



# Herbsttagung 2019 (Geheime) Daten in der Cloud

Zuzana Trubini  
Zürich, 11.09.2019



# Agenda\_

**Daten in der Cloud** (Datensicherheit in der Cloud)

**Geheime Daten in der Cloud** (Verschlüsselung und Vertraulichkeit)

**Information Right Management (IRM)**

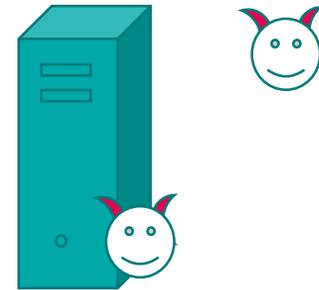
**Azure Right Management Service (Azure RMS)**

# Sicherheit der Daten in der Cloud

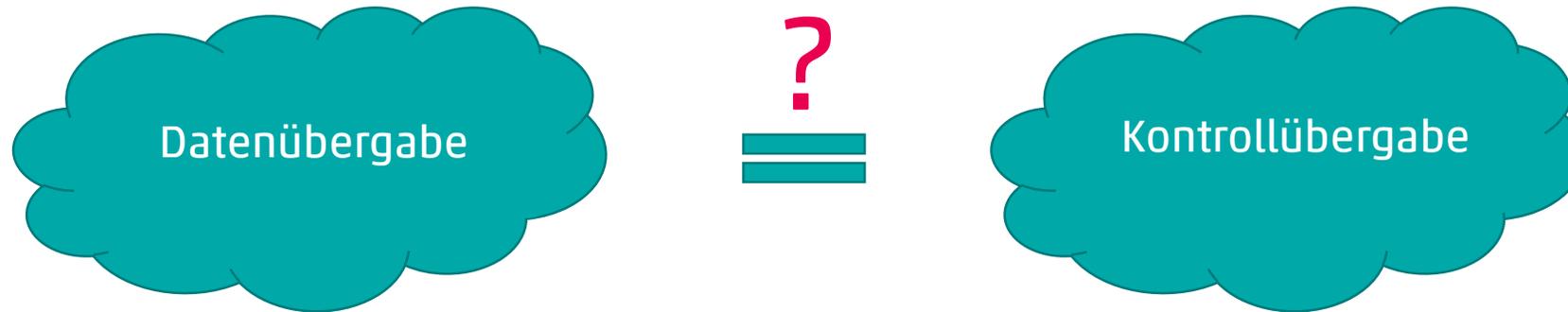
Vorstellung



Realität



# Datenhoheit



# Abhängigkeit vom Cloud-Anbieter

- Wie gross ist die Abhängigkeit?
- Kann man sie reduzieren?
- Wie?

## Abhängigkeit bezüglich Datensicherheit

- Verfügbarkeit - Backup, Notfall-Konzept
- Vertraulichkeit - Verschlüsselung **ruhender Daten**
- Integrität - Hashes, Signaturen
  
- Nachvollziehbarkeit - Logging & Auditing, Archivierung

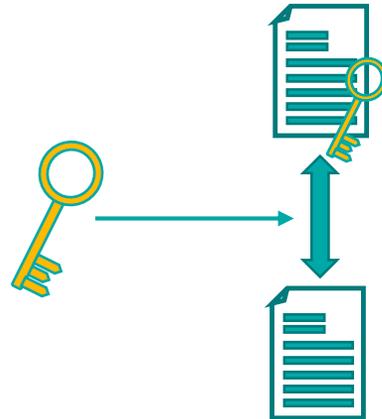
Backup, Verschlüsselung, Logging: wird auch von den Cloud-Anbietern angeboten, löst aber das Abhängigkeitsproblem nicht.

