
- Manage your encryption keys as a service in the cloud
- Highest level of security by datacenter transparency and built-in governance



Securosys Keys as a Service – globally available

We strive towards our vision.

A digital world where data is secured, identities are protected and privacy is guaranteed.

Call to action

Be digital.
Be secure.

securosys

Let’s talk about cooperation.

Contact

Securosys SA
Max-Högger-Strasse 2
8048 Zürich
Schweiz

securosys

Different ...

- Designed & produced in Switzerland
- Quick setup, simple operation, and management
- Automated clustering and failover
- Modern APIs and interfaces (REST)
- Seamless certifications

© Securosys – Data Sovereignty and Privacy in Public Clouds

The digital world is changing constantly and leads to growing challenges for all businesses.

Protect your digital systems to safeguard your

- Finances
- Identities
- Reputation

Securosys HSM protect your systems and applications.

Securosys 365 DKE

Double Key Encryption

- **Two keys needed** for *Microsoft 365* files
- No content accessible without applying both keys
- One key from *Microsoft* another one from *Securosys*
- Client processing: content always encrypted twice

The safe deposit box made available by secure keys – in the right hands