



NIS-2 – InfoSec für (fast) alle!

8. Mai 2023 | LSZ IT-Security Cyber Lounge



From the Bottom of the Oceans... to the Depths of Space & Cyberspace



#1

Worldwide in data protection

#2

Worldwide in civil satellite systems

#1

Worldwide in air traffic management

#2

Worldwide in inflight entertainment

#3

Worldwide in commercial avionics

#1

European provider of advanced sensors

#1

Worldwide in safe & smart airport solutions



Over **80,000** employees



68 Countries
Global presence



1bn € Self-funded R&D*

*Does not include externally financed R&D



Sales in 2021
16bn €

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>

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?

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.

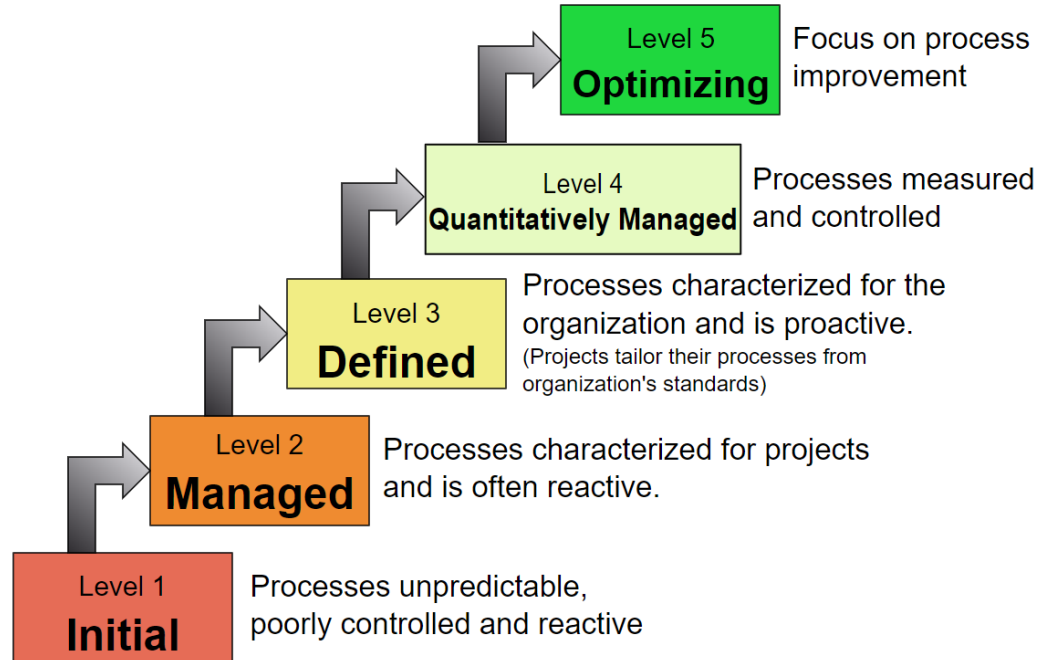
SOLL-Anforderungen:

- 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 hohem Schutzbedarf

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

Capability Maturity Model Integration



Der Prozess 😊

1. Ermitteln von potenziellen Bedrohungen

2. Ermitteln der Risiken durch Kombination Bedrohungsschaden und Eintrittswahrscheinlichkeit

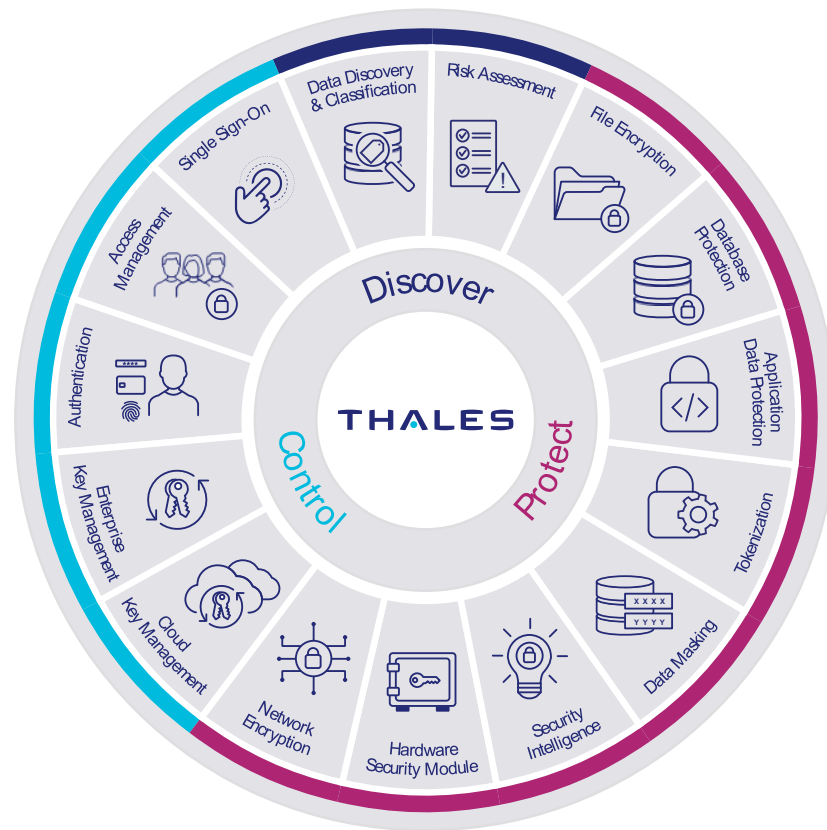
3. Risiko-Management (Akzeptanz, Reduktion, Transfer, Vermeidung)

4. Maßnahme setzen

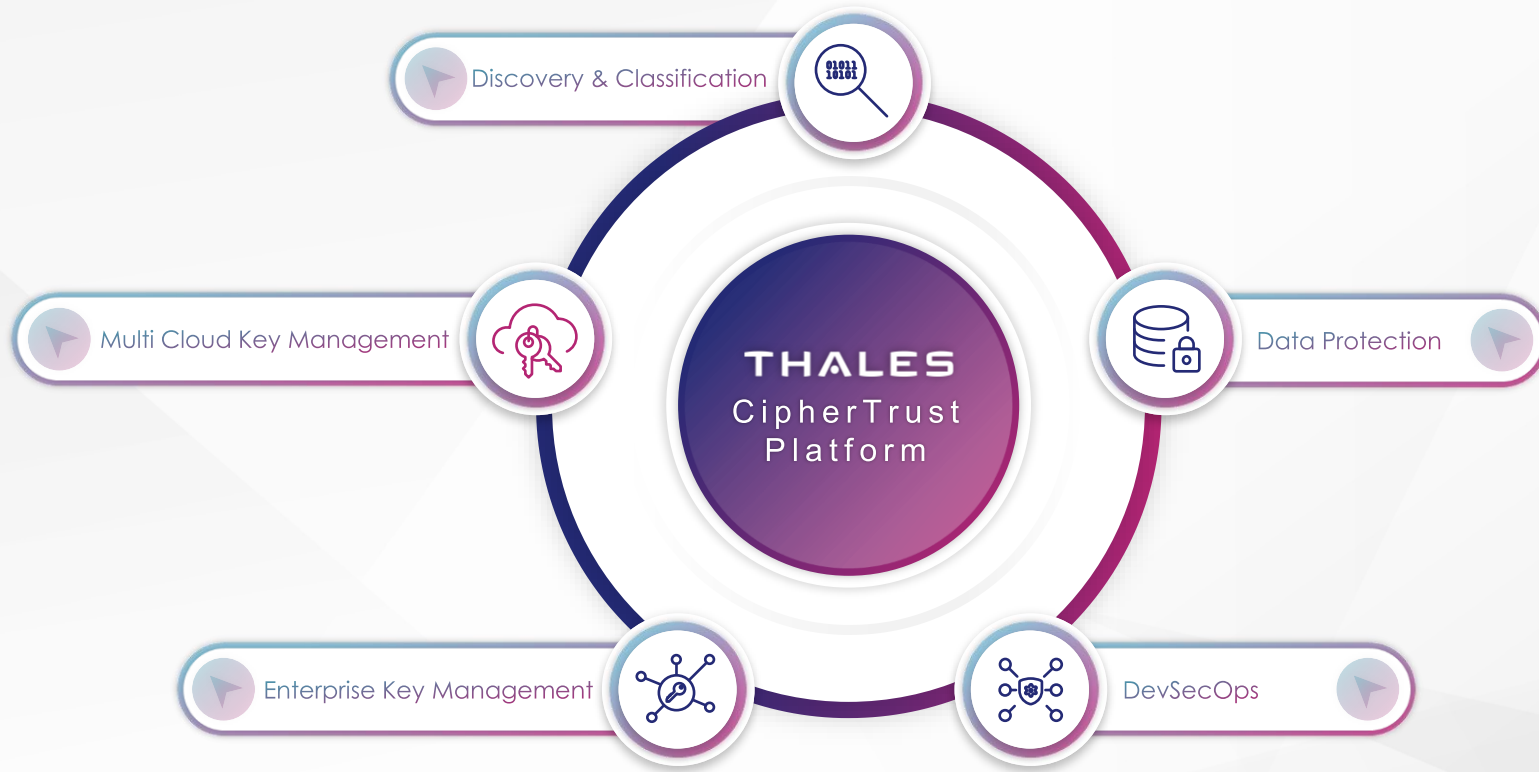
- Scoping erfordert Asset-Management und Klassifizierung
- Rollout