# Verschlüsselung und Vertraulichkeit

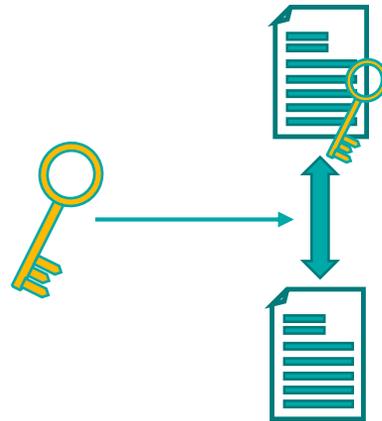
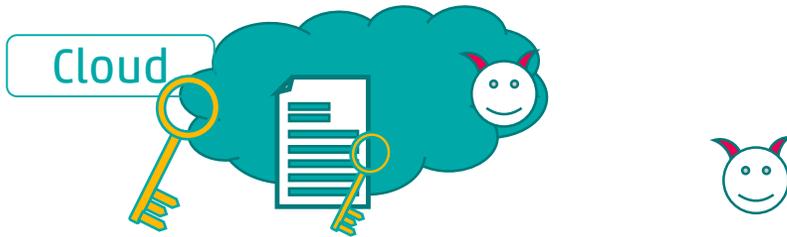


## HYOK (Hold Your Own Key)

- + Volle Schlüssel-Kontrolle
- + Datenhoheit möglich
- Volle Verantwortung
- Reduzierte Cloud-Funktionalität



# Verschlüsselung und Vertraulichkeit



## BYOK (Bring Your Own Key)

- Teilweise Schlüssel-Kontrolle
- Keine Datenhoheit
- Volle Verantwortung
- + Volle Cloud-Funktionalität

## Cloud Key (Service-Managed Key)

- Keine Schlüssel-Kontrolle
- Keine Datenhoheit
- + Keine Verantwortung
- + Volle Cloud-Funktionalität

# Schlüsselmodelle und Vertraulichkeit

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

Als Gegensatz zum  
Schutz eines  
Mediums oder eines  
Kanals

auch  
ausserhalb  
der Firma

Wer? Was?  
Wann? Wo? Wie?

