THALES
Building a future we can all trust

NIS2 – in der Praxis

Emanuel Prillwitz - August 2023

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

(2) Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
b) Bewältigung von Sicherheitsvorfällen;
c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;
f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555&qid=1677159789728&from=EN#d1e3335-80-1

THALES

Forschungsfrage(n)?

- **Warum schreibt die EU sowas rein? Warum Kryptographie?!**
- **Was bedeutet diese Krypto-Maßnahme für die Praxis?**

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

- **Reicht also HTTPS/TLS und wir machen einen Haken drunter?!**
- **Wie werden denn Krypto-Maßnahmen wo anders definiert/formuliert?**

THALES

Praxisbezug an Hand von TISAX, ISO 27k & VDA ISA

5.1.1: Inwieweit wird die Nutzung kryptografischer Verfahren gemanagt?

- Es gilt beim Einsatz von kryptografischen Verfahren, sowohl Risiken im Bereich Verfügbarkeit (verlorenes Schlüsselmaterial) wie auch Risiken durch falsch angewendete Verfahren im Bereich Integrität und Vertraulichkeit (schlechte Algorithmen/Protokolle oder unzureichende Schlüsselstärken) zu berücksichtigen.

MUSS-Anforderungen:

- Alle eingesetzten kryptographischen Verfahren (z. B. Verschlüsselungs-, Signatur, und Hash-Algorithmen, Protokolle, Applikationen) bieten nach dem Stand der Technik die notwendige Sicherheit für das Einsatzgebiet.
- Rechtliche Rahmenbedingungen für den Einsatz von Kryptographie sind berücksichtigt.

SOLL-Anforderungen:

- Erstellung eines technischen Regelwerkes mit Anforderungen an die Verschlüsselung zum Schutz von Informationen gemäß ihrer Klassifizierung.
- Ein Nutzungskonzept für Kryptographie ist definiert und umgesetzt. Folgende Aspekte sind berücksichtigt:
  - Kryptographische Verfahren,
  - Schlüsselstärken,
  - Verfahren für den kompletten Lebenszyklus von kryptographischen Schlüsseln inkl. Erzeugung, Speicherung, Archivierung, Abruf, Verteilung, Deaktivierung, Erneuerung und Löschung.
- Ein Notfallprozess zur Wiederherstellung von Schlüsselmaterial ist etabliert.

Zusatzanforderungen bei hohen Schutzbedarf

- Anforderungen an Schlüsselhoheit (insbesondere bei organisationsfremder Verarbeitung) sind ermittelt und erfüllt. (C, I)

THALES

Herausforderungen bis zur (Prozess-)Bewertung

- **Der Prozess ☺**

- **1. Ermitteln von potenziellen Bedrohungen**
- **2. Ermitteln der Risiken durch Kombination Bedrohungsschaden und Eintrittswahrscheinlichkeit**
- **3. Risiko-Management (Akzeptanz, Reduktion, Transfer, Vermeidung)**
- **4. Maßnahme setzen**
  - Scoping erfordert Asset-Management und Klassifizierung
  - Rollout
- **5. Prüfen der Effektivität und wegen PDCA zurück zum Start**

THALES

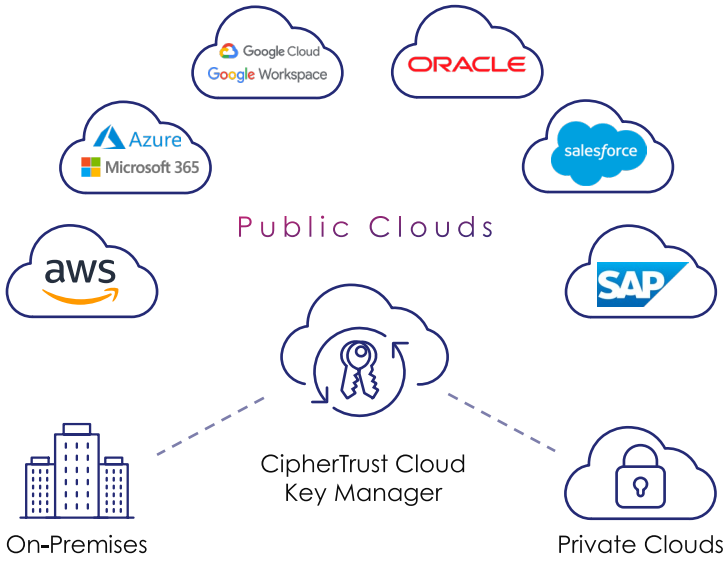
THALES
Building a future we can all trust

