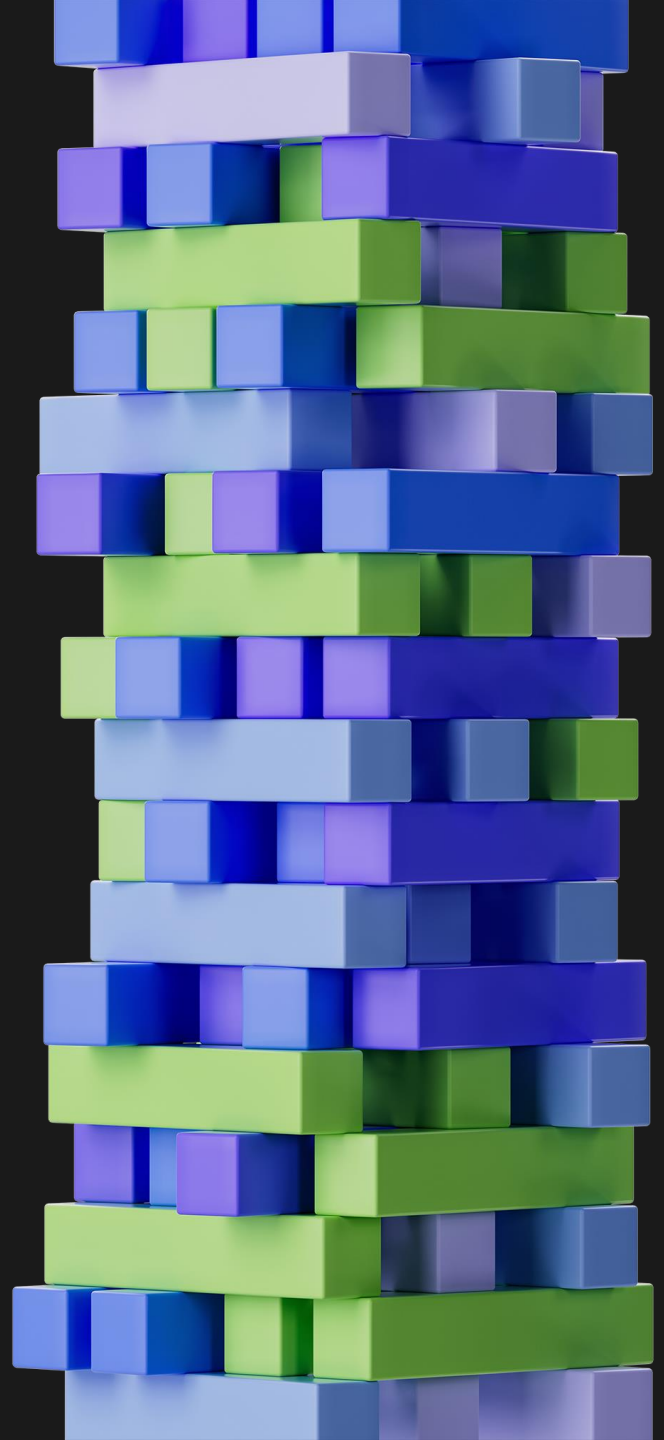
KEYFACTOR

Herausforderungen und praktische Lösungsansätze für PKI- und CLM-Experten

8. Mai 2025

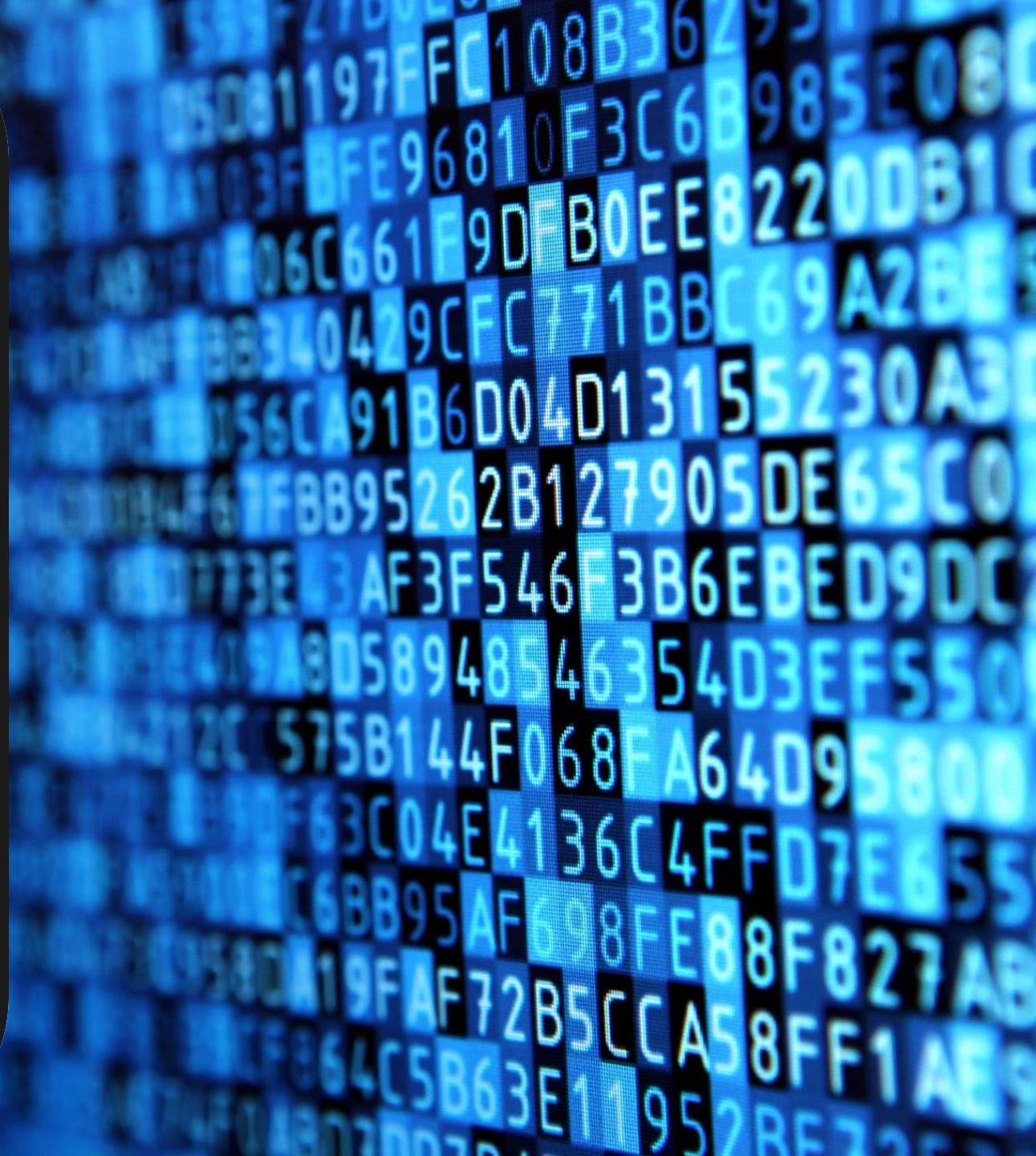
With you today

Tobias Schulz
Sales Director DACH



KEYFACTOR

Technologie führt zu neuen Lösungsansätzen



KEYFACTOR

8. Mai 2025

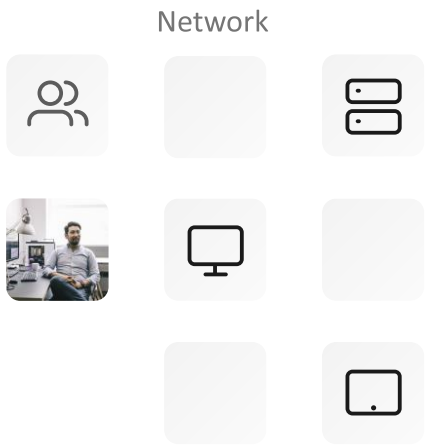
Digitale Identitäten für jedes Device

- 2023: Mehr als 40 Milliarden digitale Identitäten weltweit
- 90 % aller Unternehmen nutzen heute Zertifikate für Maschinenidentitäten
- 74 % der Sicherheitsvorfälle mit Zertifikatsbezug gehen auf menschliche Fehler oder fehlende Automatisierung zurück
- Durchschnittlich kommen 50–60 neue Zertifikate pro Tag in Großunternehmen hinzu