## Azure RMS (als Teil von AIP)

# Azure Information Protection

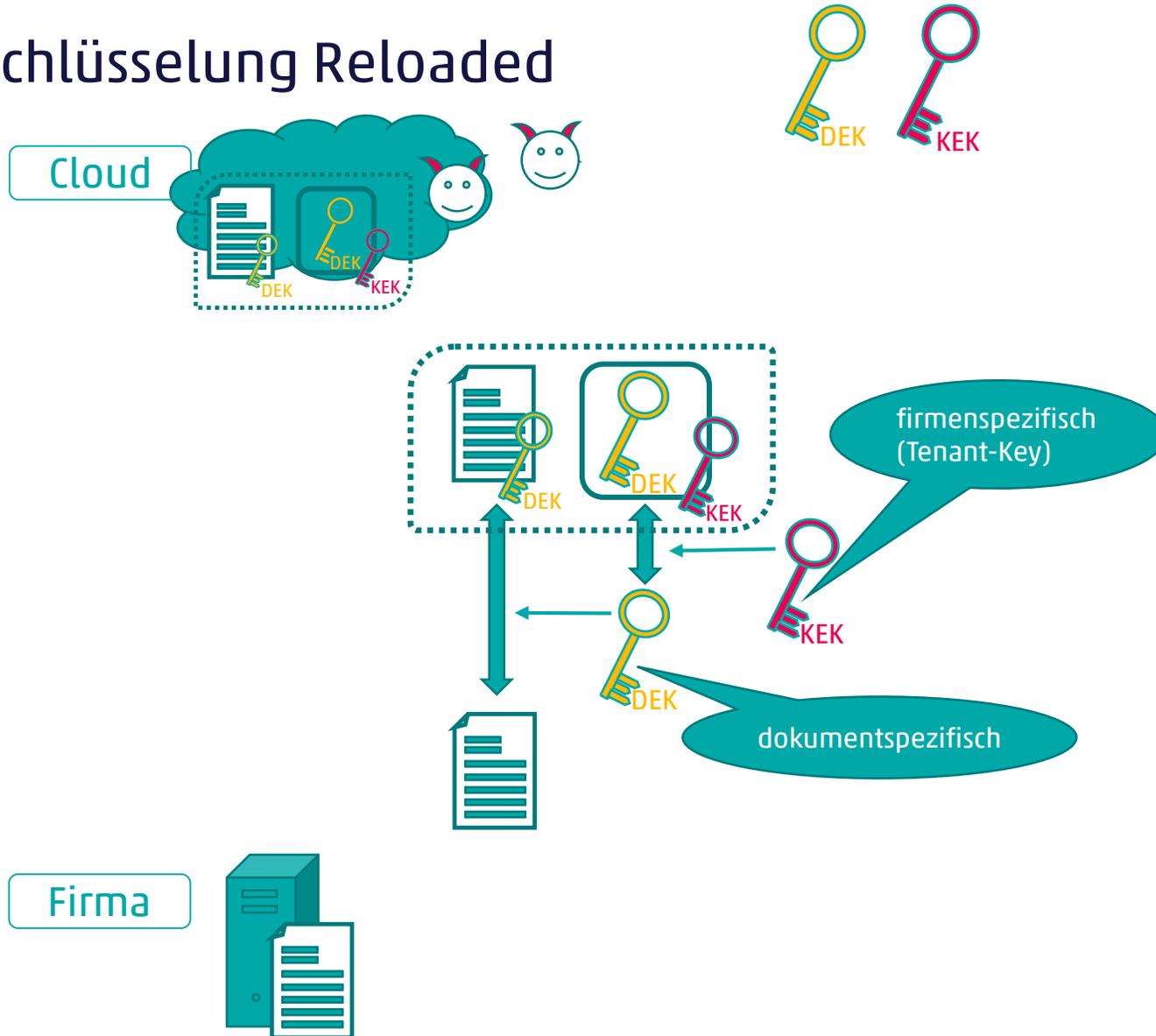


Classification  
& labelling

Protect

Monitor  
& respond

# Verschlüsselung Reloaded

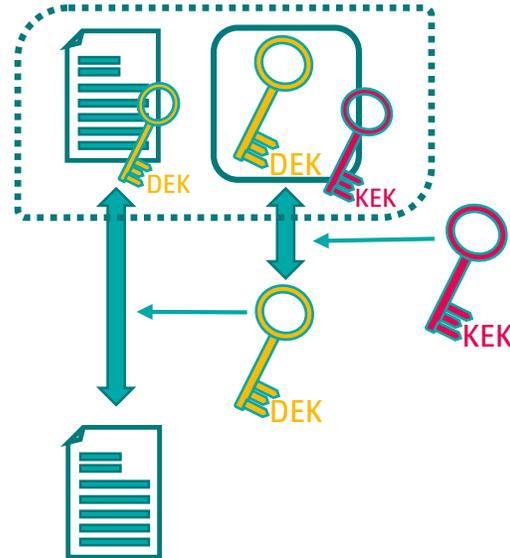


# Verschlüsselung Reloaded

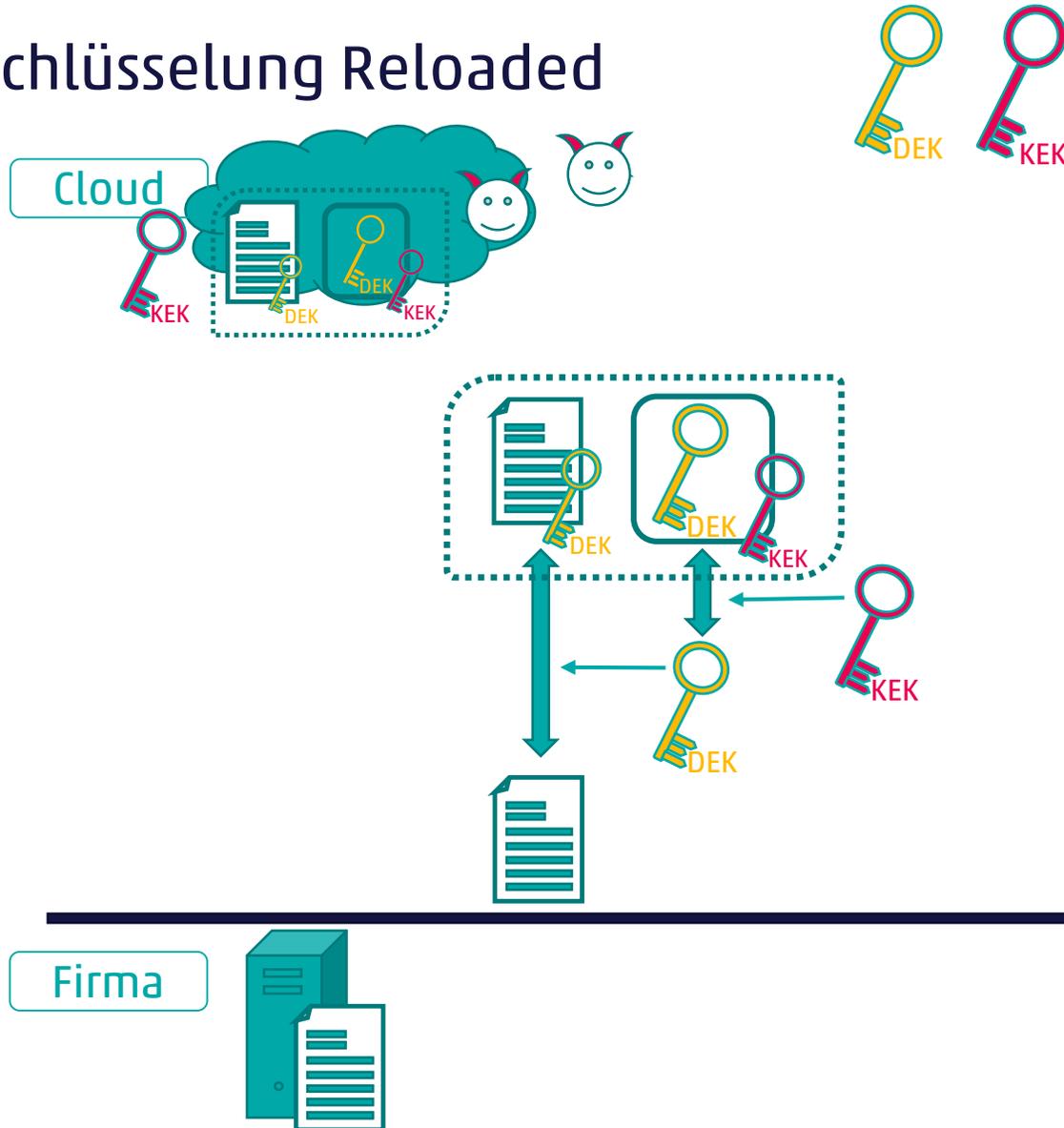


## HYOK(Hold Your Own Key)

- + Volle Kontrolle
- + Datenhoheit möglich
- Volle Verantwortung
- Reduzierte Cloud-Funktionalität



# Verschlüsselung Reloaded



## BYOK (Bring Your Own Key)

- Teilweise Kontrolle
- Keine Datenhoheit
- Volle Verantwortung
- + Volle Cloud-Funktionalität