5. Prüfen der Effektivität und wegen PDCA zurück zum Start

Lösung für einen hohen Reifegrad (Level 2+)



CipherTrust Data Security Platform



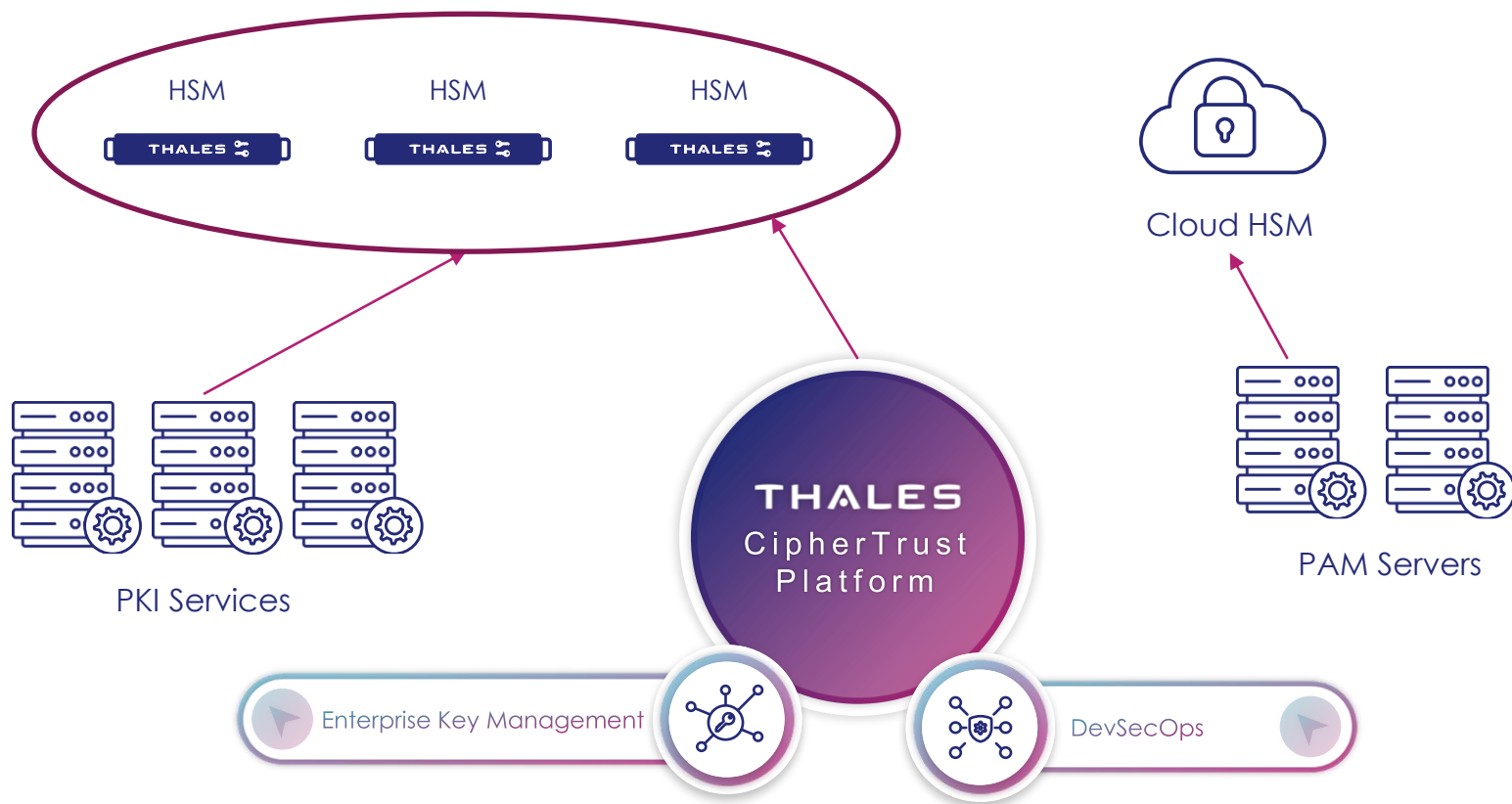


KVP-Szenario

Schritt für Schritt Maßnahmen erweitern



Von der PKI zur Crypto-Plattform





Immer öfter: Cloud-First

Thales als vertrauenswürdiger Schlüssel-Service



Double Key Encryption für Cloud-Organisationen





TISAX-Szenario

Lieferketten-Compliance als Business Critical Value



CipherTrust Transparent Encryption (CTE)

