

TeleTrust-EBCA "PKI-Workshop" 2023

Berlin, 21.09.2023

"Cross-PKI Web-of-Trust als Enabler für Zusammenarbeit"

Gregor Jehle, P3KI

Meta

- Gregor Jehle, Dipl. Inform. (FH)
- GF @ P3KI GmbH
- Web-of-Trust Technologie zur
Autorisierung/Authentifizierung seit 2014
- Kundenstamm primär Industrie, KRITIS, Defense

Wünsch dir was & Randbedingungen

- Verteilte bis dezentrale Anwendungsfälle (inkl. Offline / Air-Gap)
 - Hochresiliente Systeme mit Partitionstoleranz
 - Autorisation unvorhergesehener Interaktionspartner
-
- Kurz: nein, keine Blockchain

Technologie: keine Lösung, immer Tradeoff

- CAP
Consistency, **A**vailability, **P**artition tolerance, ...Nimm zwei!
- ACID
Atomicity, **C**onsistency, **I**solation, **D**urability
- BASE
Basically **A**vailable, **S**oft state, **E**ventual consistency

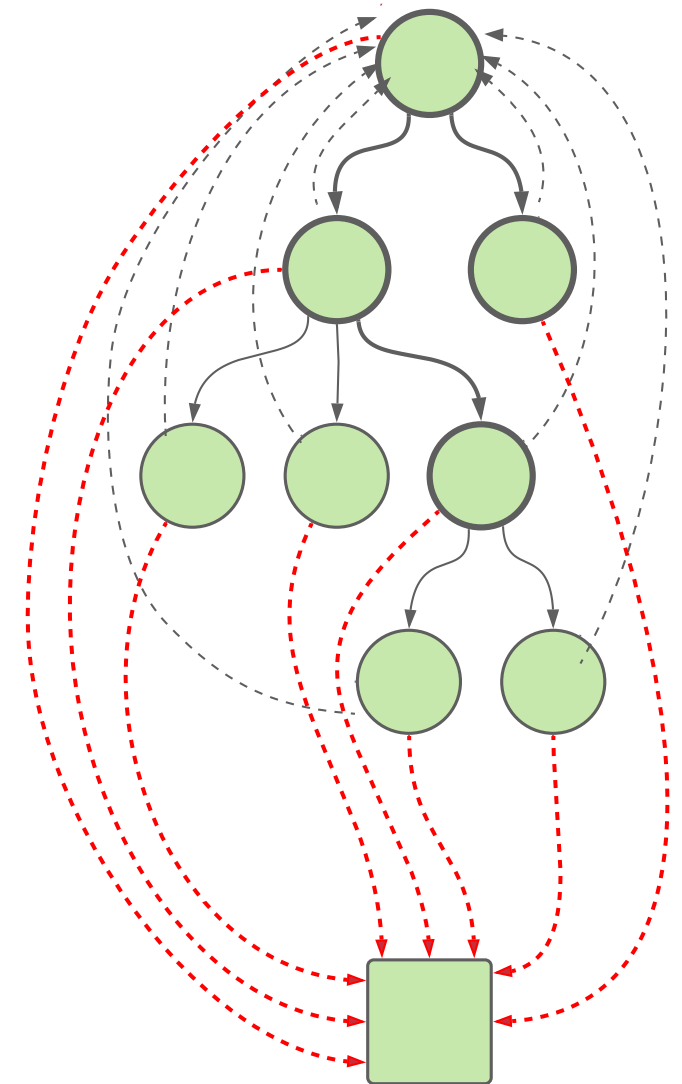
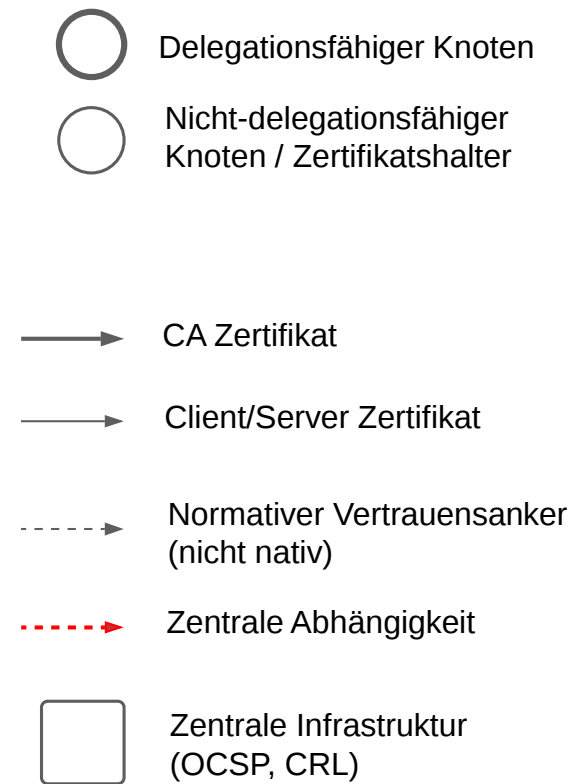
Kernaspekte PKI