KEYFACTOR

Where we came from

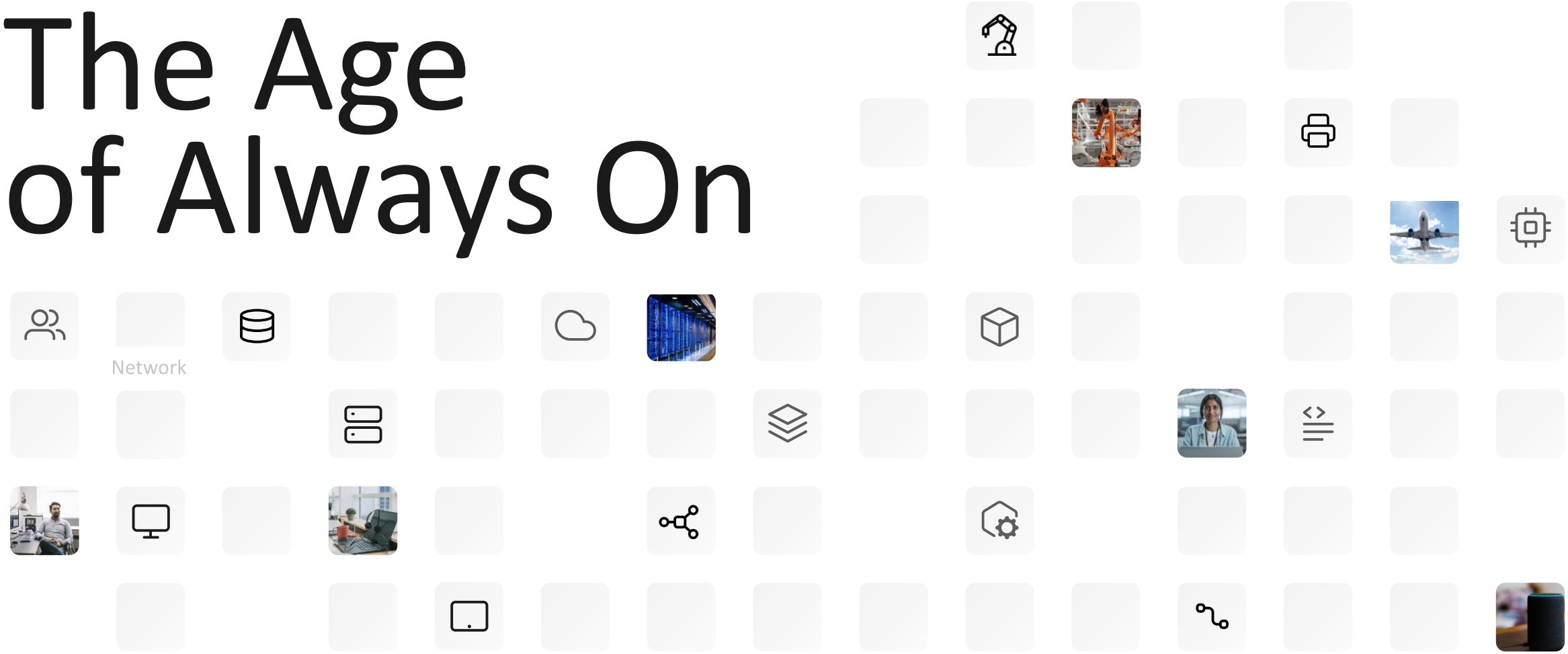
The Age of the Network



KEYFACTOR

Our hyper-connected reality

The Age of Always On



KEYFACTOR

Explosion der Maschinenidentitäten

- +40 % Zuwachs an Zertifikaten pro Jahr in großen Unternehmen
- DevOps, Zero Trust, IoT, Cloud, Container: Zertifikate überall
- 71 % der Unternehmen hatten in den letzten 2 Jahren einen Ausfall wegen abgelaufener Zertifikate
- Schattenzertifikate durch Dev- und OT-Teams ohne zentrales Management
- Audit-Lücken = Compliance-Verstöße (z. B. NIS2, ISO 27001)

KEYFACTOR

Neue Anforderungen bzgl. Compliance.