## Cloud Key (Service-Managed Key)

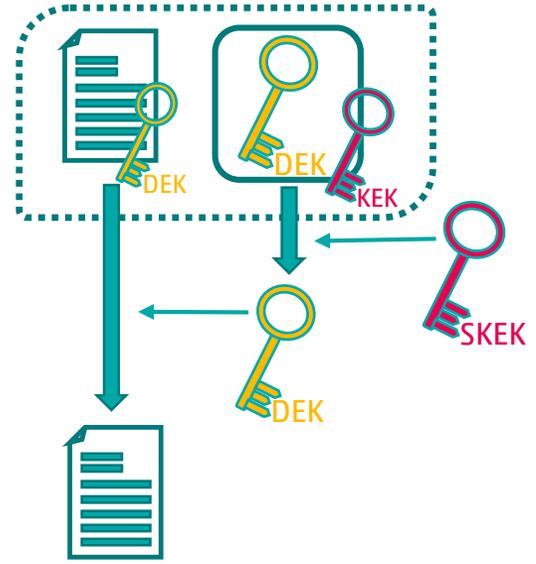
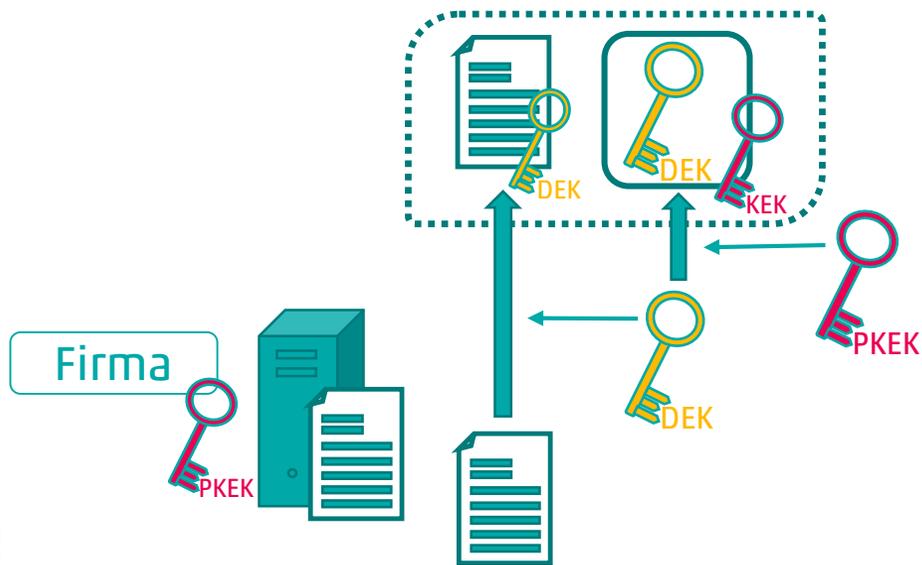
- Keine Kontrolle
- Keine Datenhoheit
- + Keine Verantwortung
- + Volle Cloud-Funktionalität