- PKI verwaltet Schlüssel und weist ihnen Namen zu
 - Widerruf Intermediate-CA impliziert Widerruf aller ihrer Äste
 - Widerrufsprüfung idR online und zentralisiert oder nicht skalierend
-
- Kurz: Machbar mit zentraler Provisionierung in Onlinesystemen!

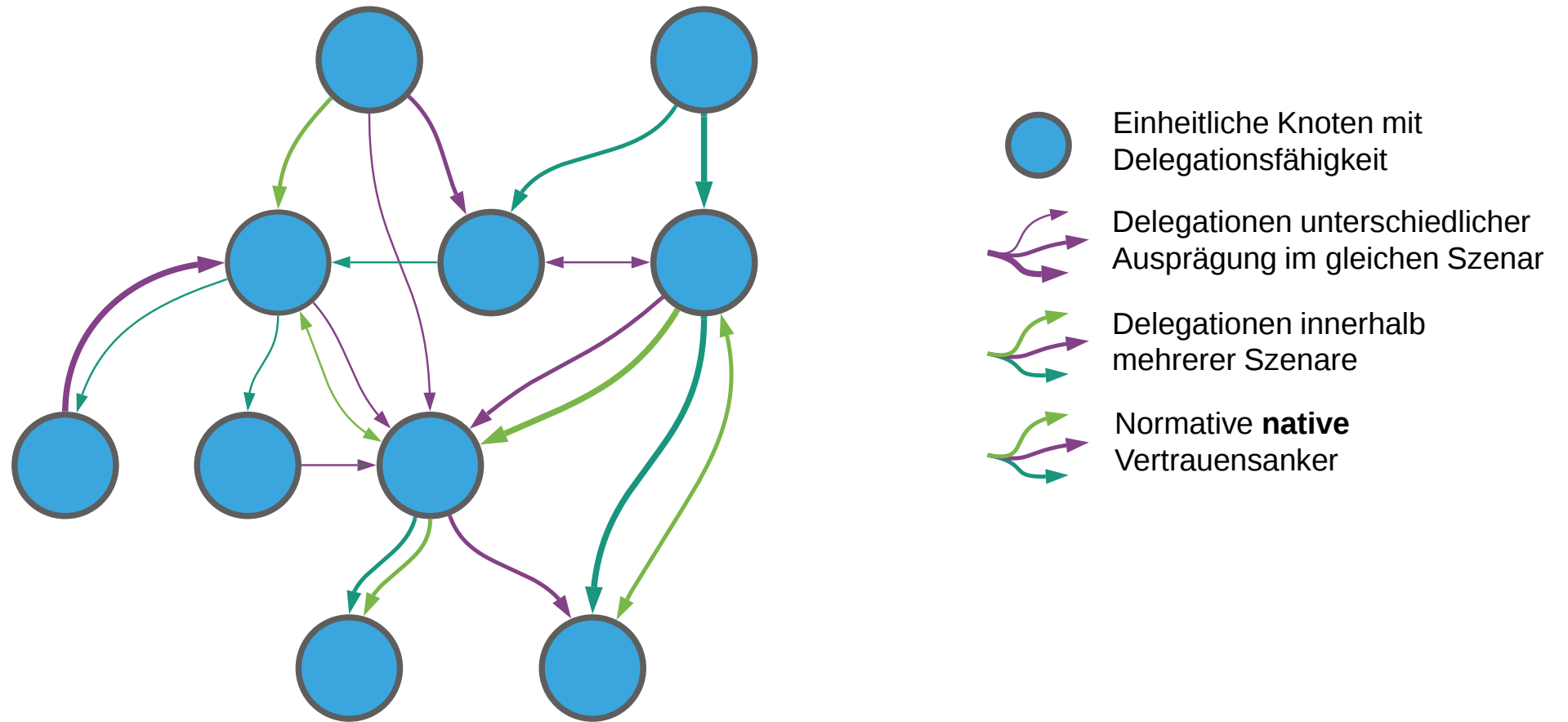
Kernaspekte PKI (cont.)