- **NIS2 (Network and Information Security Directive 2)**: EU-Richtlinie zur Verbesserung des Cybersicherheitsniveaus durch strengere Risikomanagement- und Meldepflichten für wesentliche und wichtige Einrichtungen.
- **DORA (Digital Operational Resilience Act)**: EU-Verordnung zur Sicherstellung der digitalen Betriebsstabilität von Finanzunternehmen gegenüber IKT-bezogenen Risiken und Störungen.
- **CRA (Cyber Resilience Act)**: EU-Verordnung, die verpflichtende Cybersicherheitsanforderungen für Hardware- und Softwareprodukte über deren gesamten Lebenszyklus hinweg festlegt..
- **IEC 62443** ist ein internationaler Standard zur Cybersicherheit industrieller Automatisierungs- und Steuerungssysteme (IACS), der Schutzmaßnahmen über den gesamten Lebenszyklus hinweg definiert und auf Betreiber, Integratoren und Hersteller ausgerichtet ist.

KEYFACTOR

The reality you face

Trust is Getting Complex.

More certificates

Shorter lifespans

PKI & CA sprawl

New use cases

Skills shortages

Quantum risks

KEYFACTOR

Welche Herausforderungen haben Sie mit ihren bisherigen Lösungen?

KEYFACTOR

Anforderungen an die Root of Trust

- Inventarisierung, Transparenz, Ordnung, Automatisierung.
- Deckt die Compliance Anforderungen ab.
- Integrierbar in bestehende Konzepte und Systeme.
- Flexibel im Deployment (SaaS, Cloud, On-Prem, Hybrid).
- Skaliert von kleineren bis sehr großen Zertifikatsvolumen.
- Integrierbar in IT Sicherheitskonzepte von Unternehmen.

KEYFACTOR

Microsoft CA erfüllt nicht mehr die aktuellen Anforderungen

- ADCS wird von Microsoft **nicht mehr aktiv weiterentwickelt**
- **Microsoft Cloud PKI** ausschließlich zur Erstellung von Zertifikaten über Intune
- Aktuelle **Enrollment-Protokolle** werden nicht unterstützt
  - EST – Enrollment over Secure Transport
  - ACME – Automatic Certificate Management Environment

Funktion	**MSCA**	**Moderne Pki / CLM-Plattform**
Protokolle	Nur AD	ACME, SCEP, EST, API
Plattformsupport	Windows	OS-agnostisch
Deployment	Nur On-Prem	On-Prem, Cloud, Hybrid
Automatisierung	Gering	Vollständig integriert
Reporting & Audit	Minimal	Revisionssicher
PQC-Vorbereitung	Nicht geplant	Strategien & Pilotintegration

KEYFACTOR

Flexible Deployment-Modelle im Vergleich

Modell	Beschreibung	Typische Anwendung
On-Prem	Lokale Kontrolle, hohe Regulierung	Banken, Industrie, KRITIS
Hybrid	Lokale Instanzen + Cloud PKI, CLM	IT zentral, OT dezentral. Prod. Gewerbe
Edge Deployment	Lokale CA-Proxies für OT/IIoT	Fertigung, Infrastruktur, Energie
PKI-as-a-Service	Komplett in der Cloud, API-first	kein In-House team, Automatisierungsgrad hoch.
CLM-as-a-Service	Heterogene Systeme, CLM, als managed-service durch Partner	Große Unternehmen mit verschiedenen Geschäftsbereichen, Verantwortlichkeiten.

KEYFACTOR

Beispiel:

Deutscher

Heizungsbauer

KEYFACTOR

8. Mai 2025

CRA als Treiber:

Der Cyber Resilience Act (CRA) erfordert erhöhte Sicherheitsstandards für Produkte mit digitalen Elementen in der EU.
Die Umsetzung muss bis September 2026 abgeschlossen sein.

Zielsetzung:

Eine sichere, skalierbare und flexible PKI-Infrastruktur aufbauen, die den Anforderungen des CRA gerecht wird und eine sichere Basis für die nächsten Jahrzente liefert.

1. **Sicherstellung der Authentifizierung und Autorisierung von IoT-Geräten gegenüber der Cloud.**
2. **Gewährleistung der Integrität von Software-Updates.**
3. **Erfüllung von Compliance-Anforderungen (z.B. BSI, NIST, CRA).**
4. **Bereitstellung der Lösung in wenigen Wochen.**
5. **Laufzeit der Lösung >10 Jahre.**

