
„Mit dem Wissen
wächst der Zweifel.“
Johann Wolfgang von Goethe
1749 – 1832, deutscher Dichter und Naturforscher

# „Wissen ist Macht.“

**Francis Bacon**
1561 – 1626, englischer Philosoph und Staatsmann

THALES

# Datenverarbeitung in der Cloud?

*Natürlich! Aber bitte verschlüsselt…*

Kai Wolff
Senior Channel Account Manager, Data Protection

# Ausgangslage

## EU: DSGVO (*2018), Schrems II (*2020)

Schutz personenbezogener Daten
verlangt TOMs
**Datenexporteur**



begrenzte technische Möglichkeiten
potenziell Daten ausliefern

## US: CLOUD Act (*2018)

THALES

# Privacy Shield 2.0

## Privacy Shield 2.0: USA geloben "beispiellose" Überwachungsreform

Die EU-Kommission und die US-Regierung haben erste Details zum geplanten neuen "Transatlantischen Datenschutzrahmen" bekannt gegeben.

Lesezeit: 5 Min. In Pocket speichern 53

US-Präsident Joe Biden und Kommissionspräsidentin Ursula von der Leyen nach ihrem Treffen am Freitag in Brüssel. (Bild: EU-Kommission/Christophe Licoppe)

26.03.2022 17:08 Uhr

## Schrems: Nur Zusicherungen, nicht einklagbar

Zugleich bestätigten die Kommission und die US-Regierung, dass die Zusagen Washingtons nur in eine Durchführungsverordnung ("Executive Order") aufgenommen werden sollen. Die von Schrems gegründete Datenschutzorganisation Noyb hatte zuvor kritisiert, dass die USA "keine Änderungen ihrer Überwachungsgesetze, sondern lediglich Zusicherungen der Exekutive" planten. Diese hätten "keine externe Wirkung und können nicht eingeklagt werden". Eine echte Lösung wie ein "No-Spy-Abkommen" mit "Basisgarantien unter gleichgesinnten Demokratien" stehe weiter aus.

THALES

**Mal abwarten …**

"Firewall"
"Application Firewalls"
"Next-gen Firewalls"

**Verschlüsseln, um compliant zu sein**

Native Verschlüsselung

**Verschlüsseln, um sicher zu sein**

Bring Your Own Encryption



THALES

# Wir müssen schützen, was uns ausmacht


THALES

# Was hilft uns dabei?

**DSGVO, Art. 32, 1.a)**
*„die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten“*

EU-Datenschutz-Grundverordnung (EU-DSGVO)

Infos, Schulungen und Kommentar über und zur EU-Datenschutz Grundverordnung

Inhalte DSGVO | Erwägungsgründe | BDSG (neu) | Dokumente: Links/Downloads | Schulung

## Art.32 – EU-DSGVO – Sicherheit der Verarbeitung

Finaler Text | Synopse

<<ZURÜCK Übersicht VOR >>

**Stand: 27.04.2016**

(ehem. Art. 30)

***Sicherheit der Verarbeitung***

1. Unter Berücksichtigung **des Stands der Technik**, der **Implementierungskosten** und der **Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung** sowie der **unterschiedlichen Eintrittswahrscheinlichkeit** und **Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen** treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;

b) die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste** im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

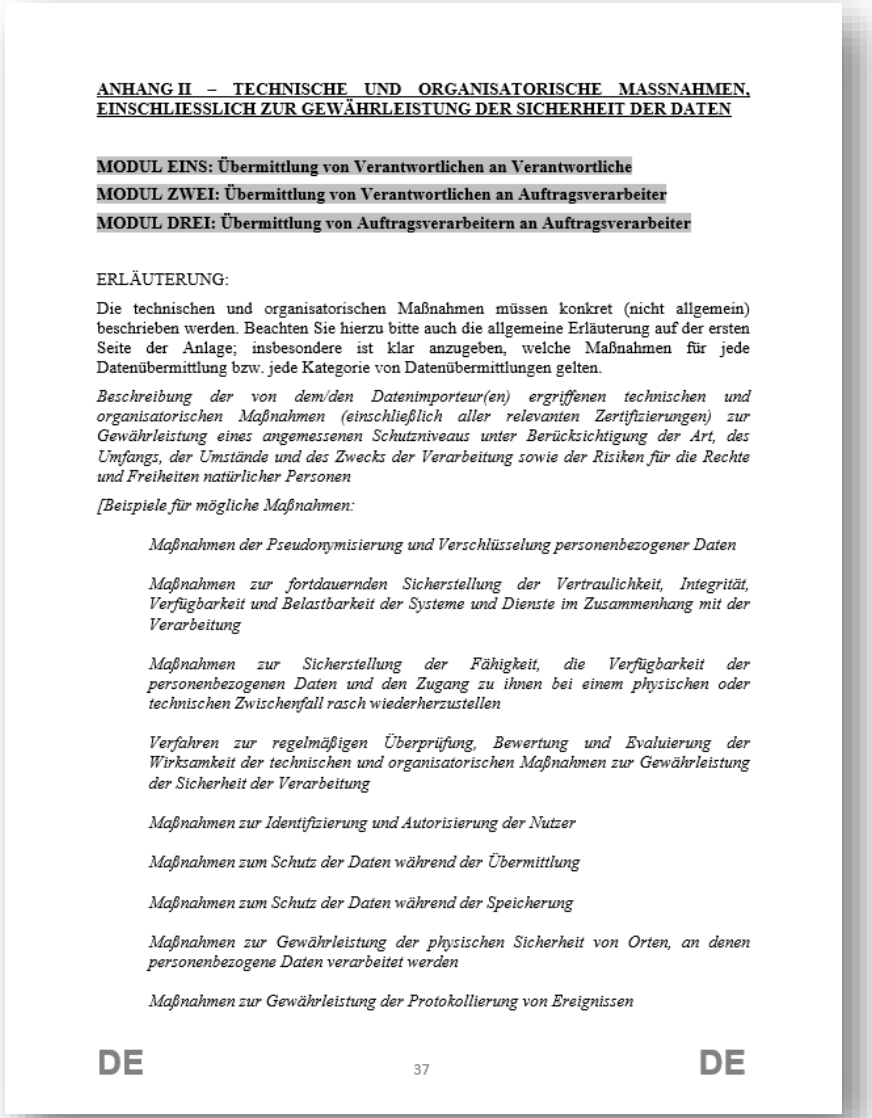
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall **rasch wiederherzustellen**;

Art.32 - EU-DSGVO - Sicherheit der Verarbeitung - EU-Datenschutz-Grundverordnung (EU-DSGVO)
edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (europa.eu)

# Was hilft uns dabei?

DSGVO, Art. 32, 1.a)
*„die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten“*

**Neue Standardvertragsklauseln (SCCs)**
*„Beschreibung … technischen und organisatorischen Maßnahmen … zur Gewährleistung des im Wesentlichen gleichwertigen Schutzniveau..“ (wie im EWR)*



**ANHANG II – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN**

**MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche**
**MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter**
**MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter**

ERLÄUTERUNG:

Die technischen und organisatorischen Maßnahmen müssen konkret (nicht allgemein) beschrieben werden. Beachten Sie hierzu bitte auch die allgemeine Erläuterung auf der ersten Seite der Anlage; insbesondere ist klar anzugeben, welche Maßnahmen für jede Datenübermittlung bzw. jede Kategorie von Datenübermittlungen gelten.