# Verschlüsselung bei Azure

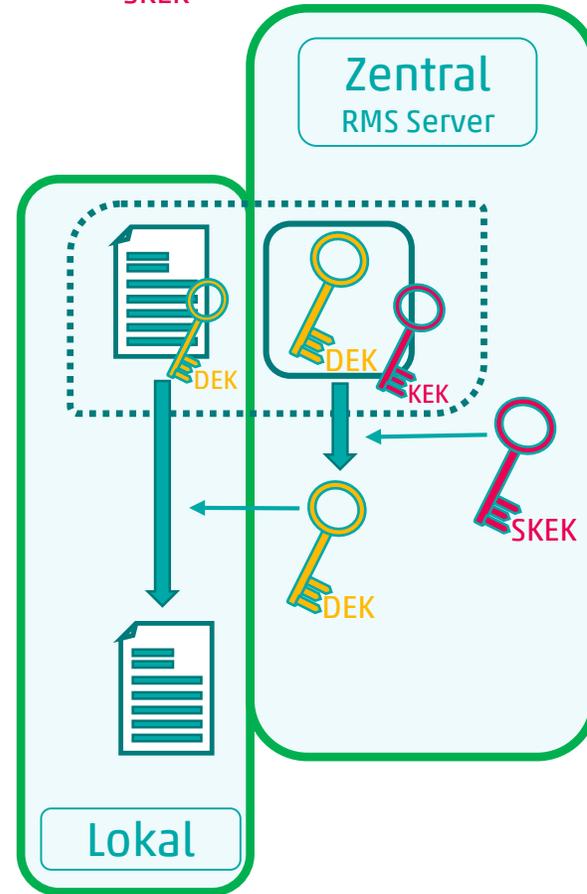
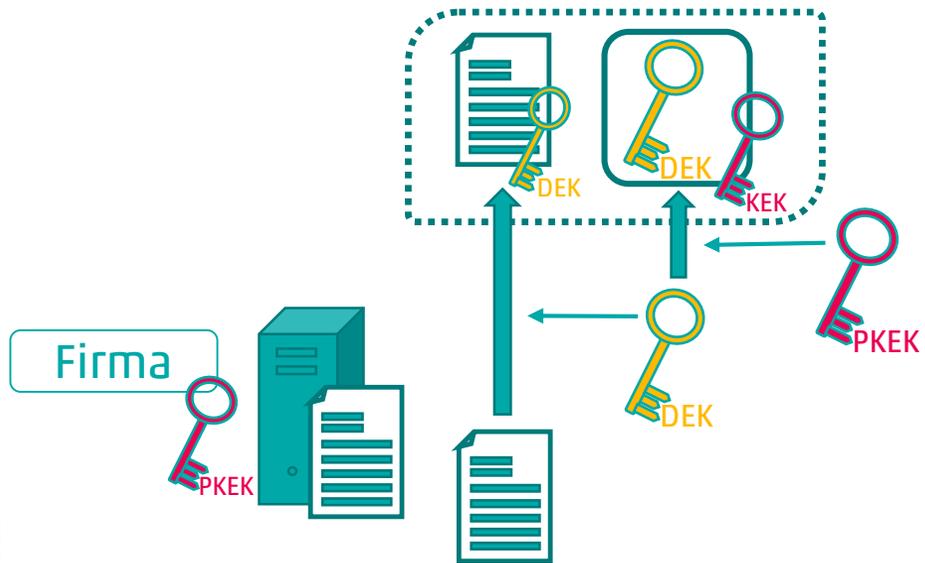
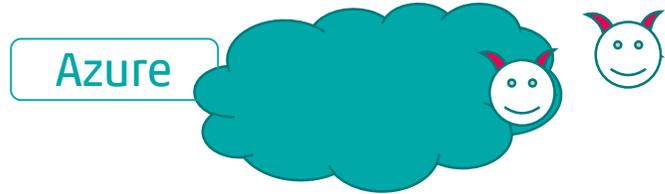