KEYFACTOR

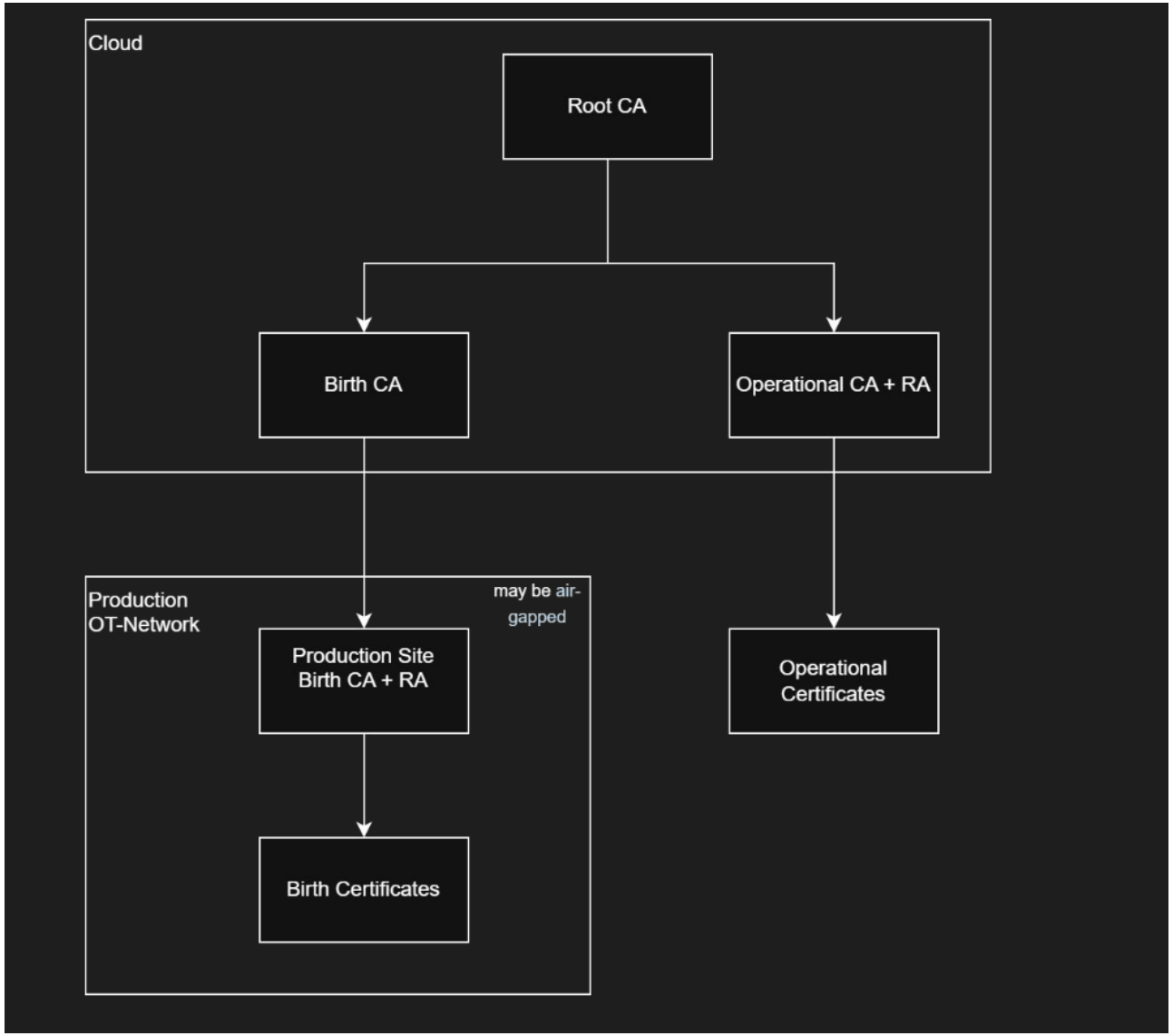
Get all the benefits of owning PKI without the risk and cost of running your own infrastructure running in a Single-Region Highly Available configuration.

Keyfactor PKI-as-a-Service Cloud Solution hosted in Azure

Hybrid CLM+PKI for Production and internal IT

Next Generation turn-key Hardware Appliance for the Offline-Air-Gaped Production Facility.

Keyfactor Hardware Appliance build in Aachen, Germany with Thales or Utimaco HSM included.