- Authorisation via PKI ist grob innerhalb enger Szenarien
 - Keine einfache Interaktion über mehrere PKI Hierarchien hinweg
 - *Name Constraints* Extension selten und inconsistent benutzt
-
- Kurz: Flexible, un-provisionierbare Szenarien nicht abbildbar

Klassische PKI



Web-of-Trust

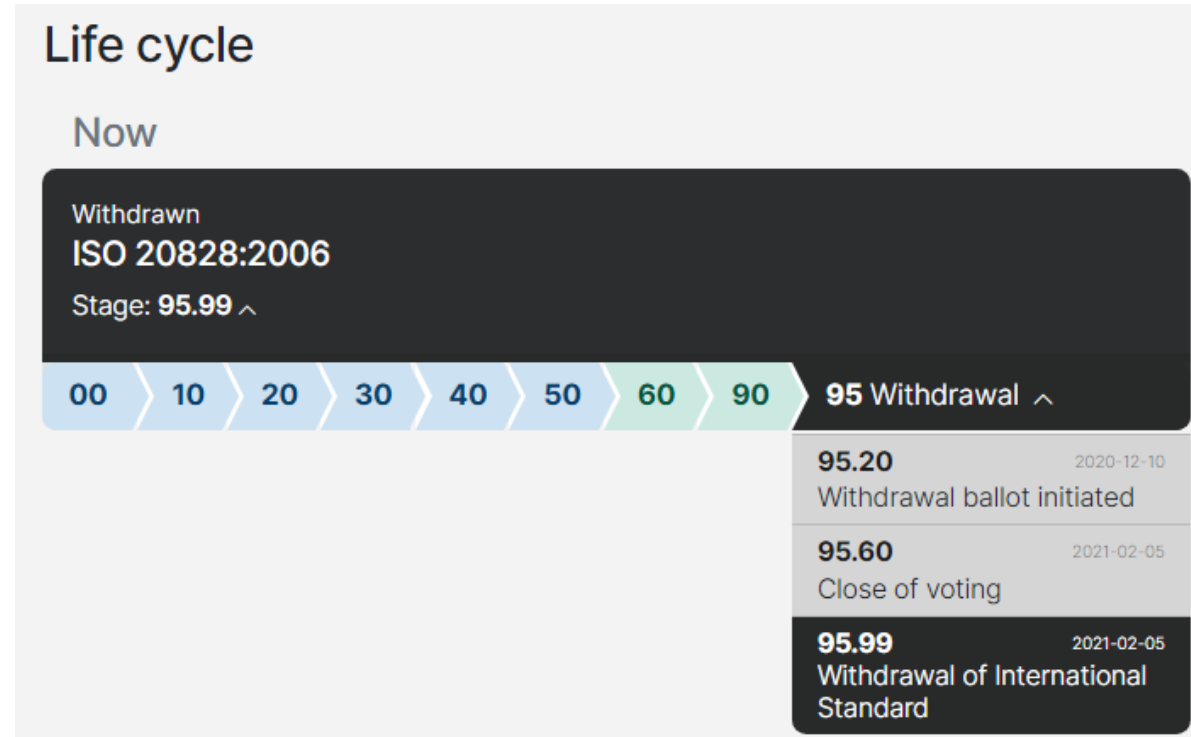


Kernaspekte Web-of-Trust

- Hierarchiefrei
 - Dezentrale Datenhaltung möglich
 - Partitionstolerant: Implizit Offline und Air-Gap tauglich
 - Dezentrales Management üblich
 - “self-sovereign” Berechtigungssystem / Vollmachtssystem
