Herbsttagung 2019
(Geheime) Daten in der Cloud

Zuzana Trubini
Zürich, 11.09.2019

cnlab

Agenda_

Daten in der Cloud (Datensicherheit in der Cloud)

Geheime Daten in der Cloud (Verschlüsselung und Vertraulichkeit)

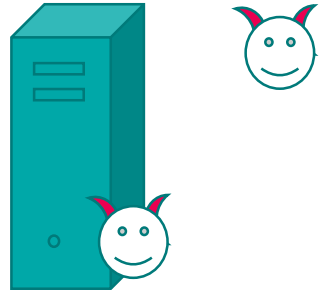
Information Right Management (IRM)

Azure Right Management Service (Azure RMS)

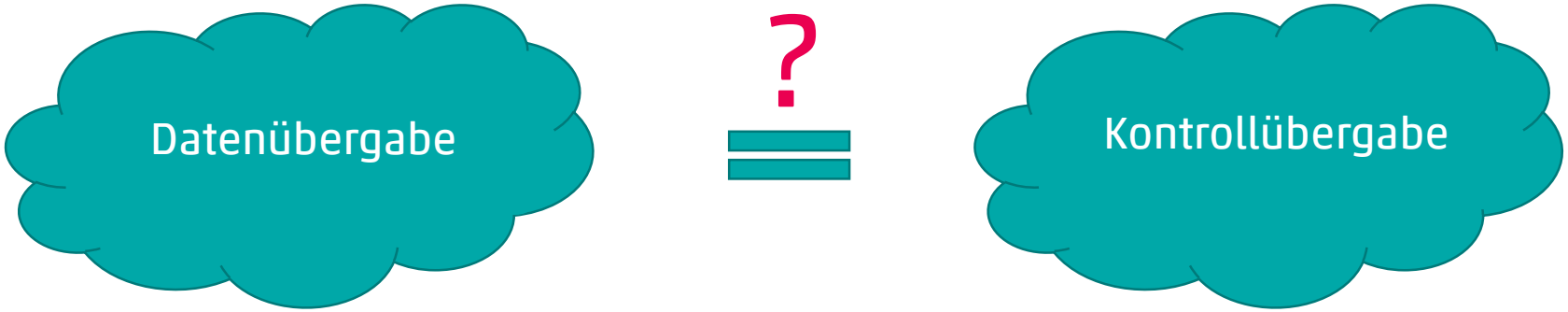
Sicherheit der Daten in der Cloud

Vorstellung

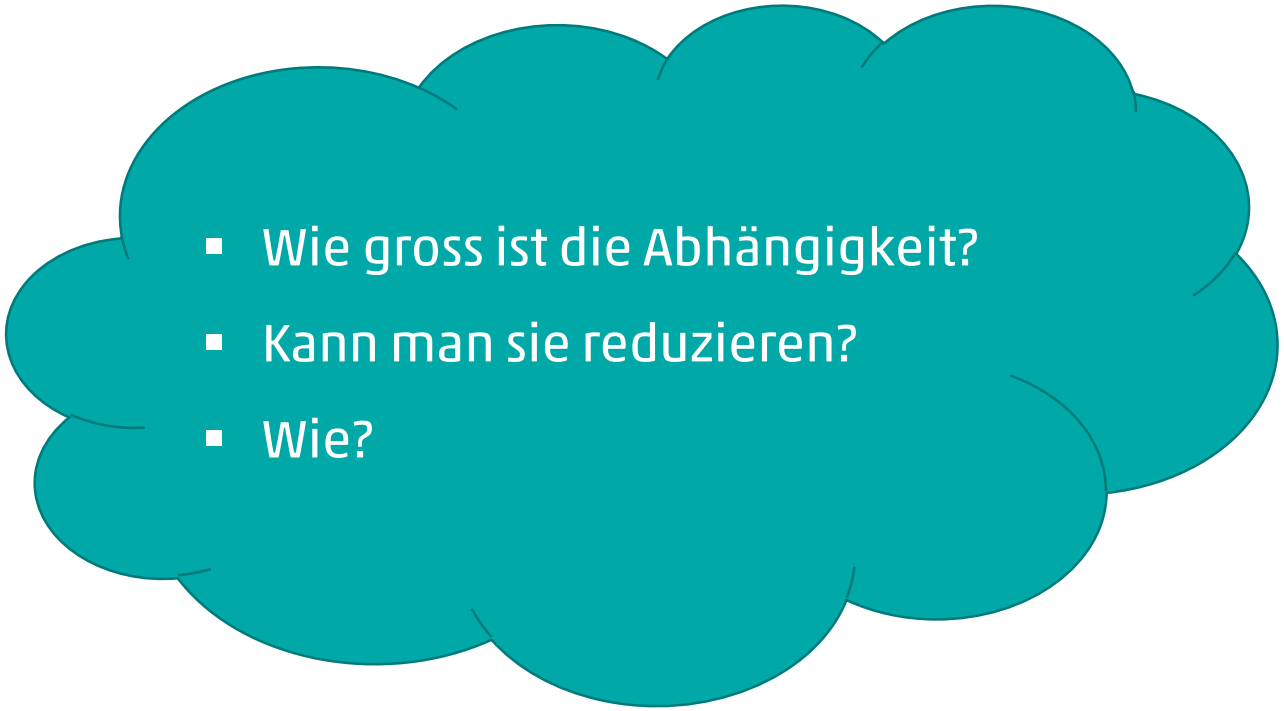
Realität