Immer öfter: Cloud-First

Thales als vertrauenswürdiger Schlüssel-Service

Take control of your sensitive data across clouds

Mitigate data security and privacy risks with separation of duty between your data and your cloud provider



Centralize multi cloud key management for BYOK, HYOK and cloud native encryption keys across any combination of clouds and on-premises with single UI

Increase efficiency with a single pane of glass view across regions, and automated key lifecycle management with a common set of APIs

Demonstrate compliance with data sovereignty laws and privacy regulations

CONTROL

THALES

BYOK / HYOK / BYOE

Bring your own Key

- Schlüsselmaterial wird lokal erzeugt und an HyperScaler übergeben
- Schlüsselhoheit liegt beim HyperScaler
- Key Life Cycle Management

Hold your own Key

- Schlüsselmaterial wird lokal erzeugt und in den eigenen Systemen verwaltet
- Schlüsselhoheit liegt beim Kunden
- Key Life Cycle Management

Bring your own Encryption

- Verschlüsselungslösungen und Schlüsselmanagement in Kundenhand
- Schlüsselhoheit liegt beim Kunden
- Key Life Cycle Management

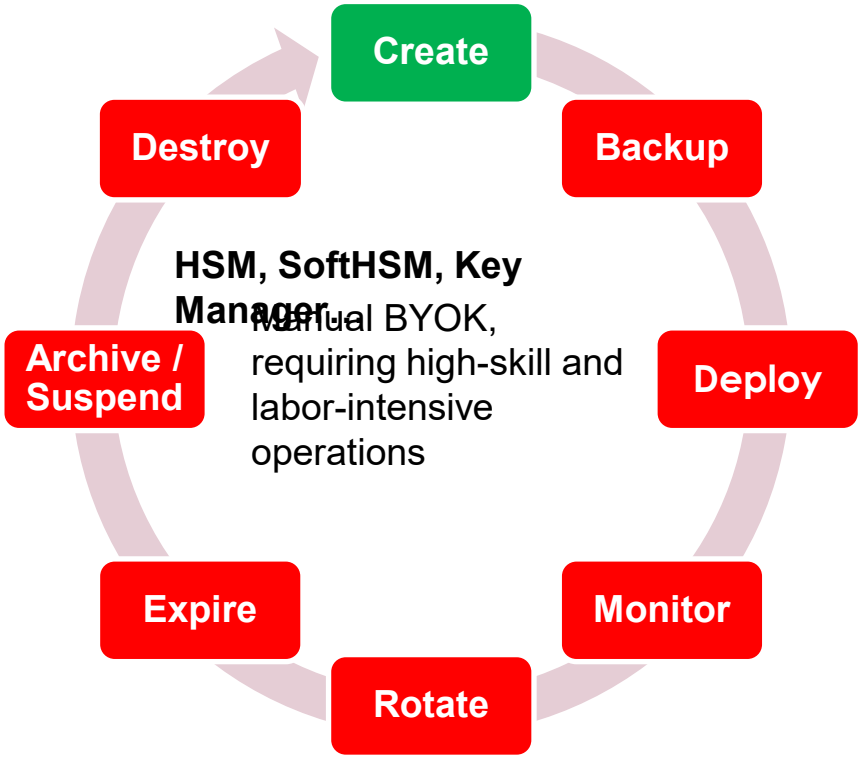
THALES

CipherTrust Cloud Key Manager

Integration with Cloud Services via BYOK scheme

Bring Your Own Key vs Managing Cloud Keys

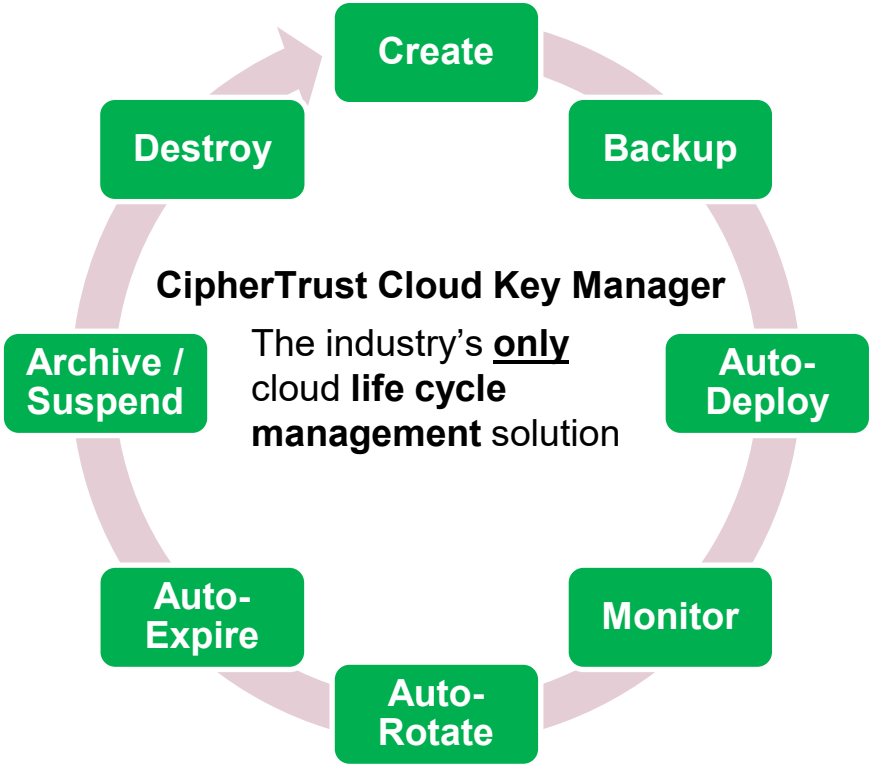
Bring Your Own Key



HSM, SoftHSM, Key Manager

Manual BYOK, requiring high-skill and labor-intensive operations

Cloud Key Life Cycle Management



CipherTrust Cloud Key Manager

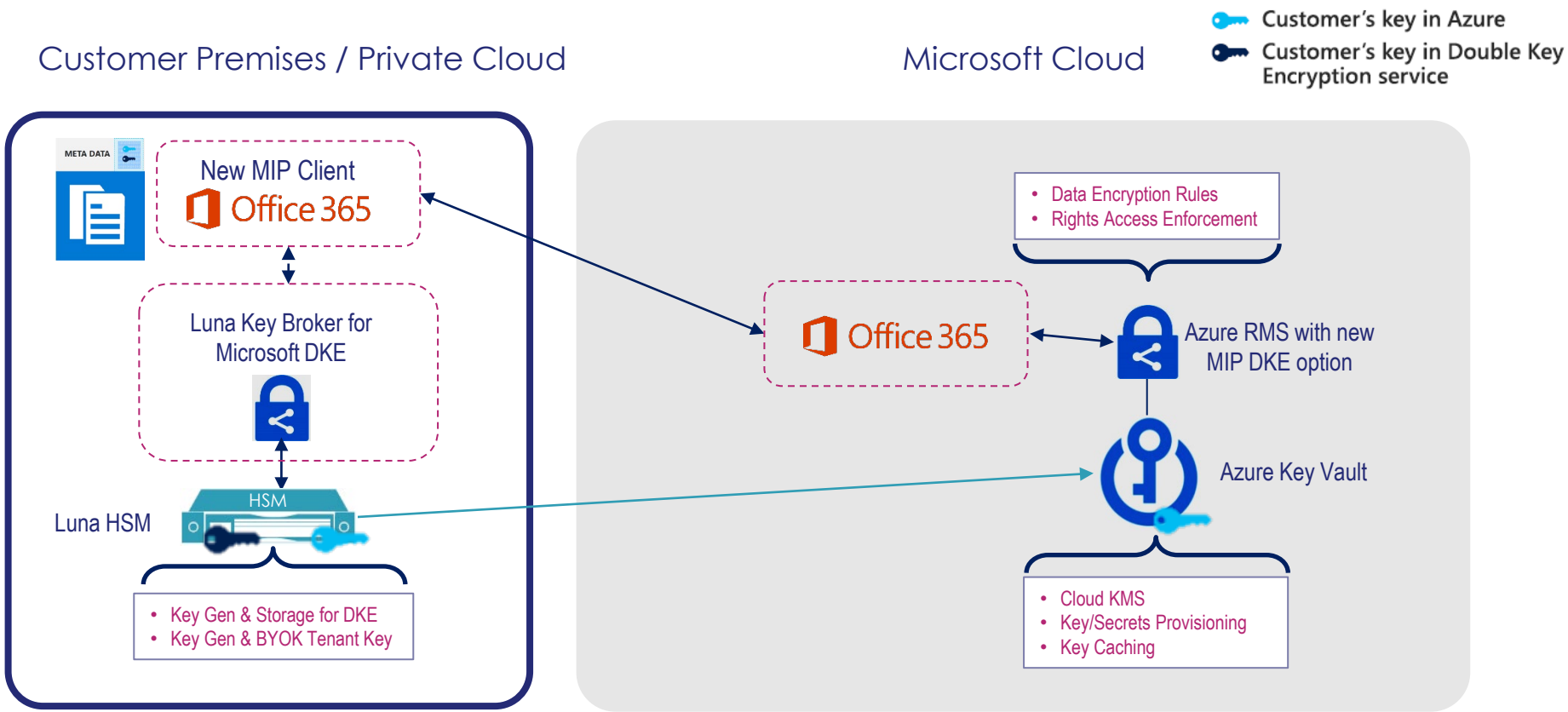
The industry's **only** cloud **life cycle management** solution