 - Individuelle statt globaler Wahrheit
-
- Kurz: hoch flexibel und resilient, aber nicht einfach orchestrierbar

Hype und Hupe: ISO 20828:2006

- Automotive sah die Zukunft und zog korrekte Schlüsse
- Verteilte Wartung und Kommunikation benötigen verteilte PKI
- Idee: super
Umsetzung: als Inspiration okay
- Standard starb mit/an Covid



Web-of-Trust Baukasten

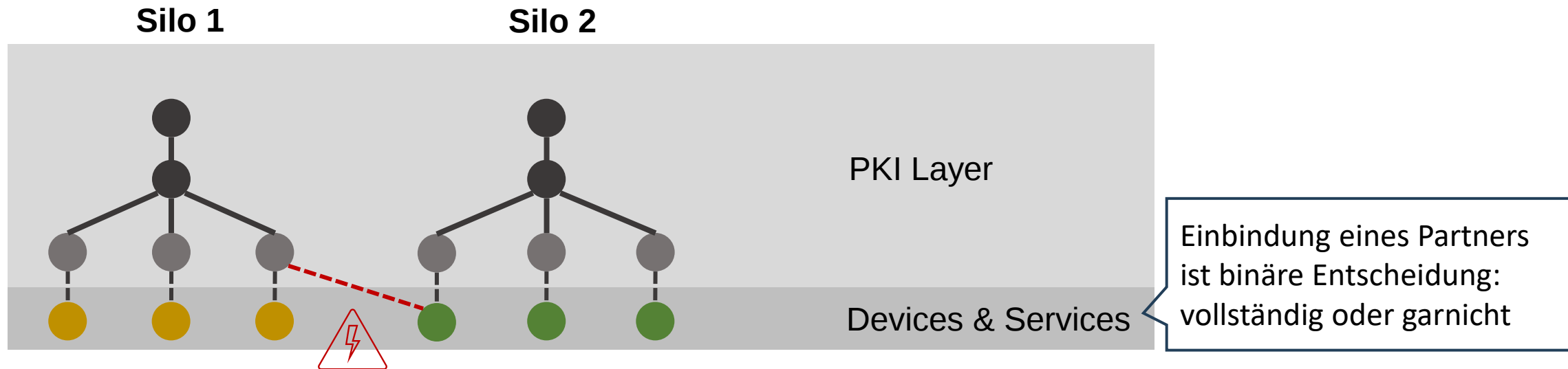
- Identitäten / Schlüsselpaare
- Gewichtete Beziehungen
- Option auf dezentrale Datenhaltung
- Flurfunkfähigkeit