*Beschreibung der von dem/den Datenimporteur(en) ergriffenen technischen und organisatorischen Maßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen*

*[Beispiele für mögliche Maßnahmen:*

*Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten*

*Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung*

*Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen*

*Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung*

*Maßnahmen zur Identifizierung und Autorisierung der Nutzer*

*Maßnahmen zum Schutz der Daten während der Übermittlung*

*Maßnahmen zum Schutz der Daten während der Speicherung*

*Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden*

*Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen*

DE 37 DE

Art.32 - EU-DSGVO - Sicherheit der Verarbeitung - EU-Datenschutz-Grundverordnung (EU-DSGVO)
edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (europa.eu)

# Was hilft uns dabei?

**DSGVO, Art. 32, 1.a)**
*„die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten“*

**Neue Standardvertragsklauseln (SCCs)**
*„Beschreibung … technischen und organisatorischen Maßnahmen … zur Gewährleistung des im Wesentlichen gleichwertigen Schutzniveau..“ (wie im EWR)*

**Empfehlungen des EDPB**
*Seite 35, Artikel 95:*
“Zero knowledge Prinzip durch Segregation of Duties (Funktionstrennung)“


*Beispiele für Szenarien, die sich auf Fälle beziehen, in denen keine wirksamen Maßnahmen identifiziert wurden*

*Use Case 6*

Artikel 95.

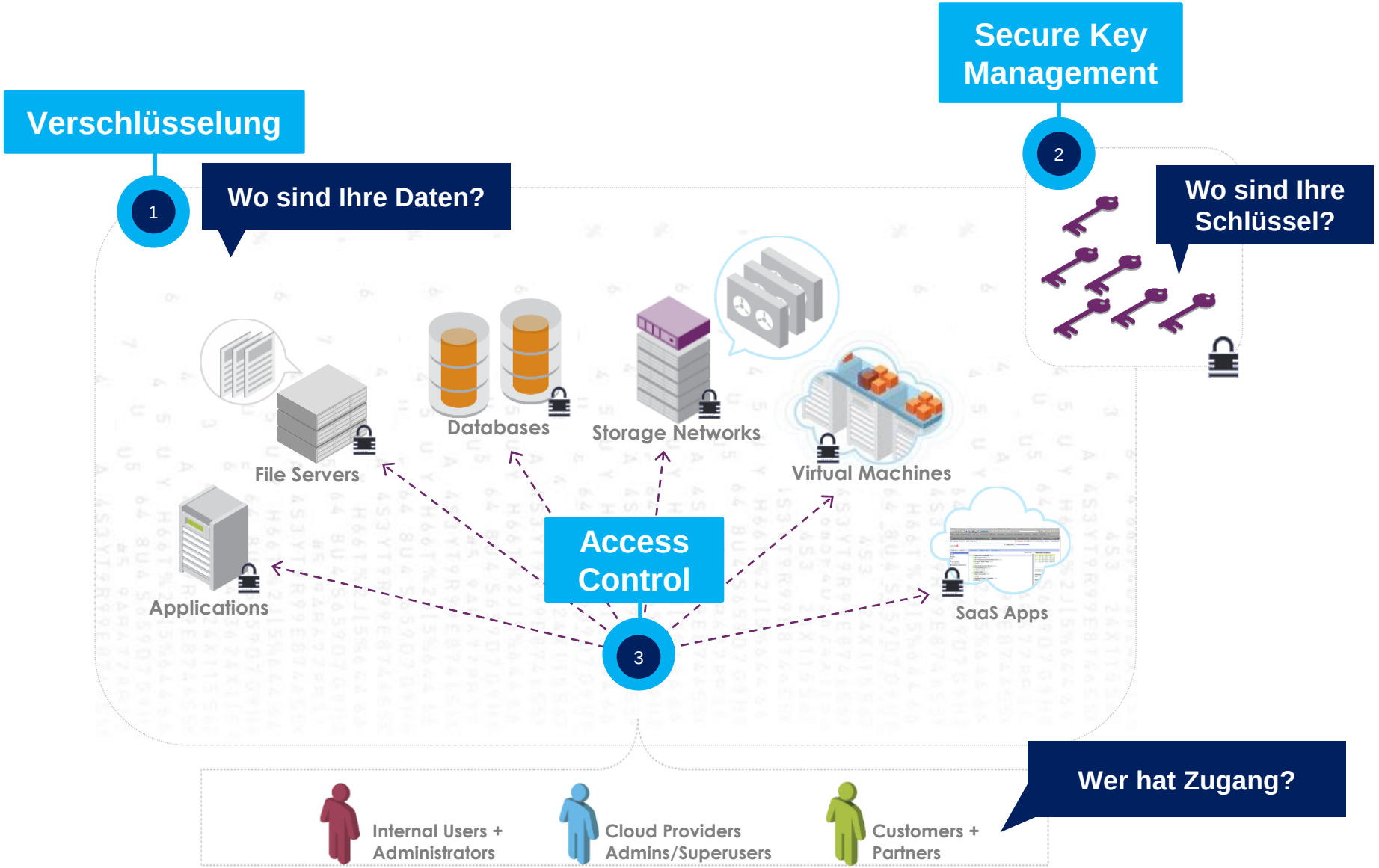
*…“die Transportverschlüsselung und die Data-at-Rest-Verschlüsselung auch in Kombination“ (stellt) „**keine zusätzliche Maßnahme** dar, die ein im Wesentlichen gleichwertiges Schutzniveau gewährleistet, wenn der **Datenimporteur im Besitz der kryptografischen Schlüssel ist.“***

Art.32 - EU-DSGVO - Sicherheit der Verarbeitung - EU-Datenschutz-Grundverordnung (EU-DSGVO)
edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (europa.eu)