THALES

Double Key Encryption für Cloud-Organisationen

THALES

Microsoft 365 Encryption with Luna Key Broker for Microsoft DKE



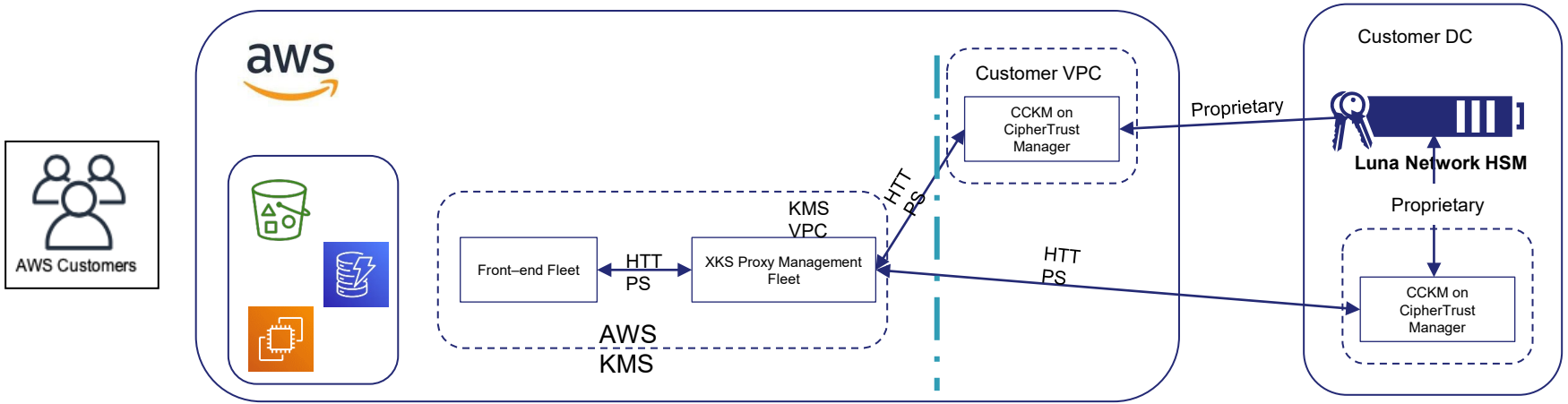
THALES

THALES

AWS KMS – External Key Store (XKS) with Thales CCKM

cpl.thalesgroup.com

AWS XKS integration with Thales CCKM