Web-of-Trust(PKI) → Hybrid-PKI

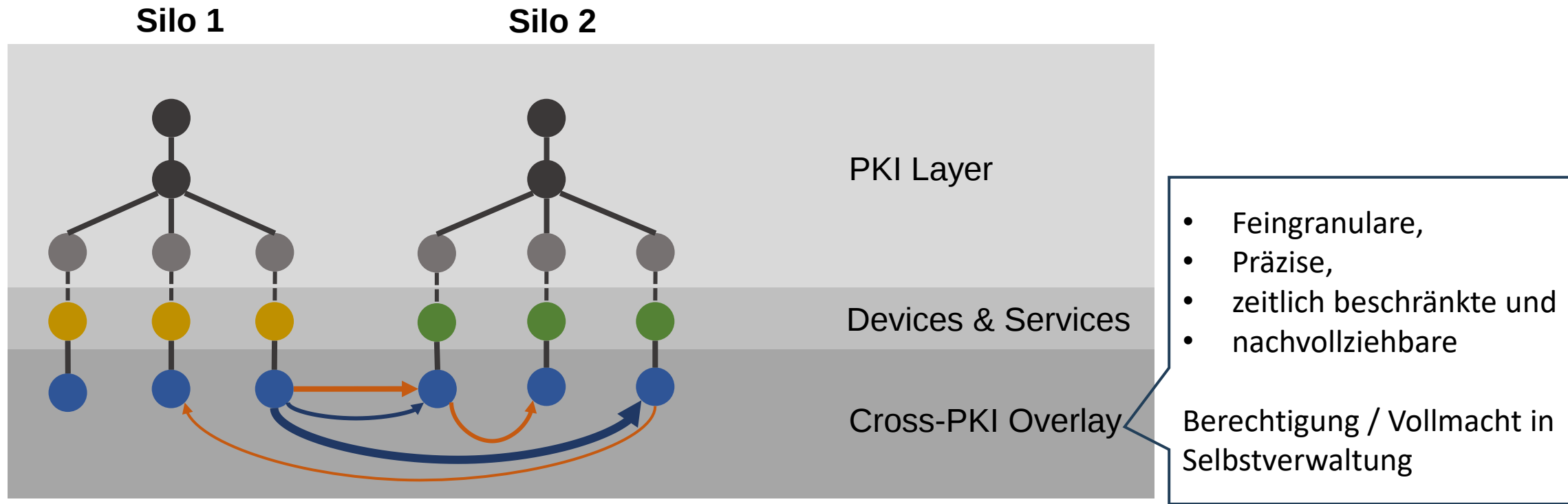
- Schlüsselmanagement, HSM, etc wie gewohnt
- Zertifizierung der PKI bleibt unberührt
- Tauschpfand:
Global eindeutige Namen,
zentrales Management,
negativer Widerruf
- Gewinn:
Ad-hoc Reaktionsfähigkeit
unter widrigsten Umständen



Silo-Interaktion (or lack thereof)



Silo-Interaktion mit WoT Cross-PKI Overlay



Nochmal langsam

- Weder PKI noch WoT lösen alle Herausforderungen individuell
- Kombination aus PKI und WoT eröffnen neue Möglichkeiten
 - Extreme Resilienz
 - Voll offlinetauglich
 - Interaktion über PKI-Hierarchien hinweg
 - Gewohnte Schlüsselhandhabung
- Nichts im Leben ist kostenlos
 - Keine globalen Namen
 - Kein rein-zentrales Management
 - Neuaussage statt Widerruf

Warum?