Datenhoheit



Abhängigkeit vom Cloud-Anbieter



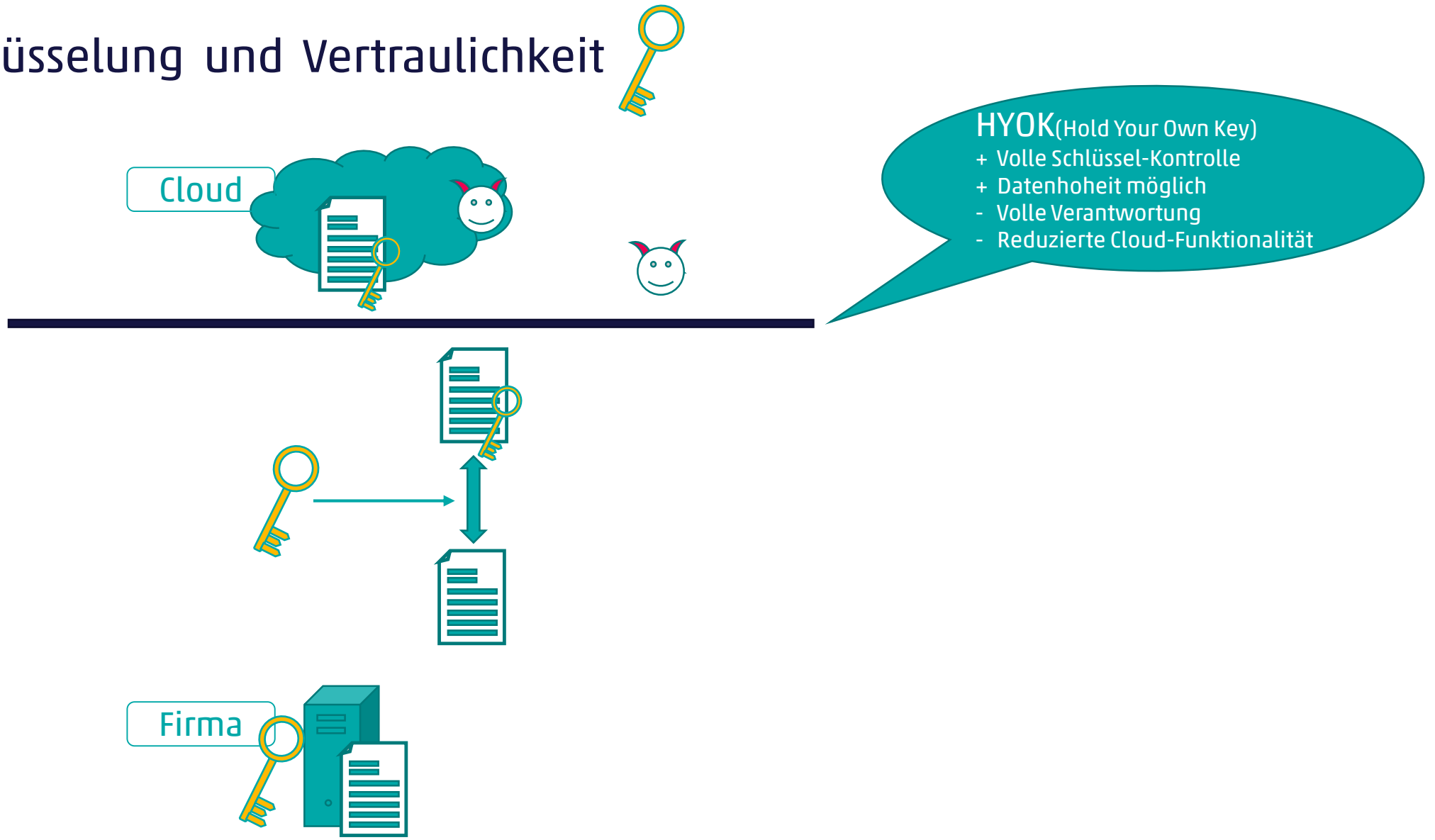
Abhängigkeit bezüglich Datensicherheit

- Verfügbarkeit - Backup, Notfall-Konzept
- Vertraulichkeit - Verschlüsselung ruhender Daten
- Integrität - Hashes, Signaturen

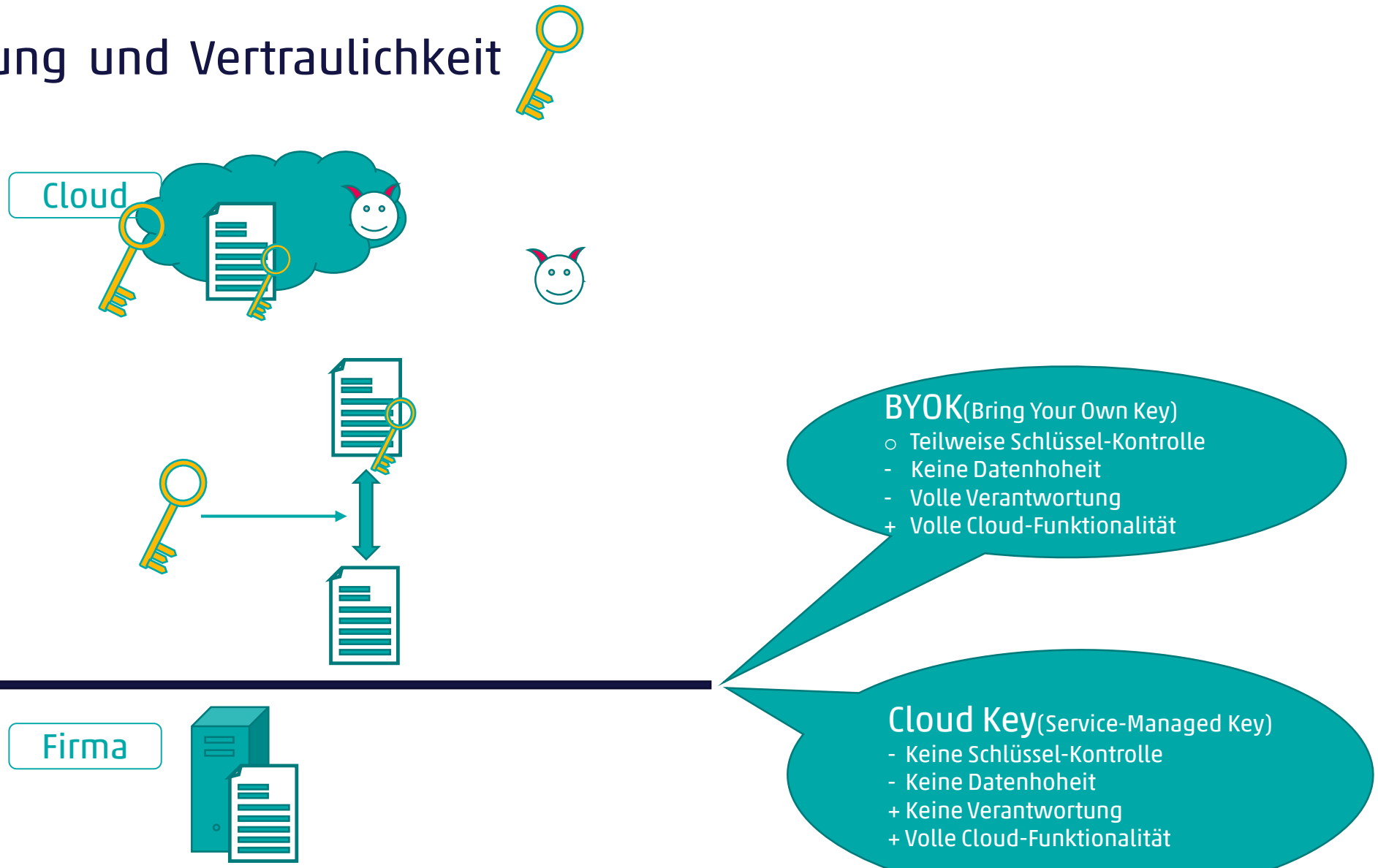
- Nachvollziehbarkeit - Logging & Auditing, Archivierung

Backup, Verschlüsselung, Logging: wird auch von den Cloud-Anbietern angeboten, löst aber das Abhängigkeitsproblem nicht.