THALES

# Exkurs: Segregation of Duties



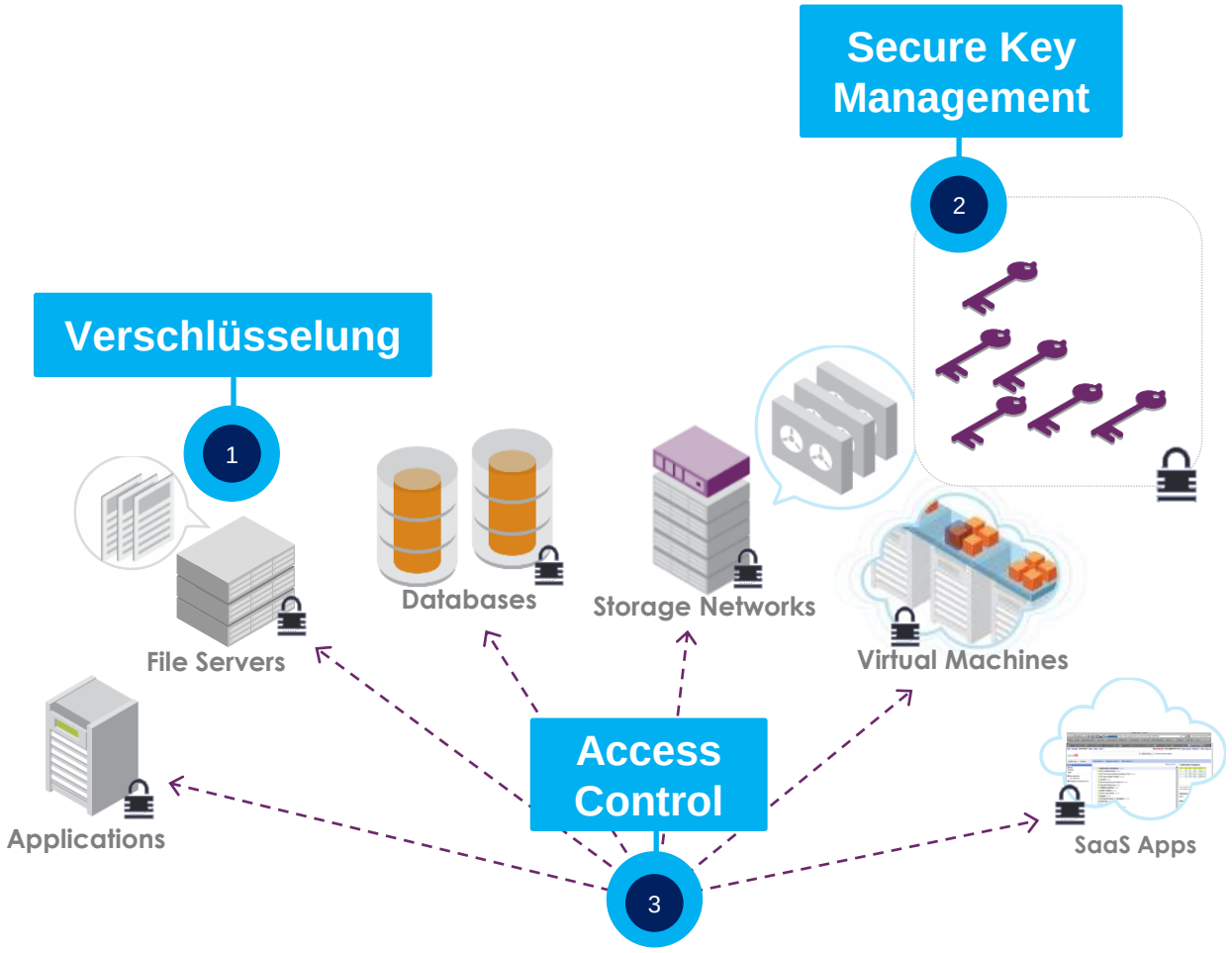



THALES

# Zusammenfassung

Sauber implementierte Verschlüsselung
Schlüssel extern halten

Zugang unter eigener Kontrolle halten






THALES

# Was ist mit der Verschlüsselung der Hyperscaler?

CMEK, CKMS, Cloud HSM, CSEK,…

aws KMS, SSE-C, Encry. SDK, keyring, …

KEK, SSE, TDE, CLE, MEK, DEC, …


*Beispiele für Szenarien, die sich auf Fälle beziehen, in denen keine wirksamen Maßnahmen identifiziert wurden*

*use case 6*

Artikel 95.

*…"die Transportverschlüsselung und die Data-at-Rest-Verschlüsselung auch in Kombination" (stellt) „**keine zusätzliche Maßnahme** dar, die ein im Wesentlichen gleichwertiges Schutzniveau gewährleistet, wenn der **Datenimporteur im Besitz der kryptografischen Schlüssel ist.**"*

**Für personenbezogene Daten nicht geeignet !**



THALES

# Was ist mit der Verschlüsselung der Hyperscaler?

## Wenn keine DSGVO relevanten Daten im Spiel – durchaus empfehlenswert

CMEK, CKMS, Cloud HSM, CSE

**Warnung:** Wenn Sie vom Kunden bereitgestellte Verschlüsselungsschlüssel verwenden oder Ihre Daten auf der Clientseite verschlüsseln, ist es wichtig, dass Sie Ihre Schlüssel sicher verwalten und vor Verlust schützen. Ohne die Schlüssel können Sie Ihre Daten nicht mehr lesen. Für die Speicherung Ihrer Objekte fallen aber weiter Gebühren an, bis sie gelöscht werden.

aws

**Wichtig**

Amazon S3 speichert den von Ihnen bereitgestellten Verschlüsselungsschlüssel nicht. Stattdessen wird ein zufällig mit einem Salt versehenen HMAC-Wert des Verschlüsselungsschlüssels gespeichert, um zukünftige Anfragen zu überprüfen. Der mit einem Salt versehene HMAC-Wert kann nicht verwendet werden, um den Wert des Verschlüsselungsschlüssels abzuleiten oder den Inhalt des verschlüsselten Objekts zu entschlüsseln. Das bedeutet, wenn Sie den Verschlüsselungsschlüssel verlieren, verlieren Sie das Objekt.

KEK, SSE, TDE, CLE, MEK, DEC, …

**Dienstverschlüsselung mit Kundenschlüssel**
Der Kunde trägt das gesamte Risiko einer Löschung von oder der Unmöglichkeit des Zugriffs auf Daten sowie von Dienstausfällen, die aus einer vom Kunden verursachten Nichtverfügbarkeit eines Verschlüsselungsschlüssels hervorgehen.

