

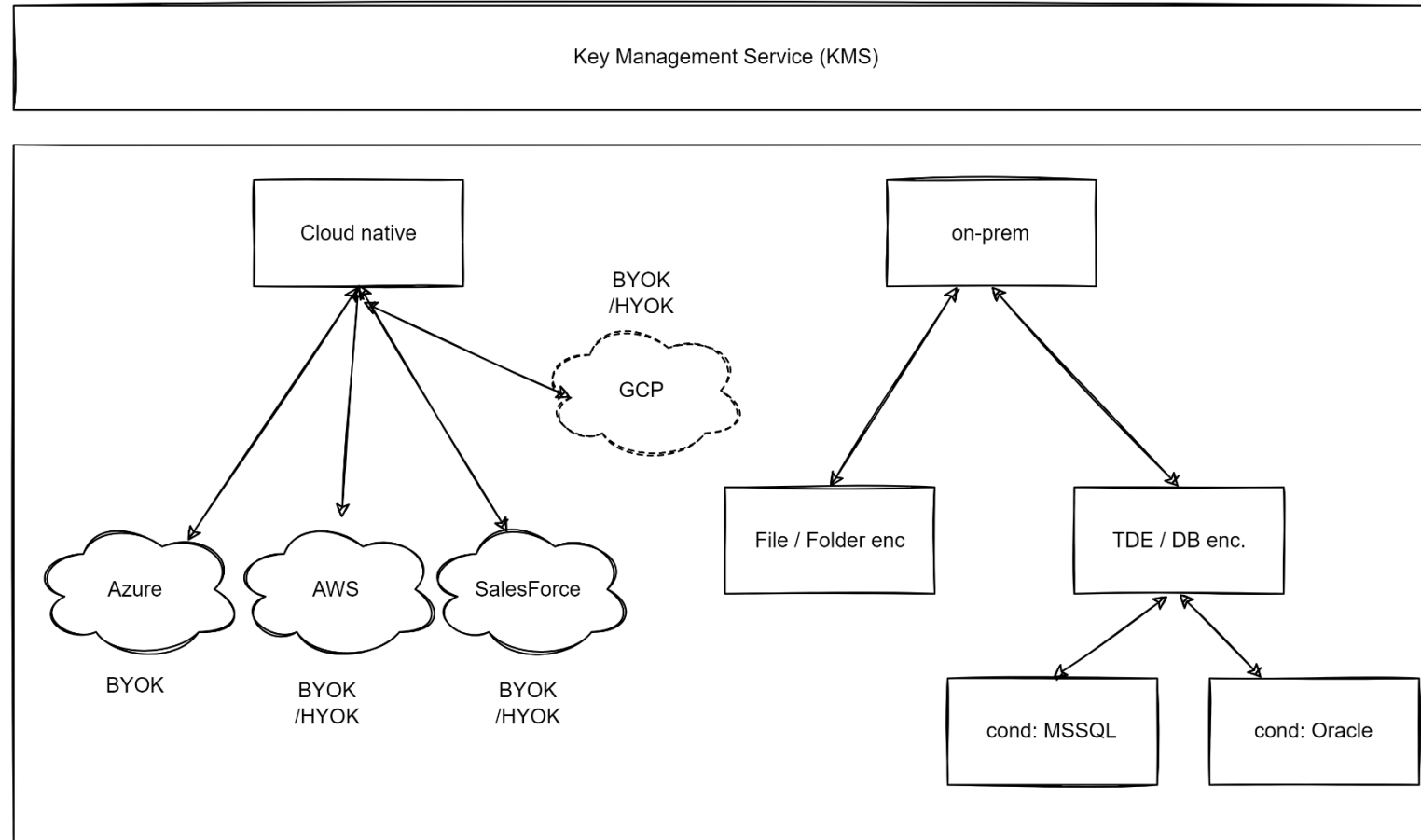
TeleTrust-EBCA "PKI-Workshop" 2023

Berlin, 21.09.2023

"Lessons learned Einführung eines Key Managements"

Stephan Plarre, E.ON Digital Technology GmbH

- Ausschreibung „Key Management System and Encryption-at-rest Services”
 - Betrieb als Service in „managed private cloud“
- Gefordert reife Software, auch wenn eher am Ende das Lifecycles
- Scope rund 400 Applikationen
 - >50% on premise