Verschlüsselung und Vertraulichkeit



Verschlüsselung und Vertraulichkeit



Schlüsselmodelle und Vertraulichkeit

	HYOK	BYOK	Cloud Key
Charakterisierung des Modelles			
Schlüsselmanagement	Firma	Firma	Cloud
Schlüsselaufbewahrung	Firma	Firma/Cloud	Cloud
Verschlüsselung/Entschlüsselung	Firma	Cloud	Cloud
Schutzlevel (Vertraulichkeit)			
Datenhoheit bei der Firma	Ja	Nein	Nein
Schutz gegen Angriffe/Fehler in der Cloud	voll	klein	klein
▪ **Diebstahl Datenträger**	Ja	Ja	Ja
▪ **Fehlerhaftes Schlüsselmanagement**	Ja	Ja	Nein
▪ **Missbrauch von Cloud-Adminrechten (durch Cloud Mitarbeiter oder Hacker)**	Ja	Nein	Nein
▪ **Direkte Zugriffe auf «Cloudmiddleware»**	Ja	Nein	Nein

Agenda_

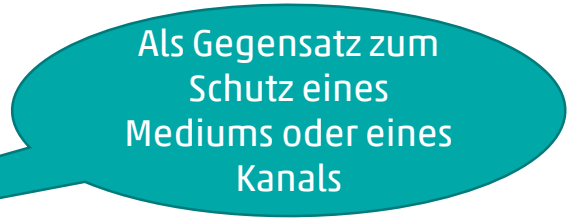
Daten in der Cloud (Datensicherheit in der Cloud)

Geheime Daten in der Cloud (Verschlüsselung und Vertraulichkeit)

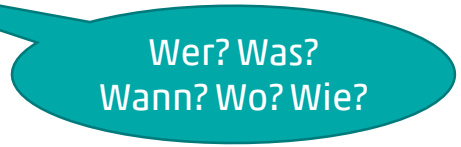
Information Right Management (IRM)

Azure Right Management Service (Azure RMS)

Information Right Management (IRM)

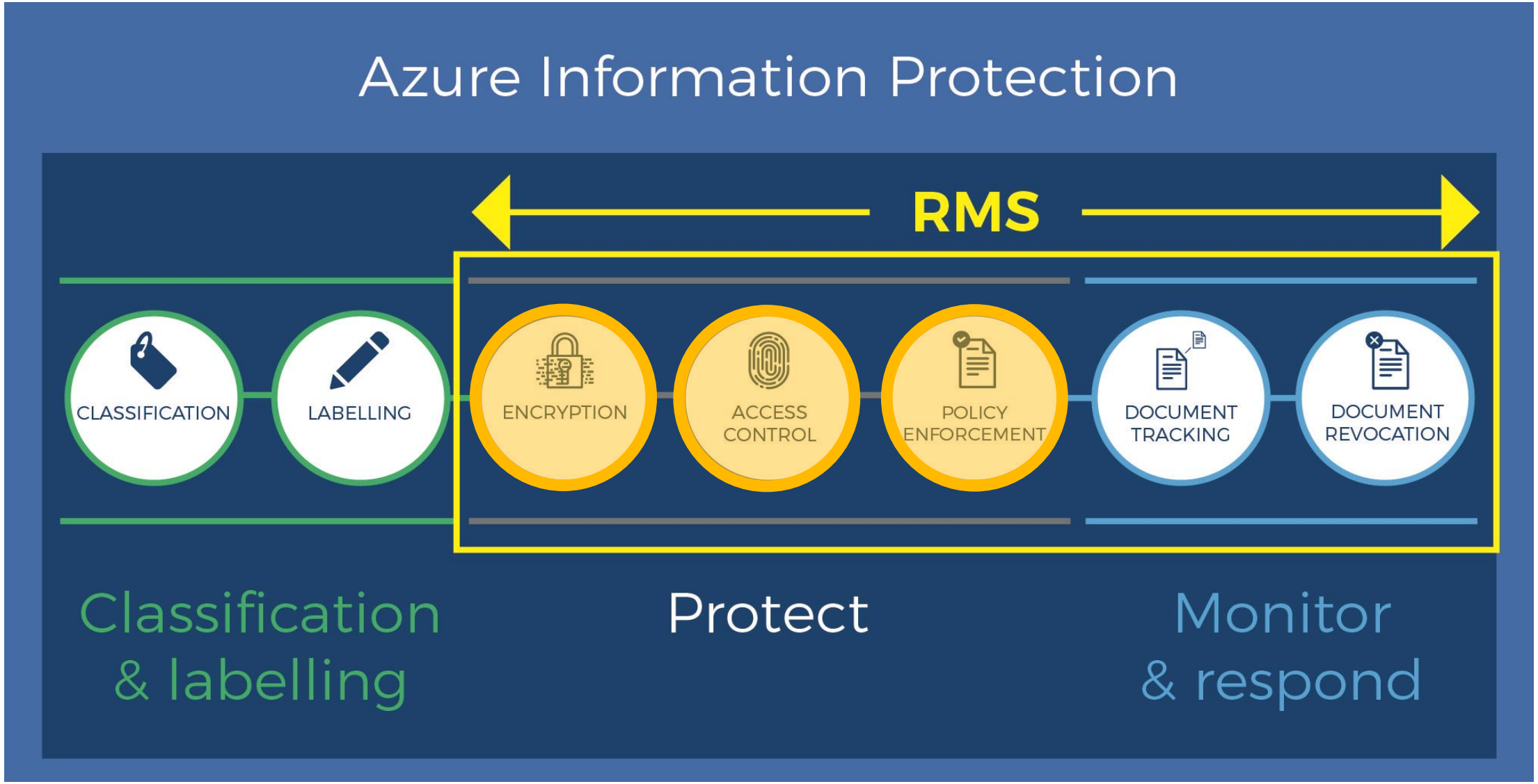


- **Bedeutung:**
  - **Datenzentrischer Schutz** von Informationen während dem gesamten Lebenszyklus
  - Dokument wird verschlüsselt und mit einer Policy versehen, so dass der Schutz beim Dokument bleibt
  - Verschlüsselung und Zugriffs- & Verwendungskontrolle