Publik Key = öffentlicher Verschlüsselungskey

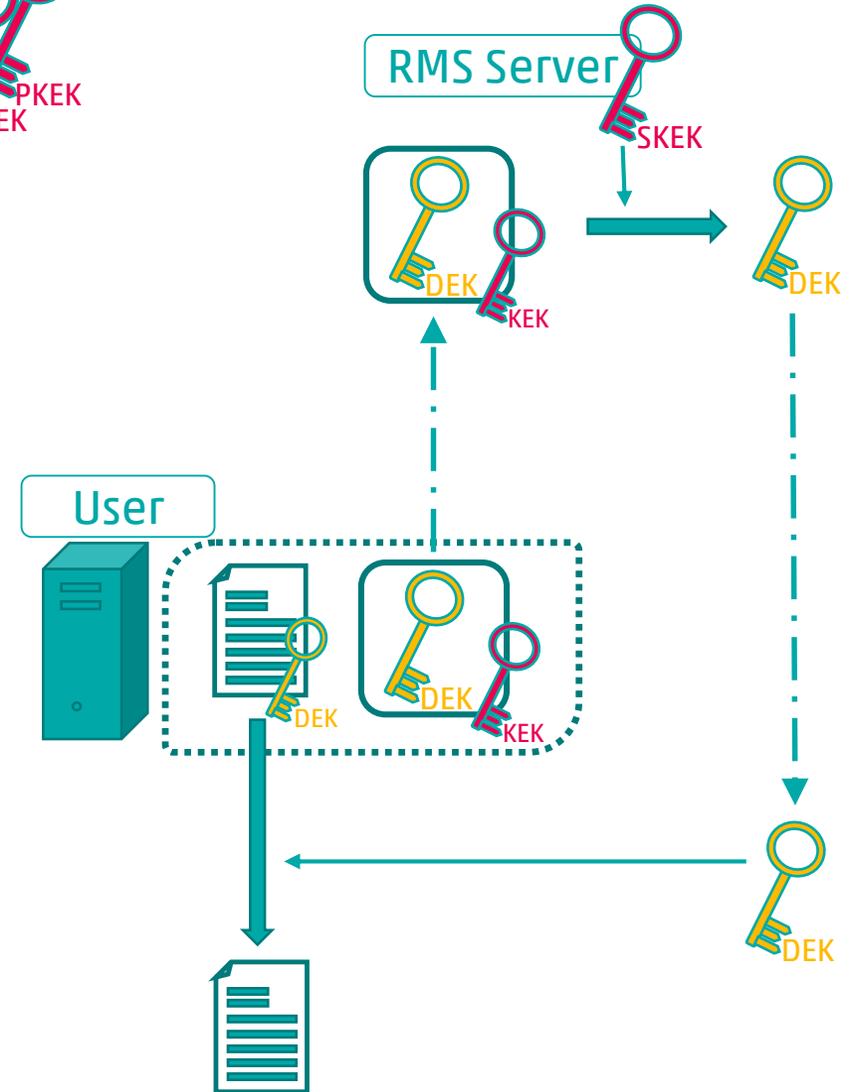
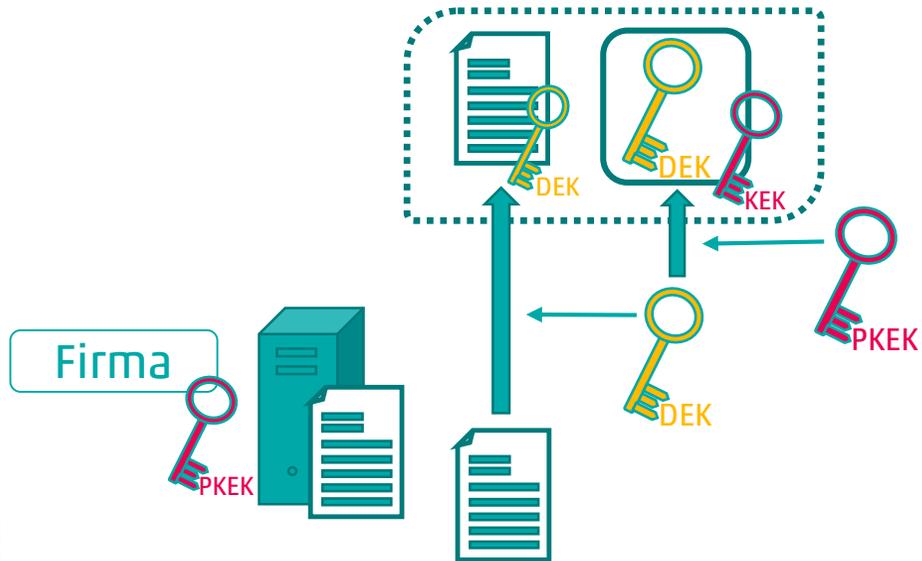
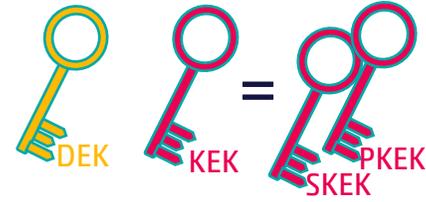
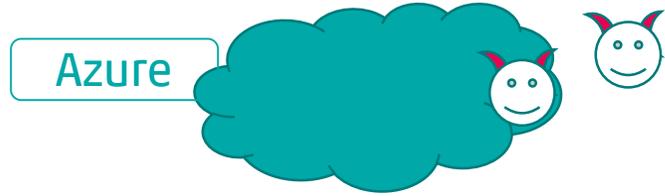
Secret Key = geheimer Entschlüsselungskey