Q4/2019

Vertragsunterzeichnung
und Projektstart



Q2/2020

Initial geplante
Fertigstellung und Go Live



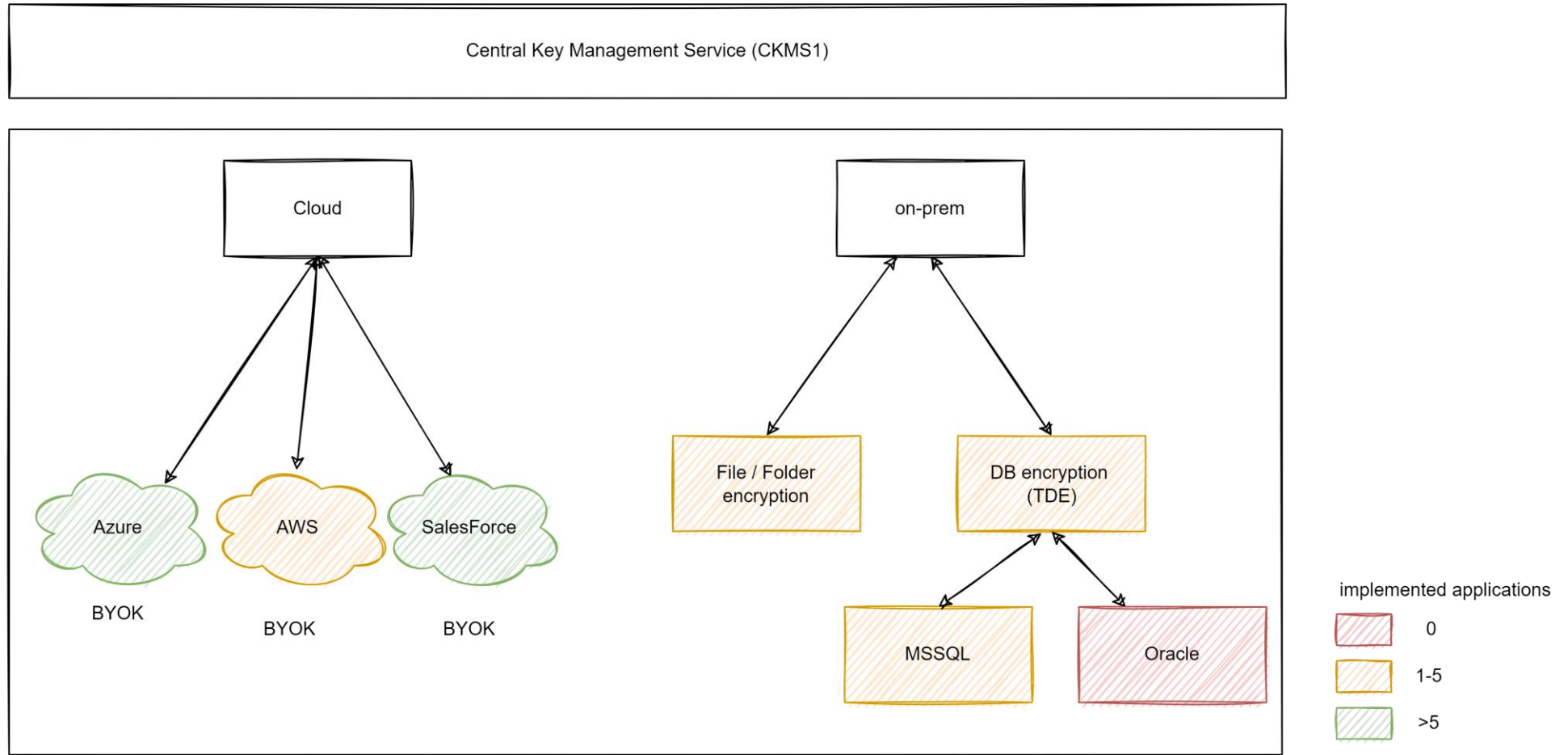
Ende Q1/2021

Golive mit ersten
Applikationen



seit Q1/2021

Anbindung von weiteren
Applikationen



- „on-prem“ ist jeweils applikationsspezifische Implementierung
- Massive Projektaufwände zur Implementierung
- Setzt tiefes Verständnis der zu schützenden Applikationen voraus
- > 6 Monate

Roll-out nicht skalierbar
nicht standardisierbar und automatisierbar

Herausforderungen – on prem

- **Verschlüsselung für Oracle - DB Cluster**
 - 40-50 DBs mit jeweils >100TB Daten
 - Verschlüsselung mit TDE - vom Hersteller supported
 - Oracle Support der DB Cluster gefährdet
 - Jedoch Einsatz nur von Oracle Vault / Key Management System supported

- SAP ähnliche Erfahrungen

Herausforderungen - Cloudification

- Covid19 hat unsere Cloud Strategie extrem beschleunigt
 - Migration von on-prem RZ's in die Cloud
- Große Herausforderungen für Applikationsteams
- Moderne Authentifizierung, Datenschutz, Key Management
- Lift & Shift für viele Applikationen

Modernisierung von Applikationen im Rahmen der Cloudification!

- Cloud ermöglicht einen niederschweligen Zugang, Verschlüsselung zu nutzen
- Cloud Stacks
 - ermöglichen Standardisierung
 - erlauben Automatisierung von Verschlüsselung / Key Management

Ist Verschlüsselung in der Cloud Homöopathie?

Nein!

Technische Betrachtung
vs.
Legal, Governance und Compliance

Bring Your Own Key / Hold Your Own Key

- Applikationsteam / ITSO setzen sich mit Situation auseinander
 - Verschlüsselung, Key Management, Datenschutz usw.
 - Sensibilisierung
- HYOK evaluiert
 - stark erhöhte Aufwände im Betrieb in unserem Setup
 - Verfügbarkeit ist Problem
 - Mehrwert kaum ersichtlich

E.ON hat sich aktuell für BYOK entschieden

- Erfüllung von GDPR Anforderungen
 - was es uns ermöglicht, diverse Supplier / Dienste zu nutzen
- Schutz gegen Supplychain Angreifer bei SaaS Anbieter
- Einführung von Verschlüsselung in der Breite

Crypto for the Masses!

- KMS als zentraler Service - unabhängig in welchem System
 - Cloud first, Standardisierung, Automatisierung, Automatisierung, Automatisierung
 - KMS 2.0 ist in Planung

KMS sollte keine Self-Ransomware sein

An aerial photograph of a dense forest of evergreen trees, likely spruce or fir, with varying shades of green and some yellowing foliage. The word "Danke" is overlaid in the center in a large, white, sans-serif font.

Danke

e-on

Stephan Plarre

Identity & Access Management

Cyber Security

M +491623343638 | stephan.plarre@eon.com

E.ON Digital Technology GmbH

Tresckowstraße 5

D-30457 Hannover