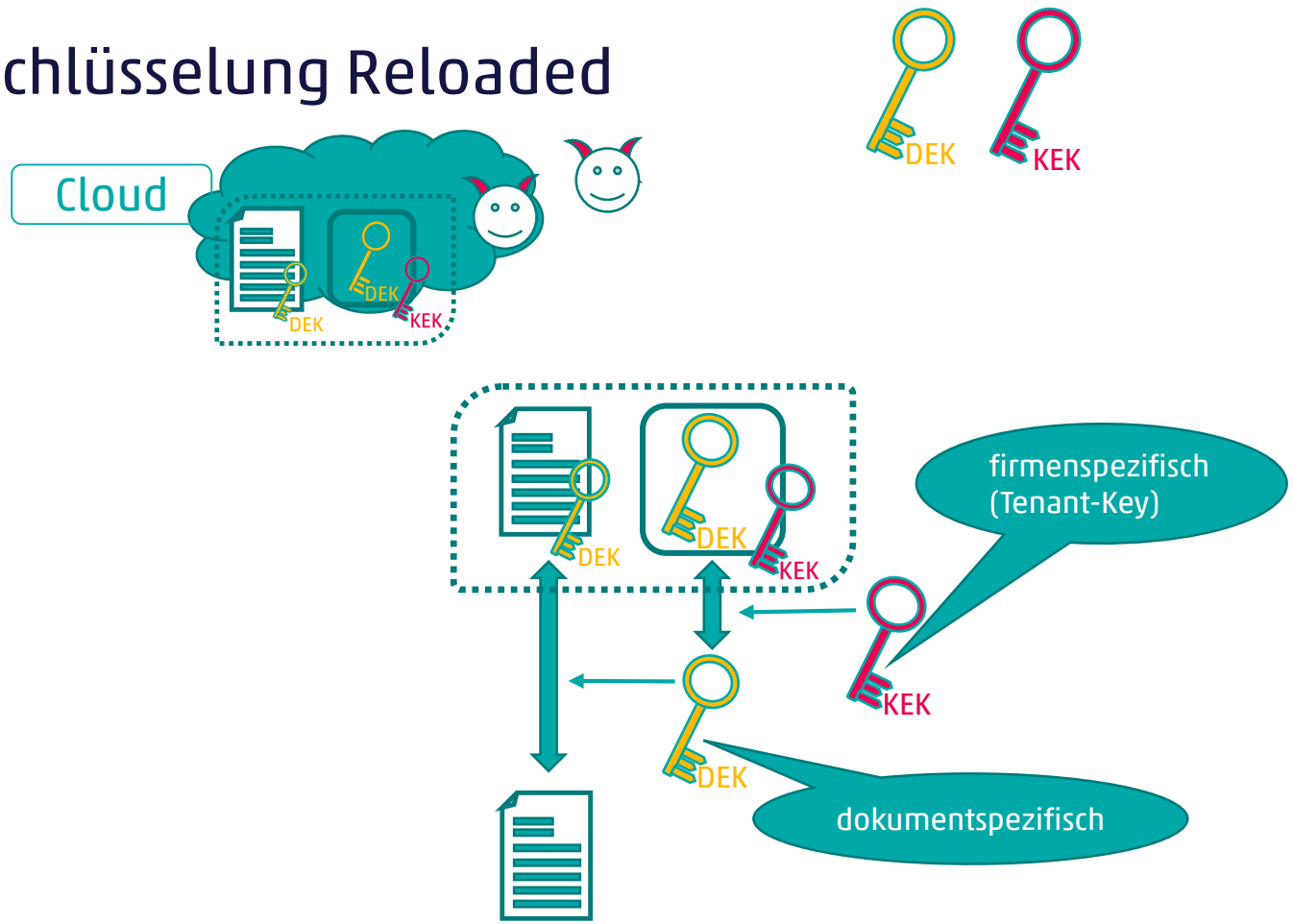


- **Alternative Bezeichnungen:**
  - Digital Right Management (DRM) → eher Urheberrecht
  - Enterprise Digital Right Management (EDRM)
  - Document Right Management (DRM)
- **Zusammenhang mit Cloud**
  - Nicht direkt, aber …
- **Beispiel: Azure Right Management Service (Azure RMS)**