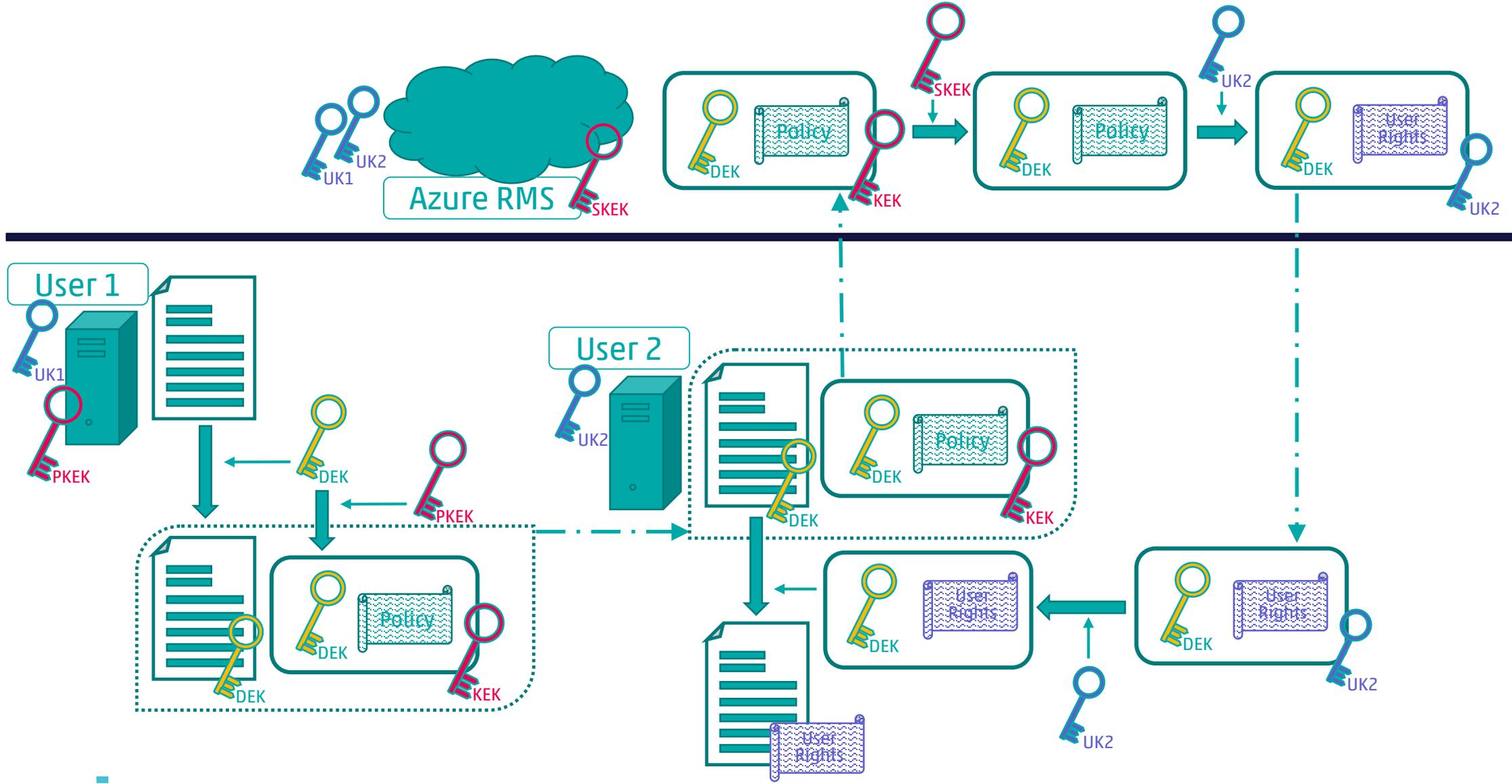
# Zugriffskontrolle mit RMS



# 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