## Cloud Key Management ist sehr wichtig – Thales hilft dabei!



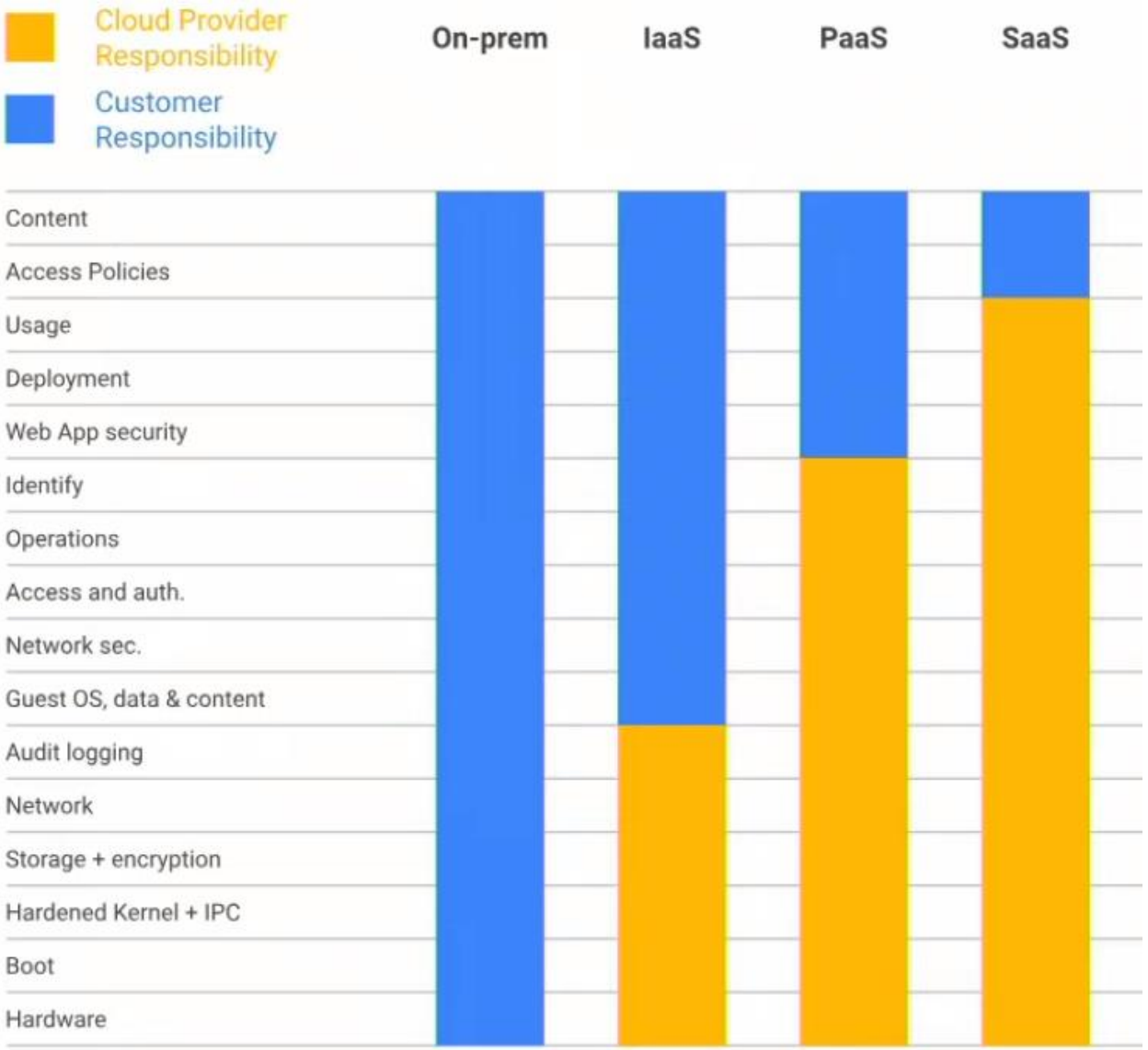
THALES

THALES

# Welche Möglichkeiten bestehen nun konkret bei den Hyperscalern …

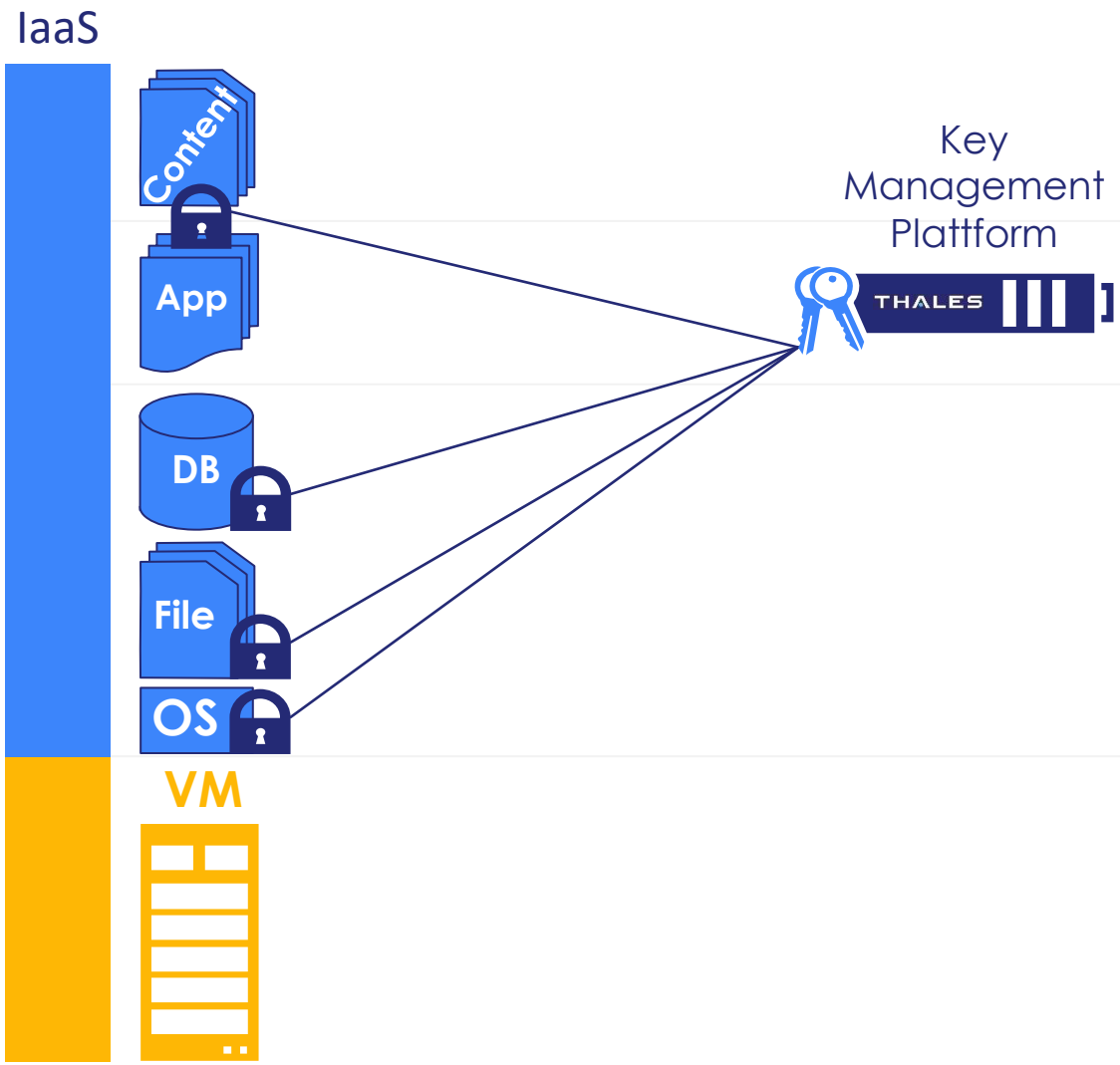
## … um Compliance herzustellen?