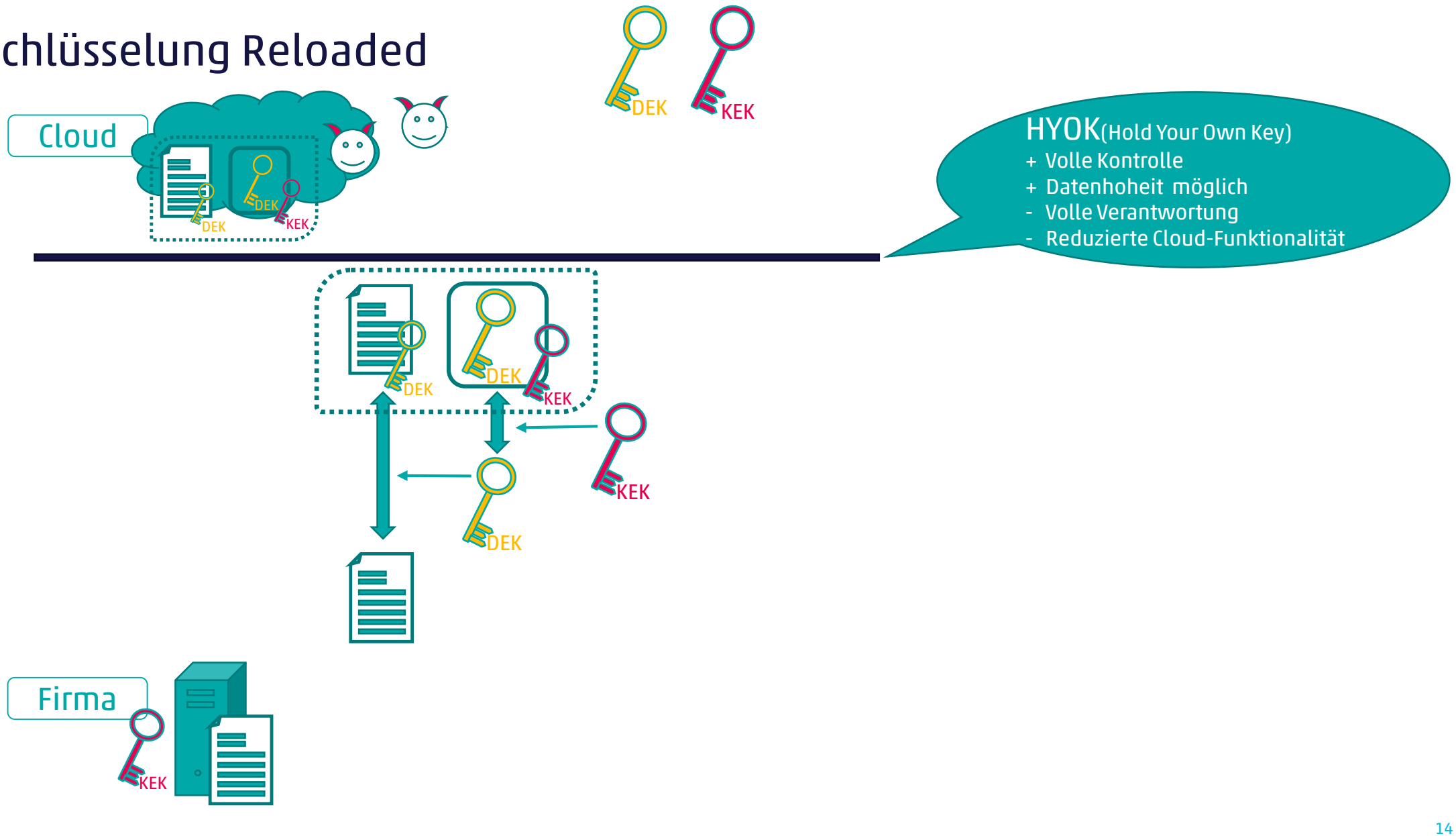
Azure RMS (als Teil von AIP)