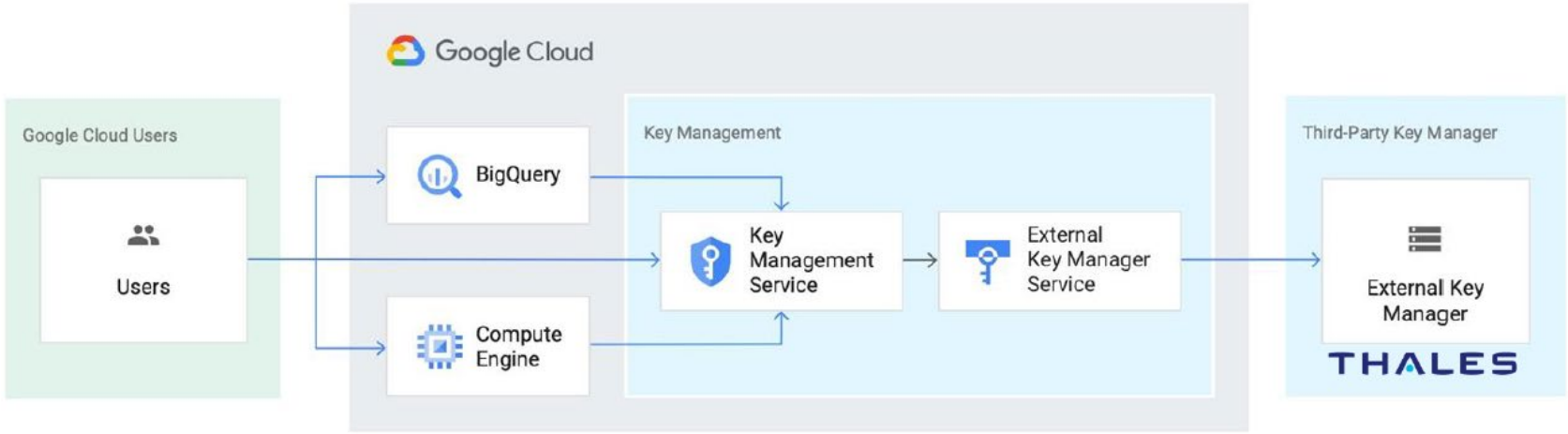
THALES

THALES

CipherTrust Key Broker for Google Cloud EKM

- What is Google Cloud EKM?
- CipherTrust Key Broker for Google Cloud EKM

Google Cloud EKM Overview



Google Cloud

THALES

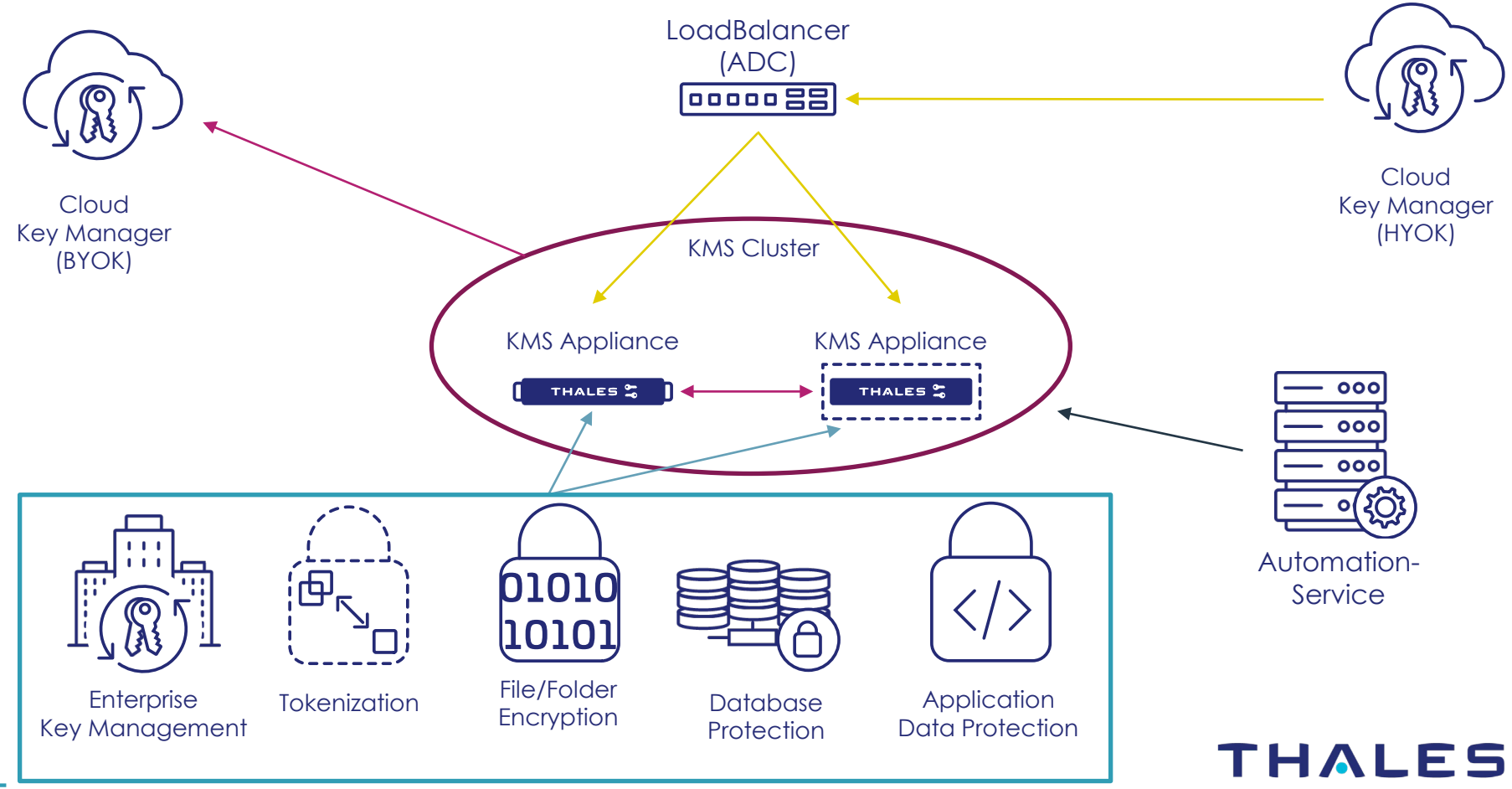
THALES
Building a future we can all trust