# Zur Orientierung: Cloud Provider Shared Responsibility Model




 https://cloudsecurityalliance.org/

# Datensouveränität bei den Hyperscalern: IaaS




Verschlüsselung in der Applikation

Datenbank-Verschlüsselung

File/Folder-Verschlüsselung

Festplattenverschlüsselung



Cloud Provider Responsibility  Customer Responsibility

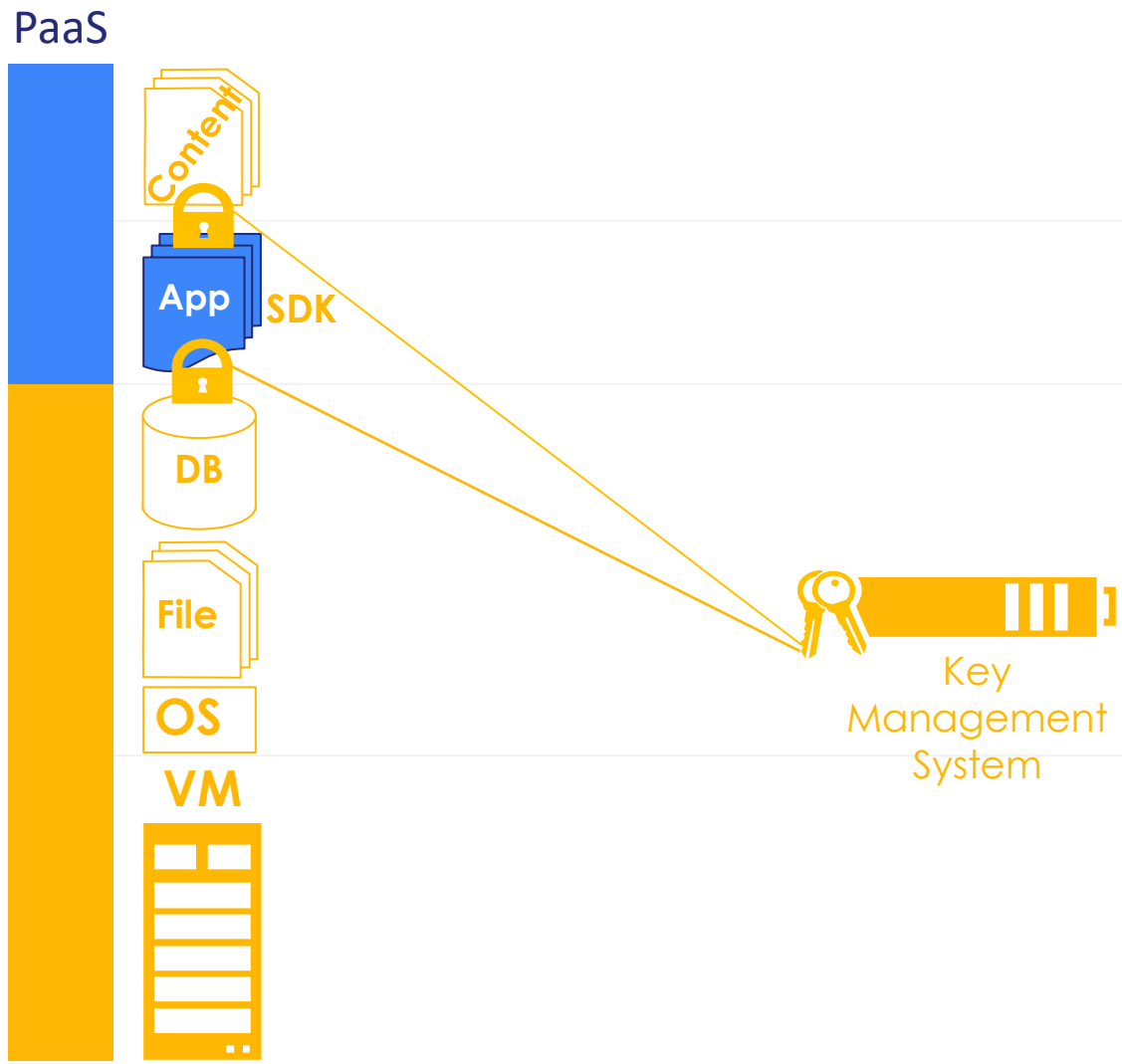
# Datensouveränität bei den Hyperscalern: PaaS (1/4)