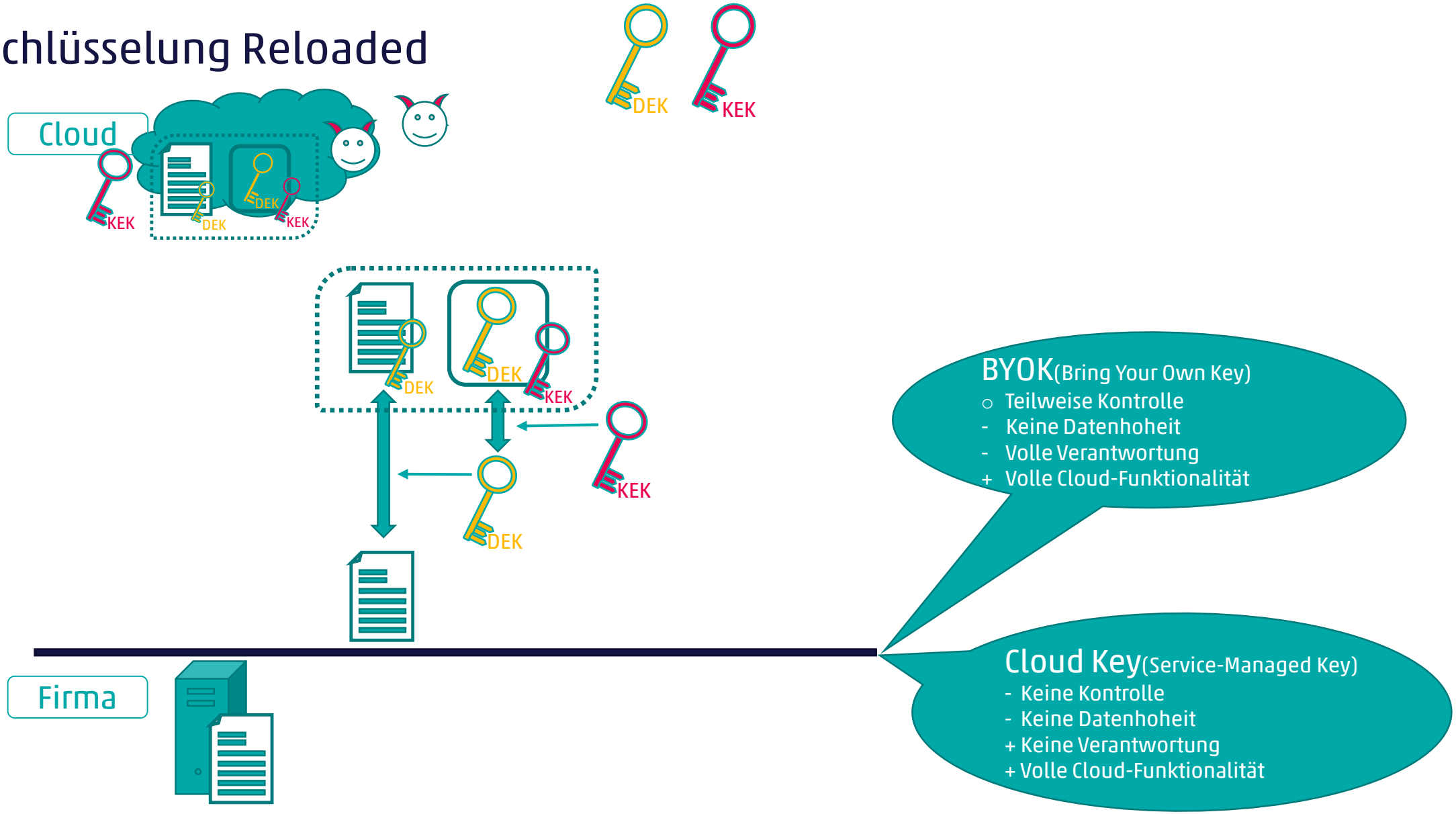
Verschlüsselung Reloaded



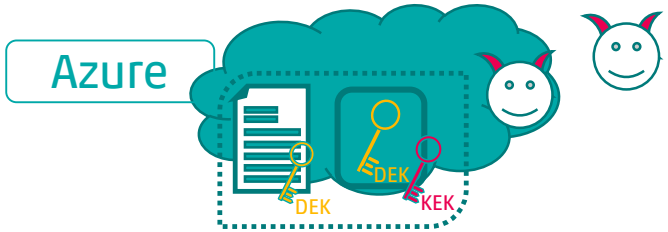
Verschlüsselung Reloaded

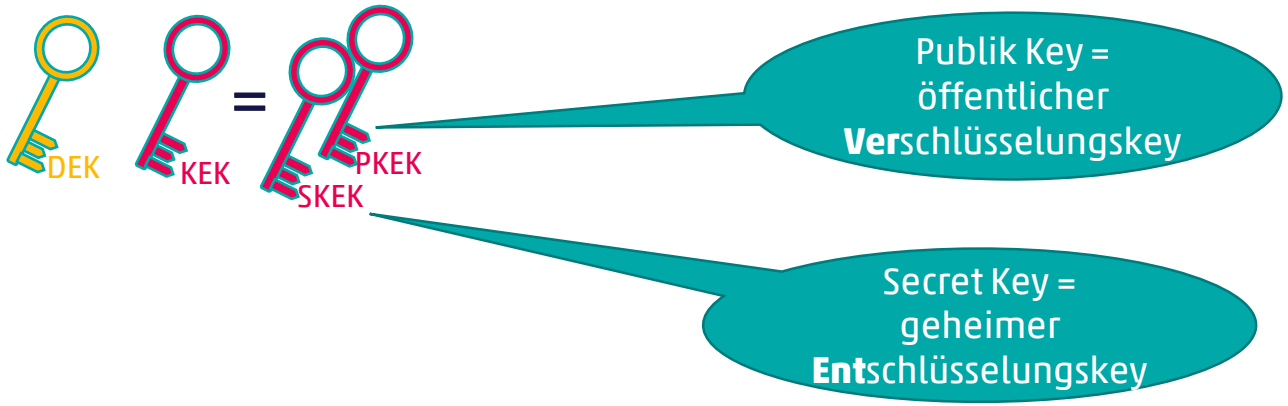


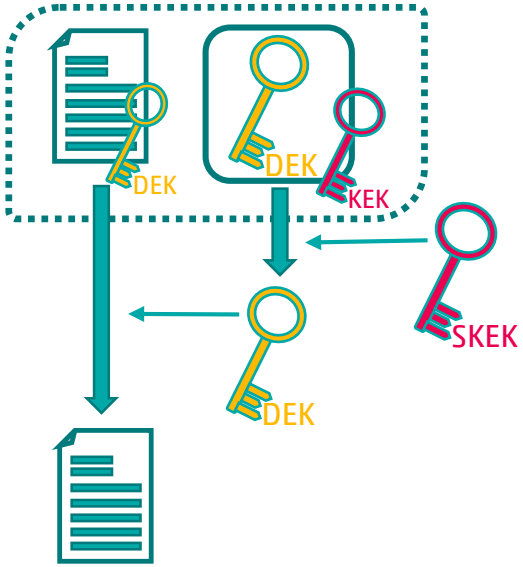
Verschlüsselung Reloaded

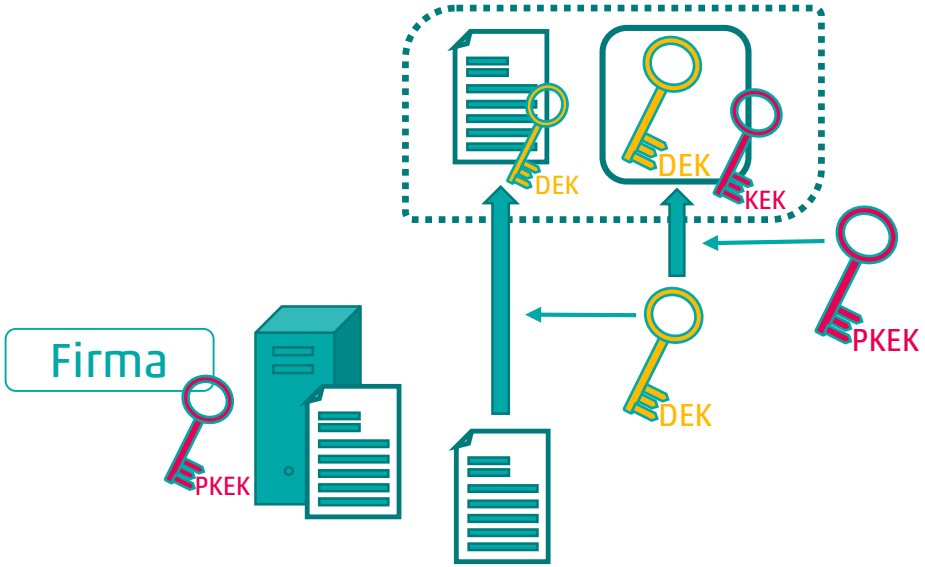


Verschlüsselung bei Azure

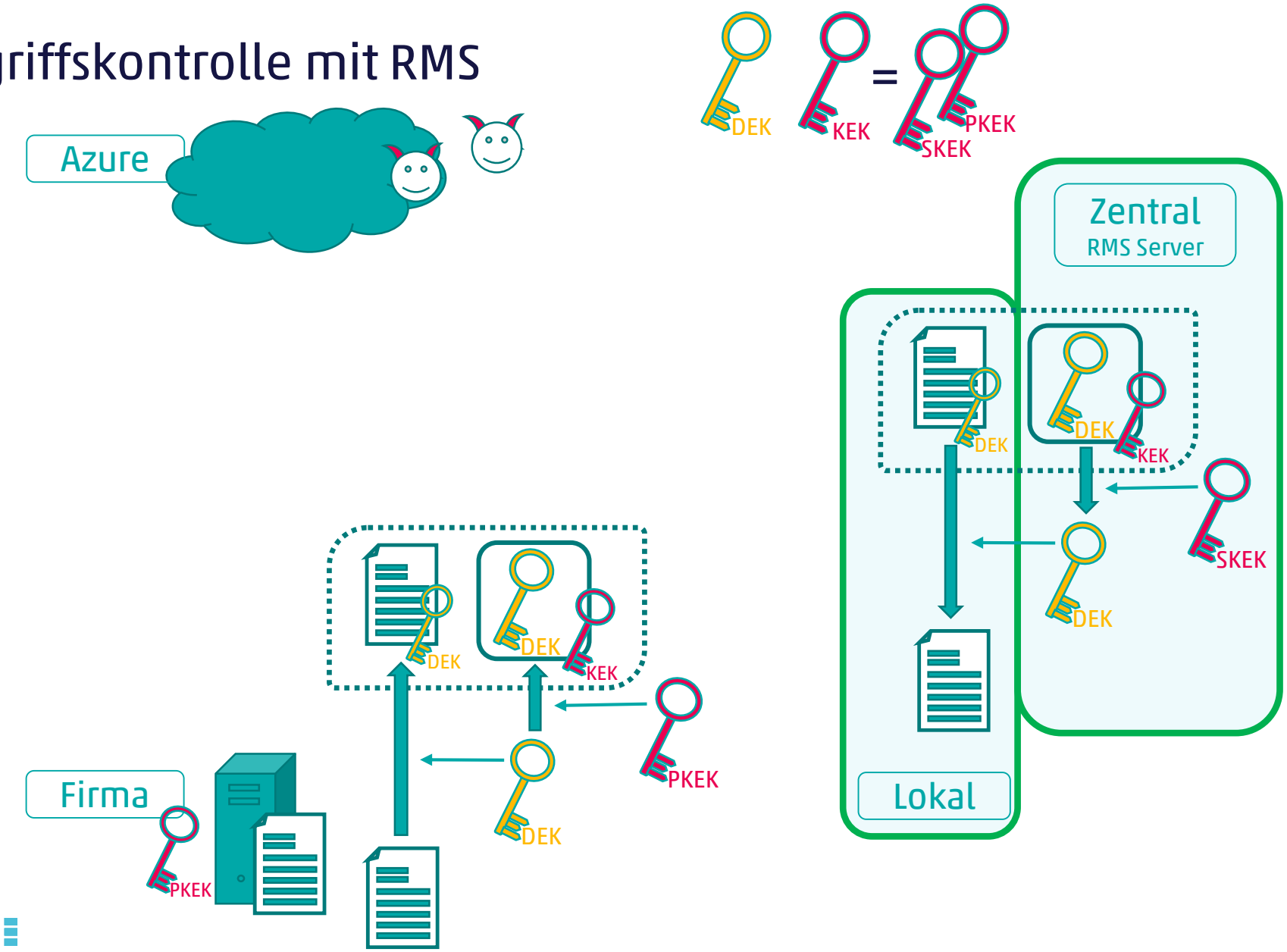




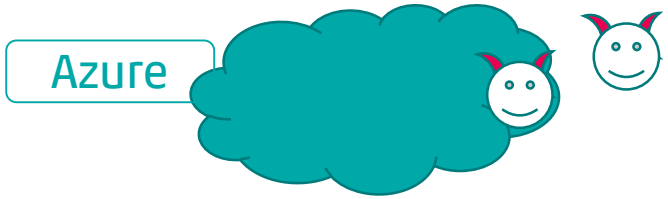


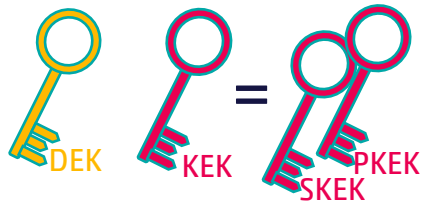


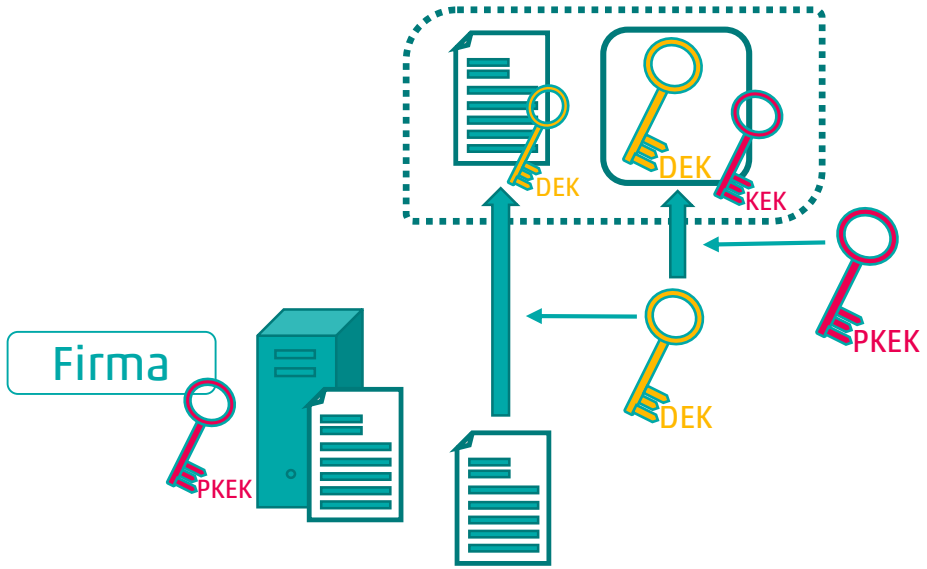
Zugriffskontrolle mit RMS