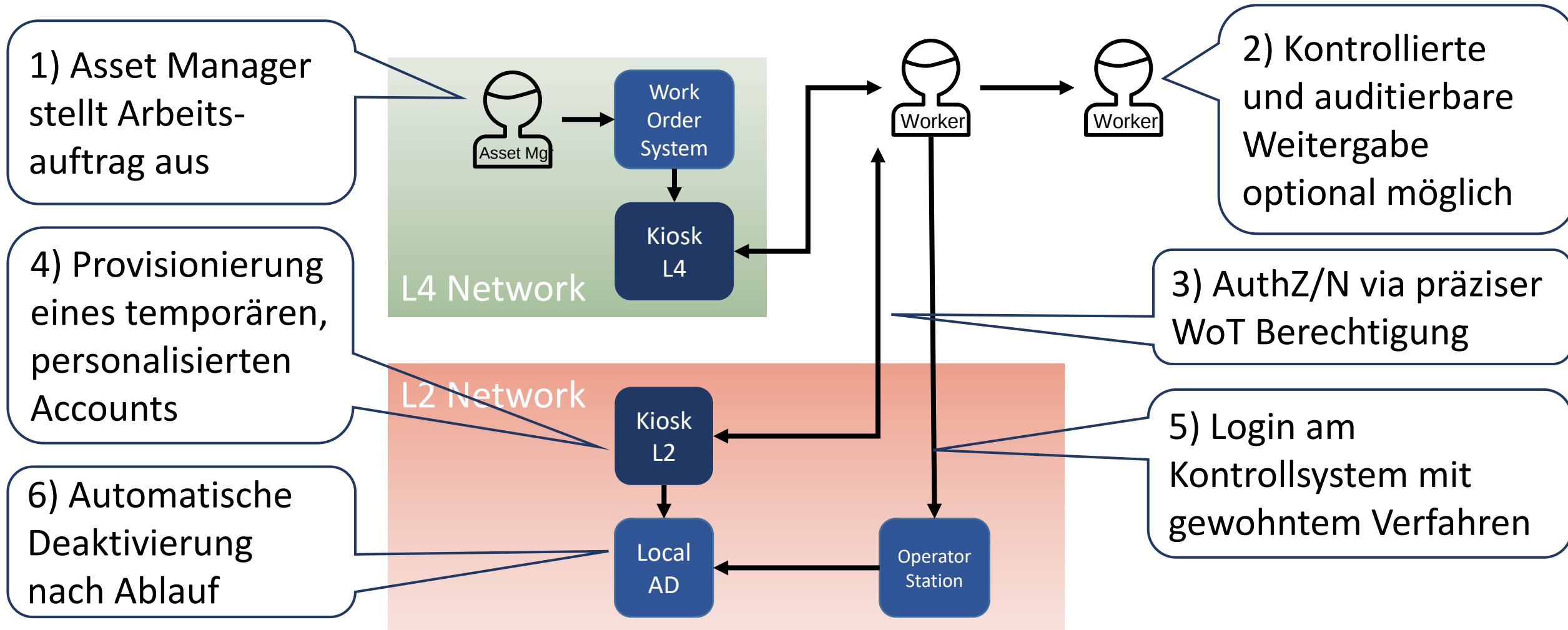
- Resilienz und Skalierbarkeit sind keine Stärken klassischer PKI

Praxisbeispiel BASF:

- 700 eigenverwaltete, abgetrennte Anlagen alleine in Ludwigshafen
 - Keine zentrale Verwaltung möglich
 - Zusammenführung unter einer PKI Hierarchie nicht praktikabel und entgegen Sicherheits- Regulatorikanforderungen
- Unzählige Systemzulieferer und externe Dienstleister
 - Zertifikatsbasierte AuthN/Z keine skalierbare Option
 - Personalisierte Accounts ebenfalls nicht umsetzbar

BASF Szenario für PKI + WoT

Personalisierte Berechtigungen für Mitarbeiter & Dienstleister



Quo vadis?

- Konzepte sind schön, Standards besser
 - NAMUR AG zur Autorisierung für Feldgeräte unter Federführung BASF
 - Mehrere Anwendungsfälle in Verwaltung, Verteidigung, KRITIS
 - Ziel: Nicht W3C/DIF replizieren
- Was wünschen sich Anwender?
- Wie in klassische PKI Modelle (technisch, kaufmännisch) integrieren?



Gregor Jehle

gregor@p3ki.com
+49 157 8688 2567

PGP: 0 x 2C59 96E1 DBD3 6223