Cloud Provider Responsibility  Customer Responsibility

THALES

# Datensouveränität bei den Hyperscalern: PaaS (2/4)



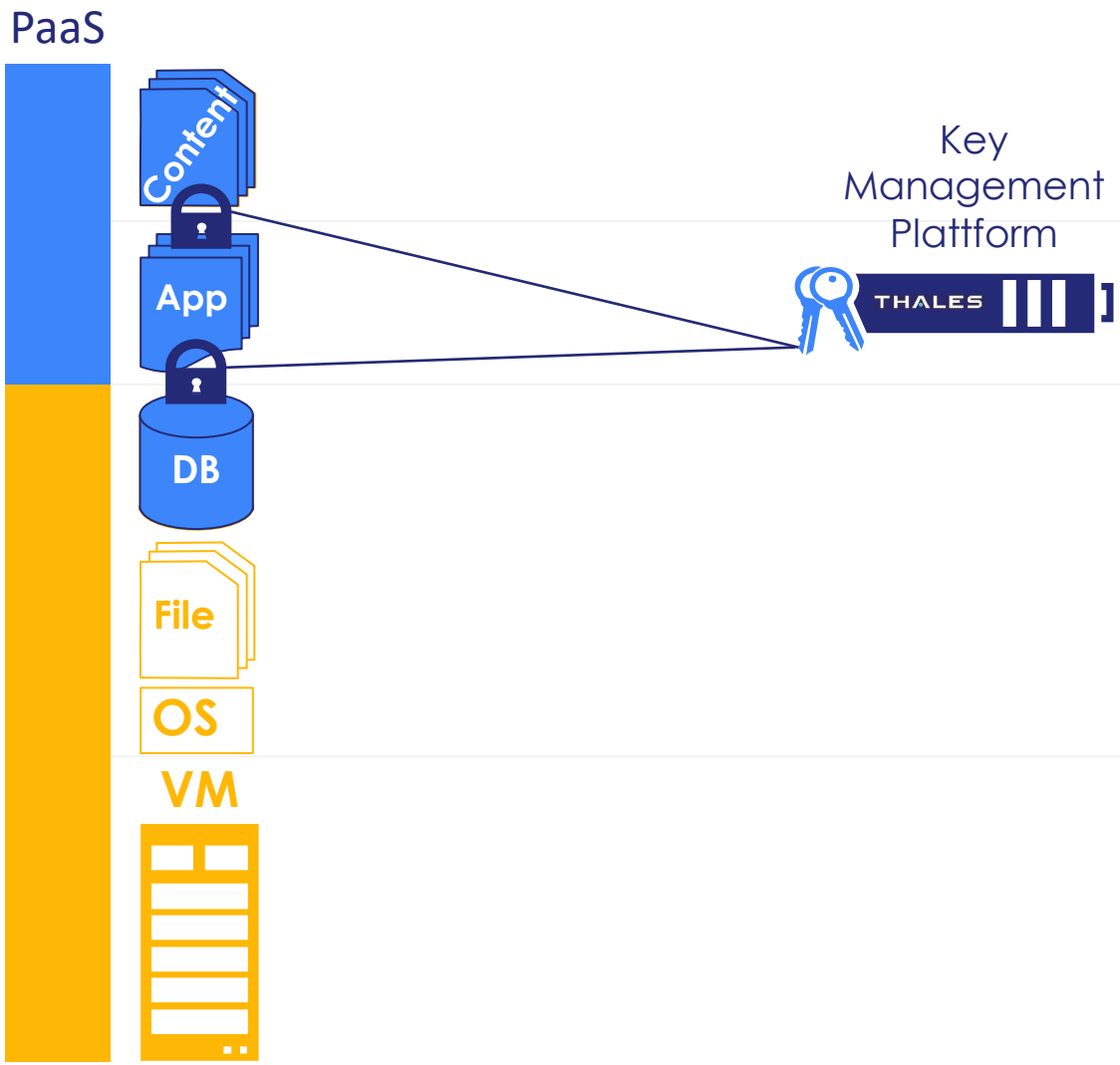

Verschlüsselung und Key Management des Hyperscalers



Cloud Provider Responsibility  Customer Responsibility

THALES

# Datensouveränität bei den Hyperscalern: PaaS (3/4)



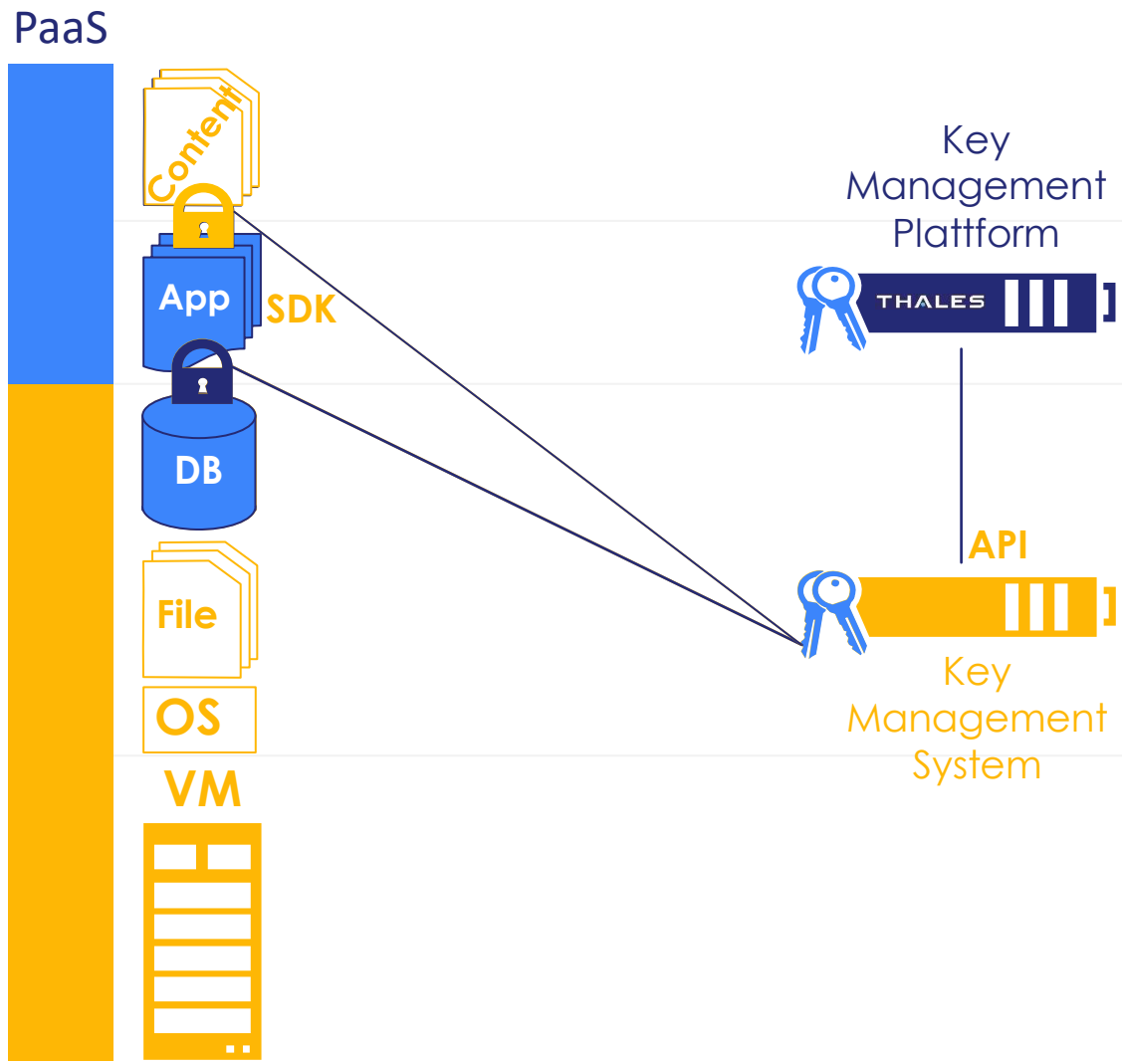

Verschlüsselung in der Applikation



Cloud Provider Responsibility  Customer Responsibility

THALES

# Datensouveränität bei den Hyperscalern: PaaS (4/4)




Schnittstelle zum Key Management des Hyperscalers