DSGVO-Szenario

„Stand der Technik“ umgesetzt im Bankenumfeld

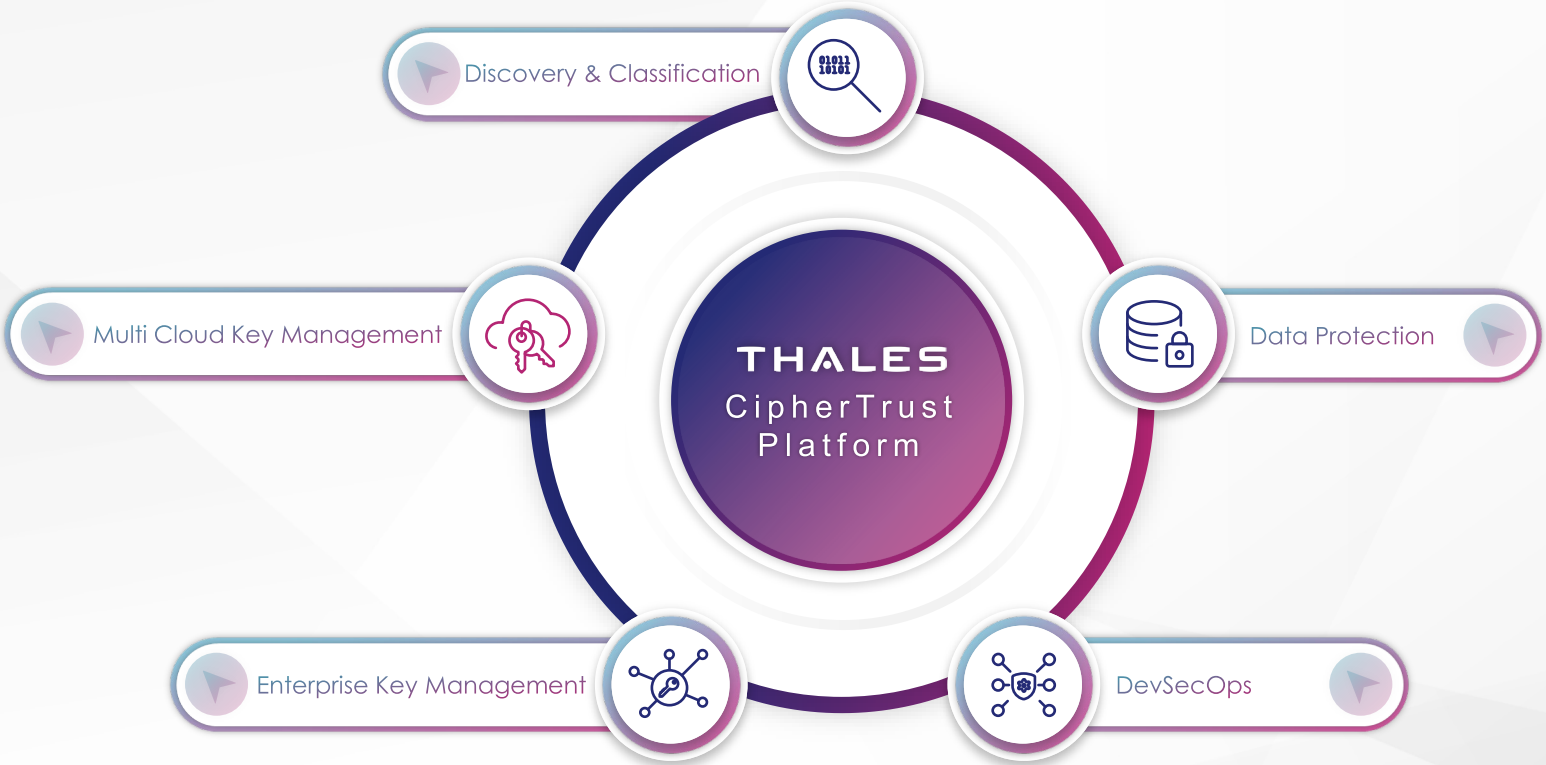
cpl.thalesgroup.com

Allgemeine Architektur



THALES

CipherTrust Data Security Platform



THALES

THALES
Building a future we can all trust

Ende