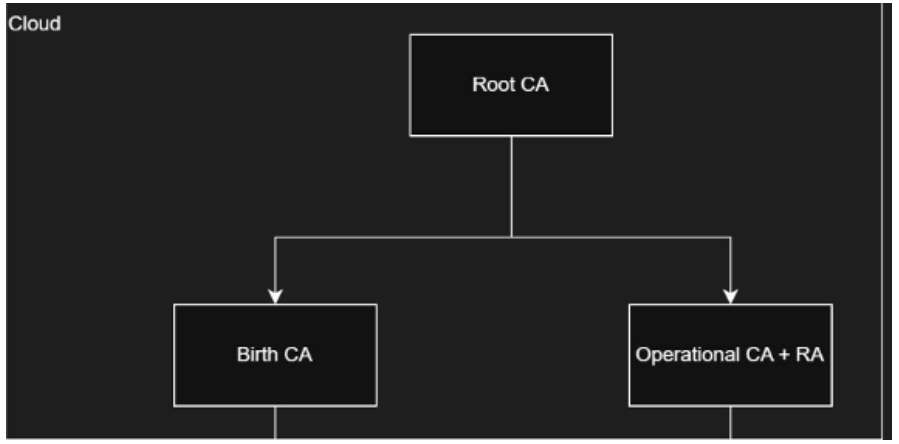
KEYFACTOR

Keyfactor PKI-as-a-Service Cloud Solution hosted in Azure

Fully managed by Keyfactor- delivered as-a-service

- Hosted in EU- 2 Datacenters for High Availability
- 99.95% uptime of Keyfactor Command and EJBCA
- RTO/RPO 4 hours
- PKI Root Hosted in SOC 2 Type II compliant primary datacenter
- Protected by FIPS 140-2 Level 2 Hardware Security Module (HSM) (Root)
- Industry best practice secure and auditable root signing ceremony (Root)
- Minimum of 2 certified Keyfactor employees required to access root materials K-of-N smart card HSM access redundancy between primary/secondary datacenter

Included:
• 1 offline root CA
• 1 FIPS 140-2 Level 2 HSM
• 1 root signing ceremony
• 1 signed root signing ceremony transcript
• 3 sets of HSM smart cards



System Setup

- Professional Services engagement required
- Root key signing ceremony
- Scripted Platform & Infrastructure deployment
- Scripted Configuration
- Admin Account Setup
- OIDC integration to customer IAM system

KEYFACTOR

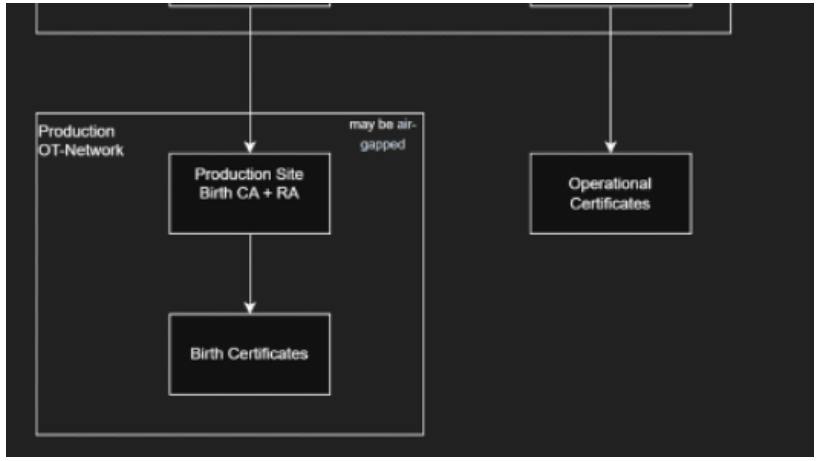
Offline-Air-Gapped Solution- Keyfactor HW Appliance

Fully Automated turn-key Appliance

- Hardware Appliance Platform
- Installation, configuration, and maintenance tasks are performed from a user-friendly graphical user interface
- Built in FIPS 140-2 Level 3 Certified HSM
- HA support with Master-Master replication for redundancy and performance
- Remote syslog shipping
- Secure & Automated Backup Mechanism
- 2 Factor Authentication
- Dedicated Mng & App Interfaces
- SNMP, Syslog, Audit Log

Included:

- Common Criteria certified
- CAB Forum / eIDAS / Webtrust / ETSI
- Unrestricted number of PKI hierarchies
- X.509 and CVC certificates
- Supports all major algorithms and protocols
- Highly flexible and scalable



System Setup

- Professional Services engagement required

KEYFACTOR

Quantum-ready solutions