**APIs:**
**Google EKM** - External Key Manager

**xKS** - External Key Storage (Q2/22)

**Microsoft** – keine generelle Schnittstelle


Cloud Provider Responsibility
Customer Responsibility
THALES

# Datensouveränität bei den Hyperscalern: SaaS


Google Workspace

Amazon Rekognition

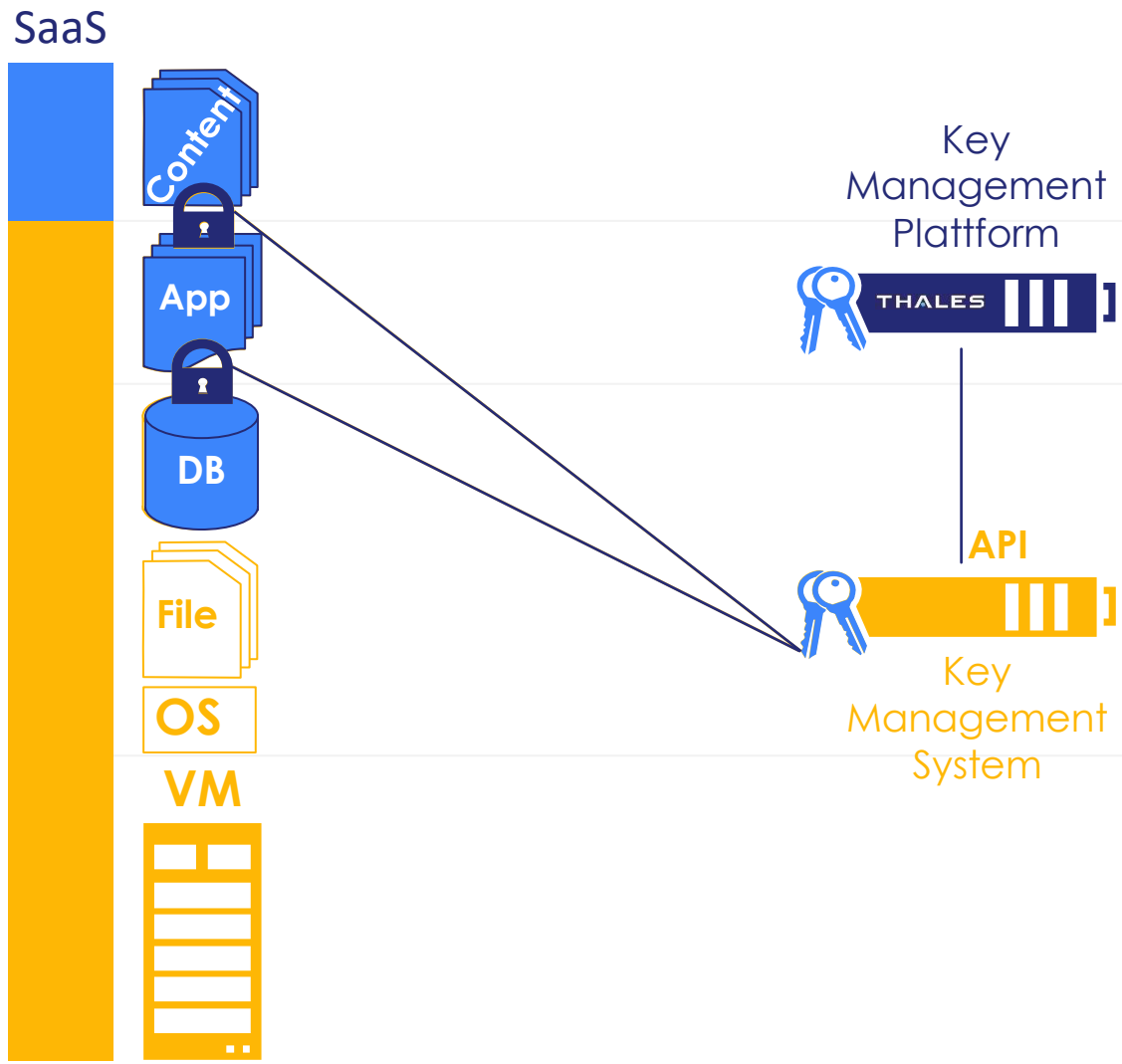
Microsoft 365



Cloud Provider Responsibility  Customer Responsibility

THALES

# Datensouveränität bei den Hyperscalern: SaaS (1/2)




Schnittstelle zum Key Management des Hyperscalers

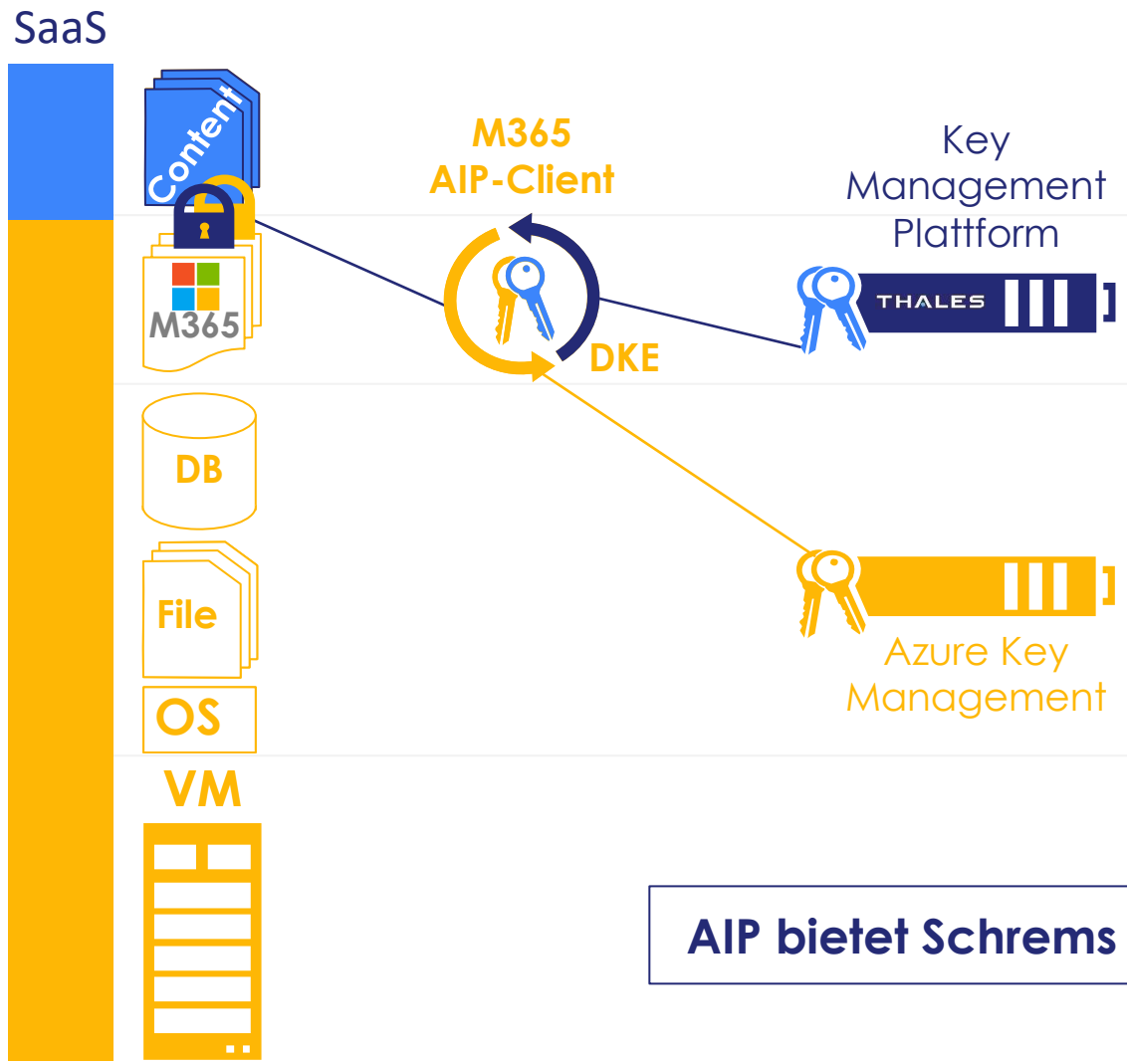
**APIs:**
**Google EKM** - External Key Manager

**xKS** - External Key Storage (Q2/22)

**Microsoft** – keine generelle Schnittstelle


Cloud Provider Responsibility
Customer Responsibility

# Datensouveränität bei den Hyperscalern: SaaS (1/2)




**AIP** - Azure Information Protection

**API:**
**DKE** – Double Key Encryption for M365

**AIP bietet Schrems II-Konformität für viele Dokument-Typen**

File types supported by the Azure Information Protection (AIP) unified labeling client | Microsoft Docs

Cloud Provider Responsibility  Customer Responsibility

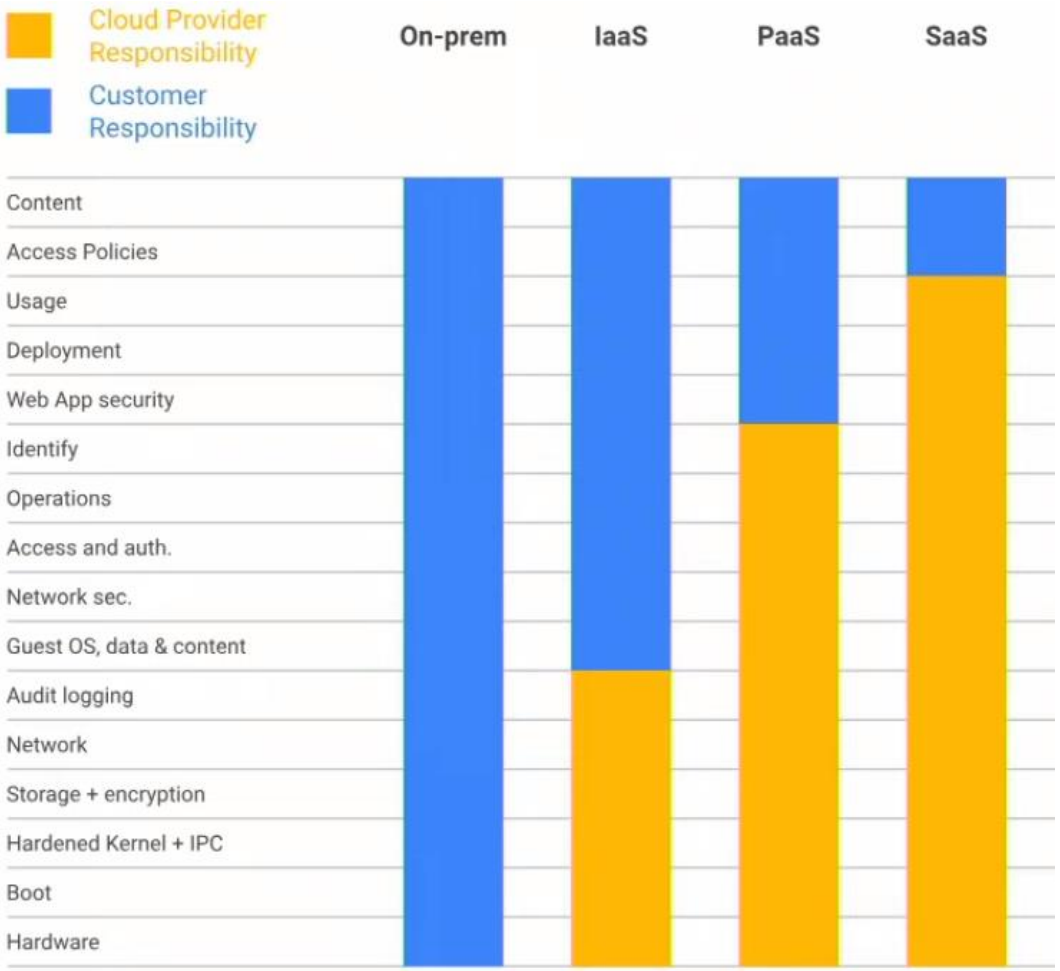


THALES

# Fazit

Mehr Verantwortung beim Provider, bedeutet weniger Optionen.

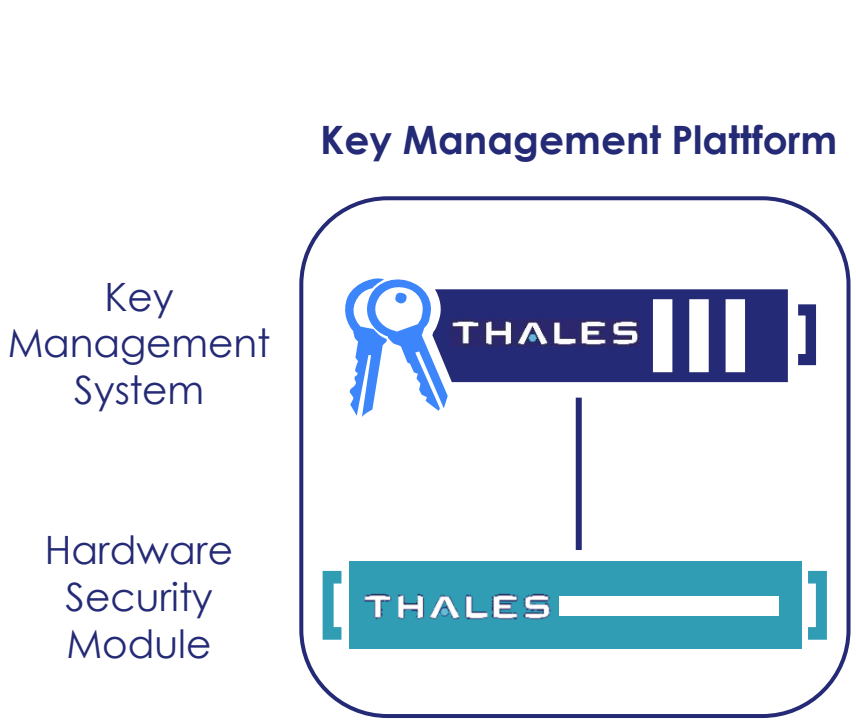
**Aber:**
TOMs auf vielen Ebenen möglich.






THALES

# Key Management Plattform - Komponenten




**Daten überall finden und klassifizieren**

**Daten überall schützen durch Verschlüsselung**

**Den Betrieb sicherstellen, zentralisieren, automatisieren, Kontrolle ausüben**



THALES