Transparently protects file system, volume data-at-rest

CipherTrust Transparent Encryption Agent

Allow/Block Encrypt/Decrypt/report



Privileged Users

Encrypted & Controlled

*\$^!@#){
-|"_]?\$%-
:>>



Approved Users

Clear Text

John
Smith
401 Main
Street



Cloud Admin

Encrypted & Controlled

*\$^!@#){
-|"_]?\$%-
:>>



**Transparent,
file-level encryption**

For all databases
and file types



**Privileged user
access controls**

Allows root users to
do their job, without
abusing data



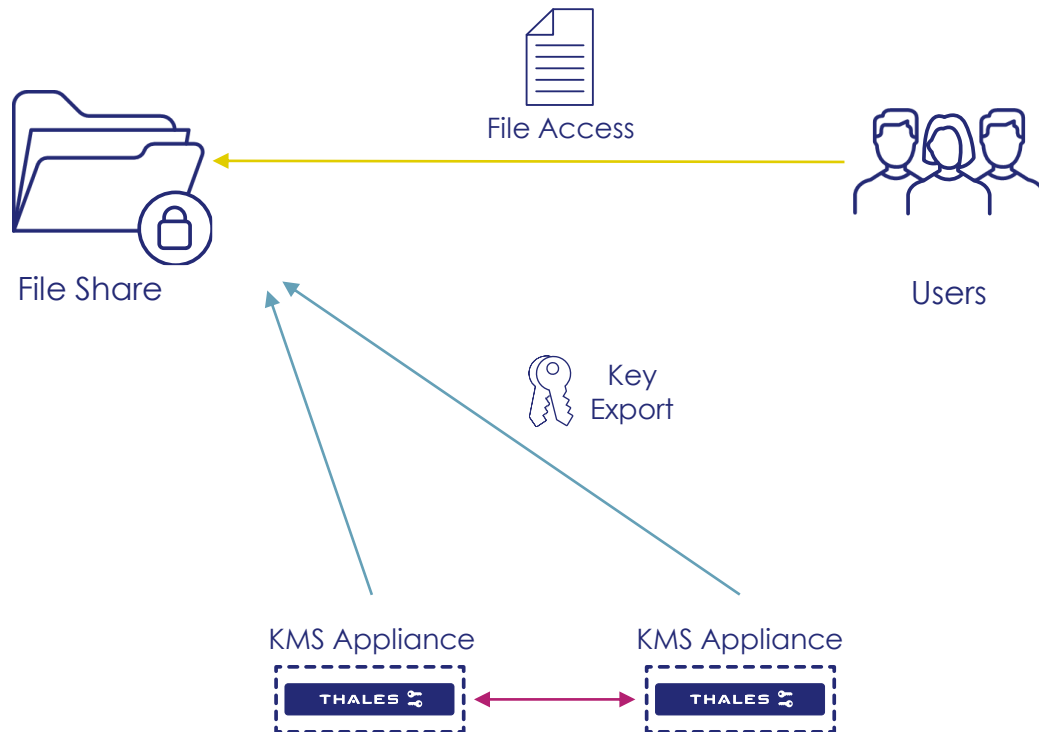
**Data access
audit logging**

Accelerate threat
detection and
ease forensics



**Centralized
encryption key and
data access policy
management**

Streamline
operations,
reduce risk,
satisfy compliance

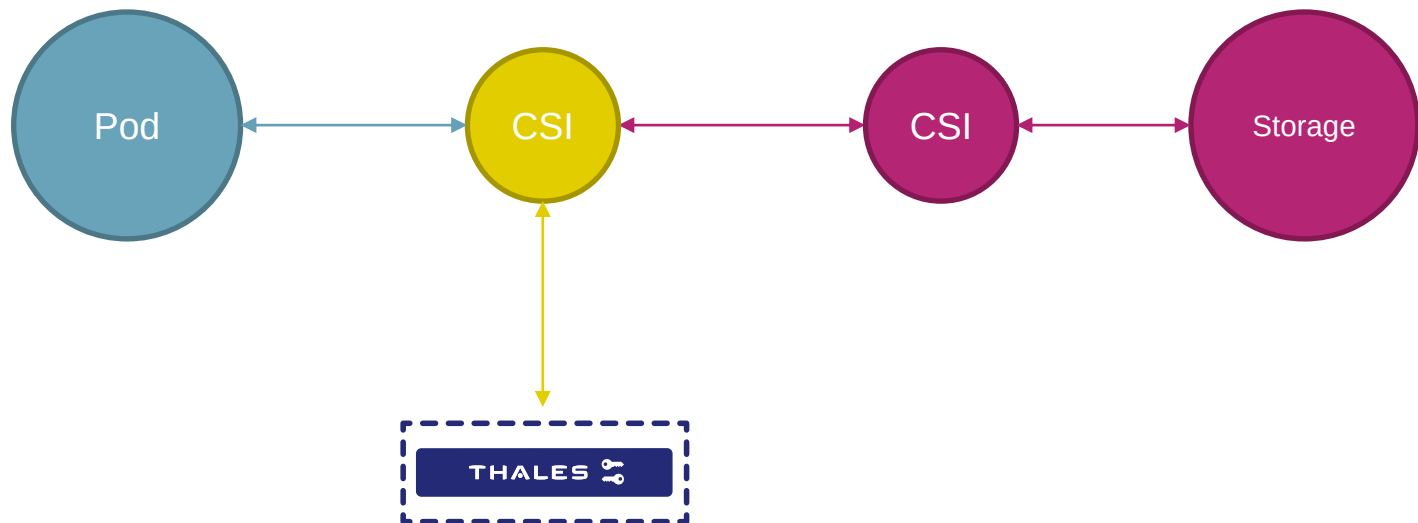




Verschlüsselung für moderne Apps

Beispiel aus dem öffentlichen Sektor





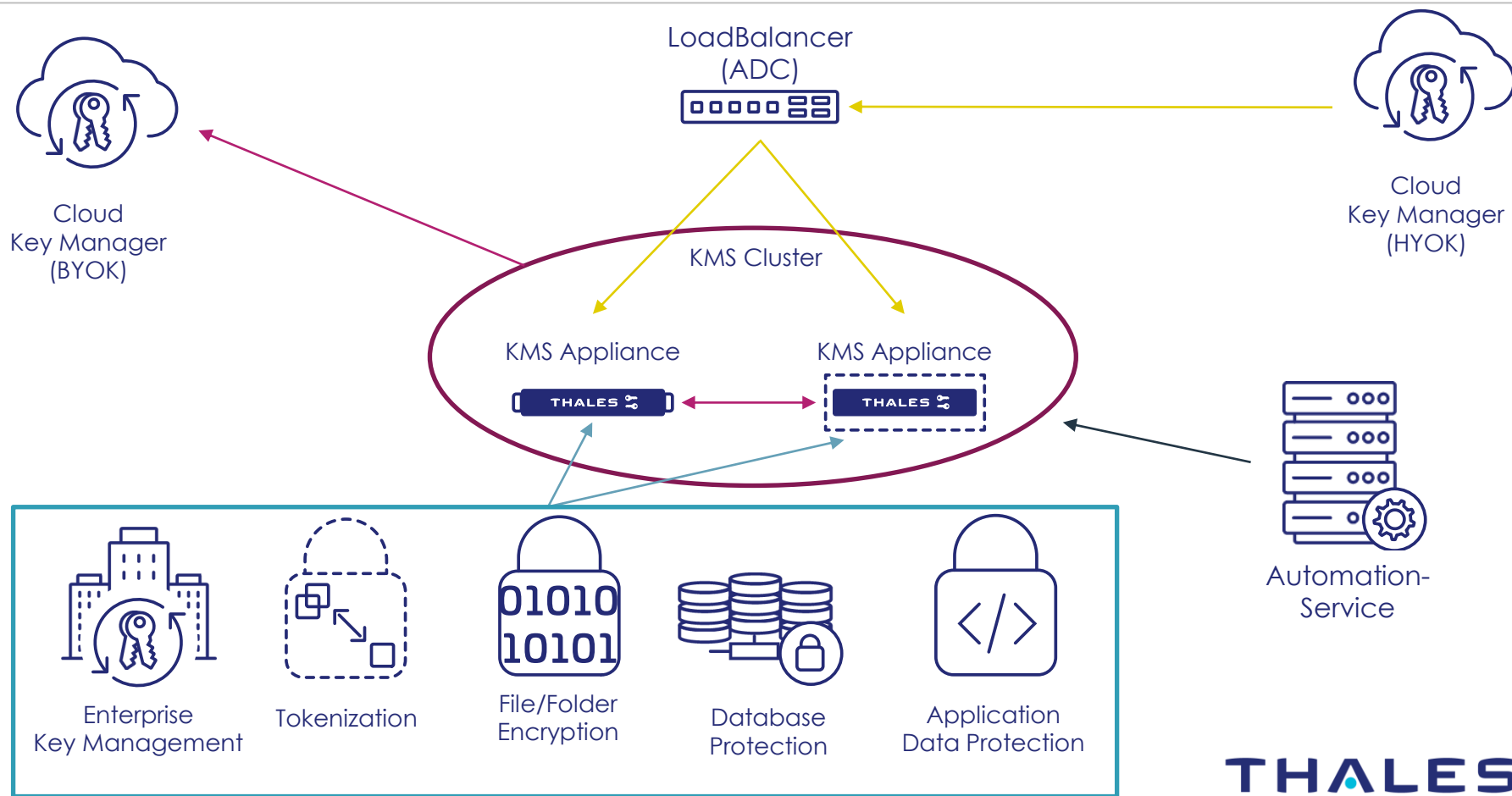


DSGVO-Szenario

„Stand der Technik“ umgesetzt im Bankenumfeld



Allgemeine Architektur





Ende

Fragen jetzt oder später

Thank you

Gracias شكراً لكم

धन्यवाद Merci

Danke 謝謝

ありがとうございました