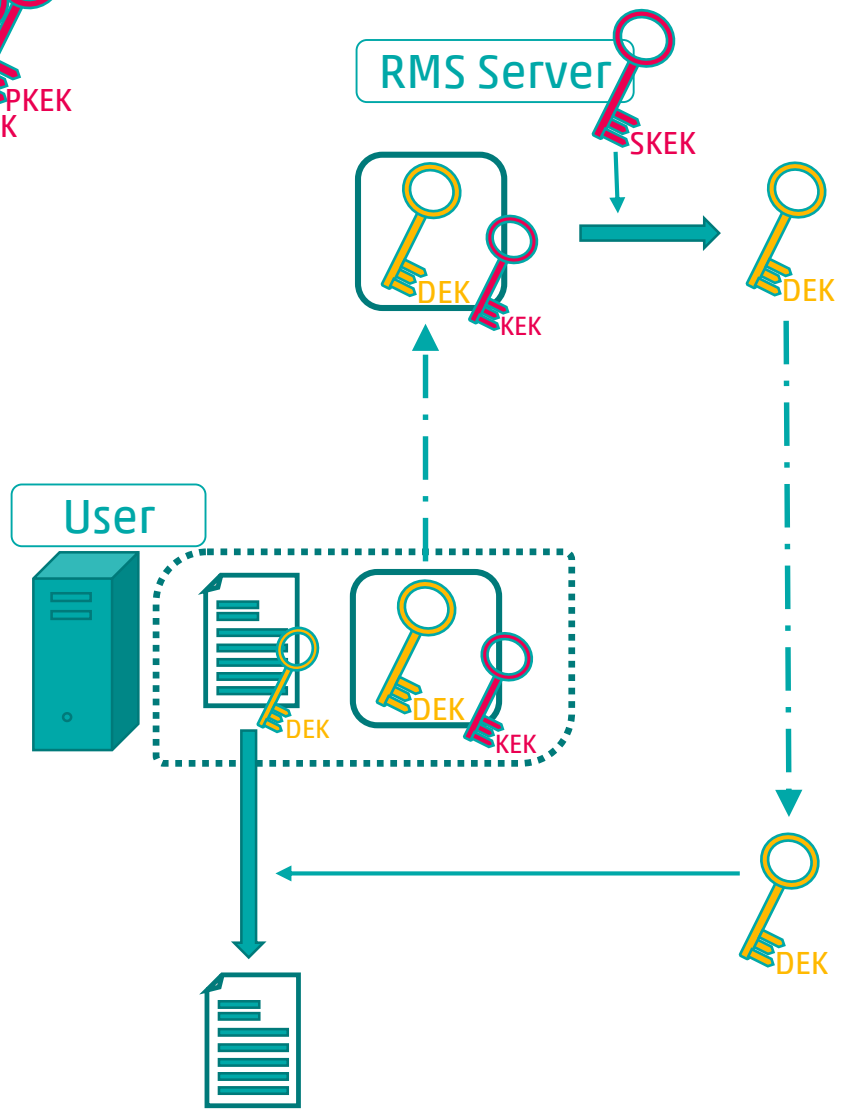


Zugriffskontrolle mit RMS

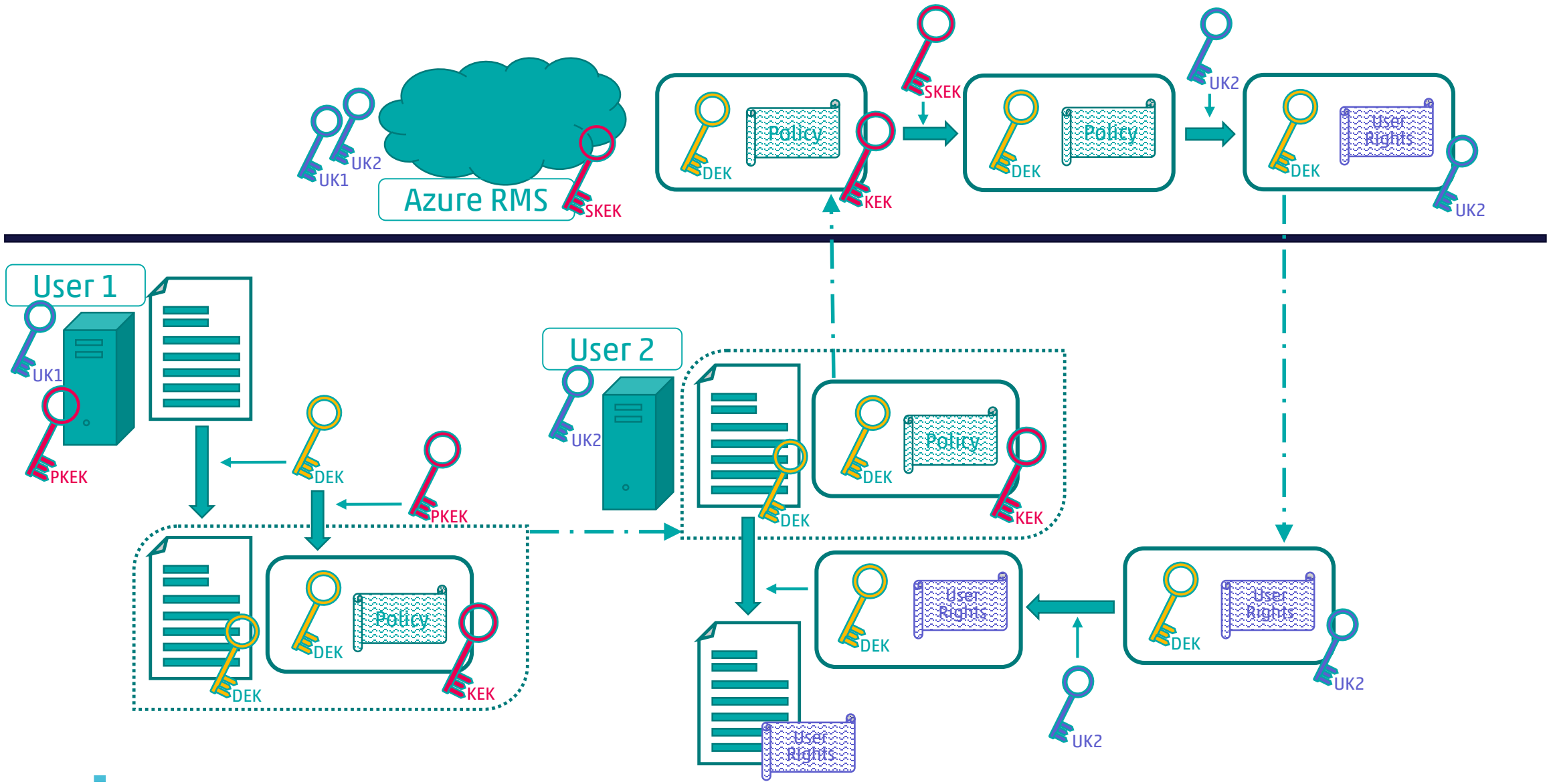








Azure RMS mit Cloud Key



Betriebliche Aspekte von Azure RMS

- Die Anwendung mit der ein geschütztes Dokument geöffnet werden soll muss RMS unterstützen.
- Alle Teilnehmer müssen sich bei Azure authentisieren können.
  - Insbesondere auch ein Empfänger, der eine geschützte Email öffnen will
  - Federation mit verschiedenen Identity Providern möglich
- Schlüsselmodelle sind miteinander kombinierbar.
  - z.B. HYOK für sensitive Daten & Cloud Key für den Rest
- Für HYOK ist ein lokaler RMS Server nötig.
- RMS Verschlüsselung und Verschlüsselung in anderen Azure-Services sind voneinander unabhängig.
  - Müssen separat konfiguriert werden
  - Können verschiedene Schlüsselmodelle verwenden
- Policy Enforcement schützt vor allem gegen Fehler.

Vielen Dank für Ihre Aufmerksamkeit_

Zuzana Trubini
Zuzana.Trubini@cnlab.ch
+41 55 214 33 34

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland