

TeleTrust-EBCA "PKI-Workshop" 2026

Berlin, 08.10.2026

Sicherheit mit System: Automatisierte Zertifikatsprozesse für die Gebäudeautomation

Dr. Nina Bindel, MTG

Agenda

01 OT und Gebäudeautomatisierung

02 PKI in der Gebäudeautomatisierung

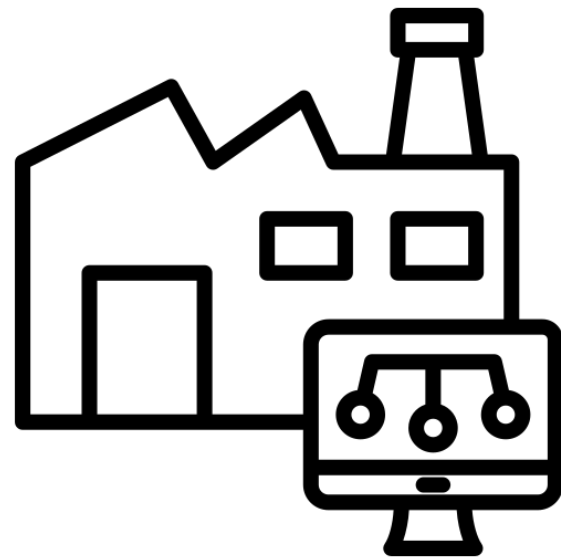
03 Vom Konzept zur Praxis

01

OT und Gebäudeautomatisierung

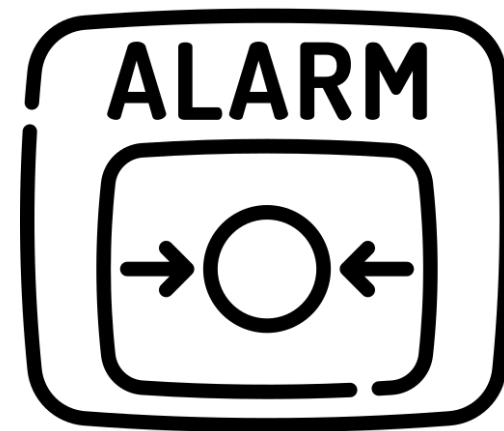
Operational Technology (OT)

- **OT** steuert und überwacht physische Prozesse, wie z.B. Ventile, Motoren, Temperaturregulation
- **IT** verarbeitet digitale Informationen, wie z.B. E-Mail, Zertifikate, Anmeldungen über Credentials



Industrielle Steuerungssysteme (Industrial Control Systems -- ICS)

Systeme zur Steuerung von Maschinen, Fertigungslinien oder verfahrenstechnischen Anlagen



Physische Sicherheitssysteme (Physical Access Control -- PAC)

Systeme, die die physische Integrität einer Anlage schützen.



Gebäudeautomatisierung (Building Automation Systems -- BAS)

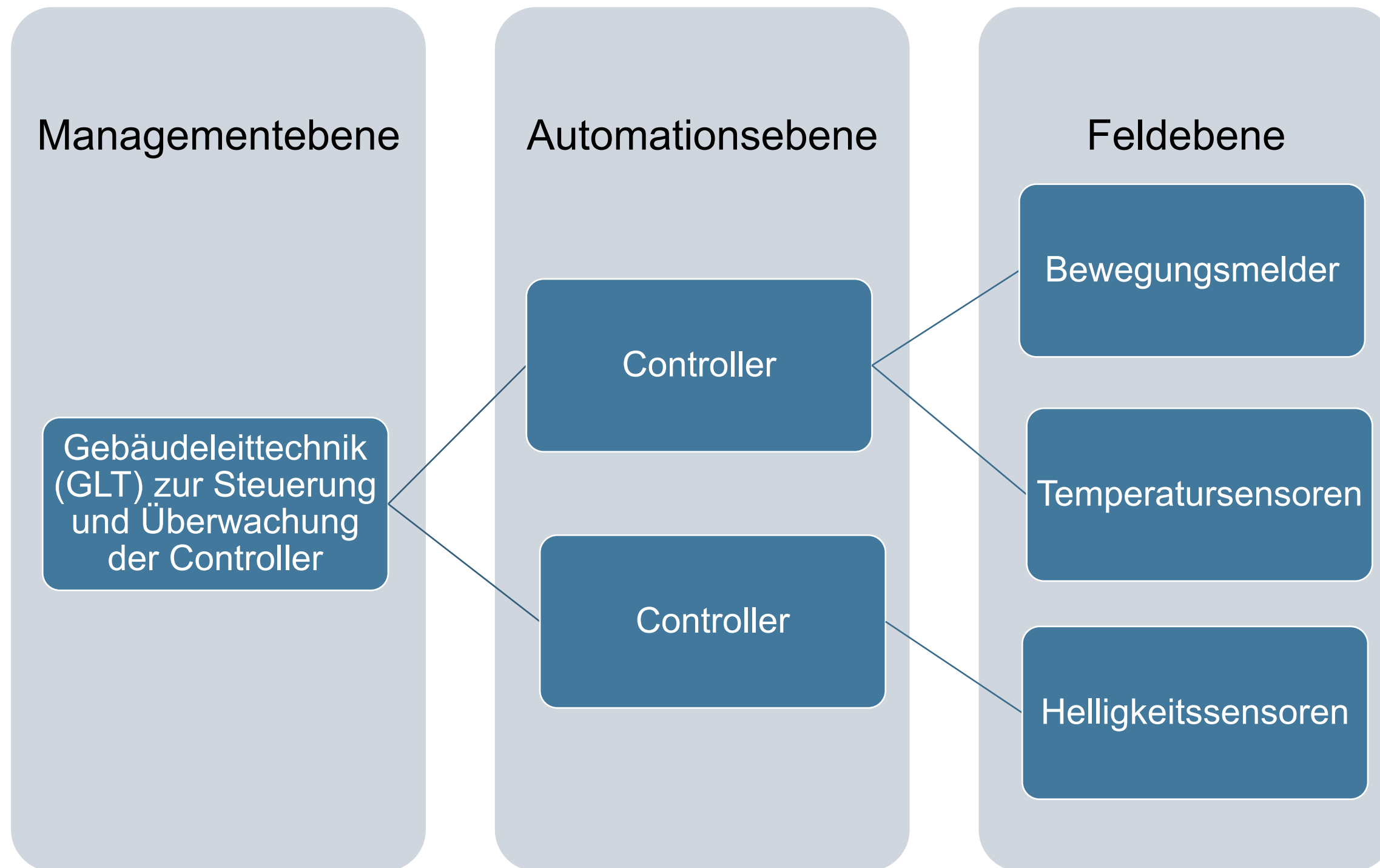
Systeme zur automatischen Steuerung, Regelung und Überwachung von technischen Gebäudeausrüstungen

IT oder OT ?

Kriterium	IT	OT, siehe z.B. IEC 62443
Priorität	1) Vertraulichkeit, Integrität, Authentizität 2) Verfügbarkeit	1) Verfügbarkeit, Safety 2) Vertraulichkeit, Integrität, Authentizität
Lebensdauer von Hardware	ca. 3–5 Jahre	10–25 Jahre häufig
Ausfalltoleranz	Minuten oft akzeptabel	Sekunden können kritisch sein, in GA allerdings Minuten akzeptabel
Change-Prozess	standardisiert, häufig	abhängig von Produktionsfenstern/Abnahmen
Protokolle	z.B. TCP/IP, HTTP(S), SQL	z.B. Modbus, Profinet, OPC UA, BACnet/SC

IT für OT!

Gebäudeautomatisierung



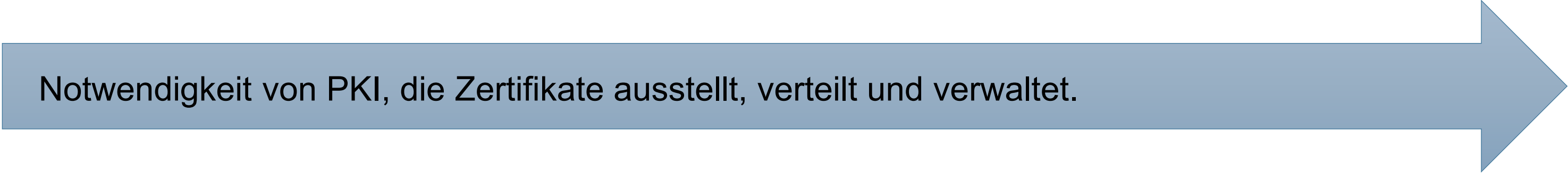
BACnet „Building Automation and Control Networks“ =
Standardisiertes,
herstellerunabhängiges
Datenübertragungsprotokoll
über all drei Ebenen

Regulatorik

Bisher: **Nachweis Funktionalität**

Durch „IT for OT“ verstärkt Cybersicherheit: **Nachweis der Integrität der gesamten Anlage**

- Verschärfung gesetzlichen Rahmenbedingungen:
 - Betreiber kritischer Infrastrukturen und Zulieferer für kritische Sektoren:
 - europäische **NIS2**-Richtlinie
 - **KRITIS**-Dachgesetz
 - Hersteller:
 - Cyber Resilience Act (**CRA**)

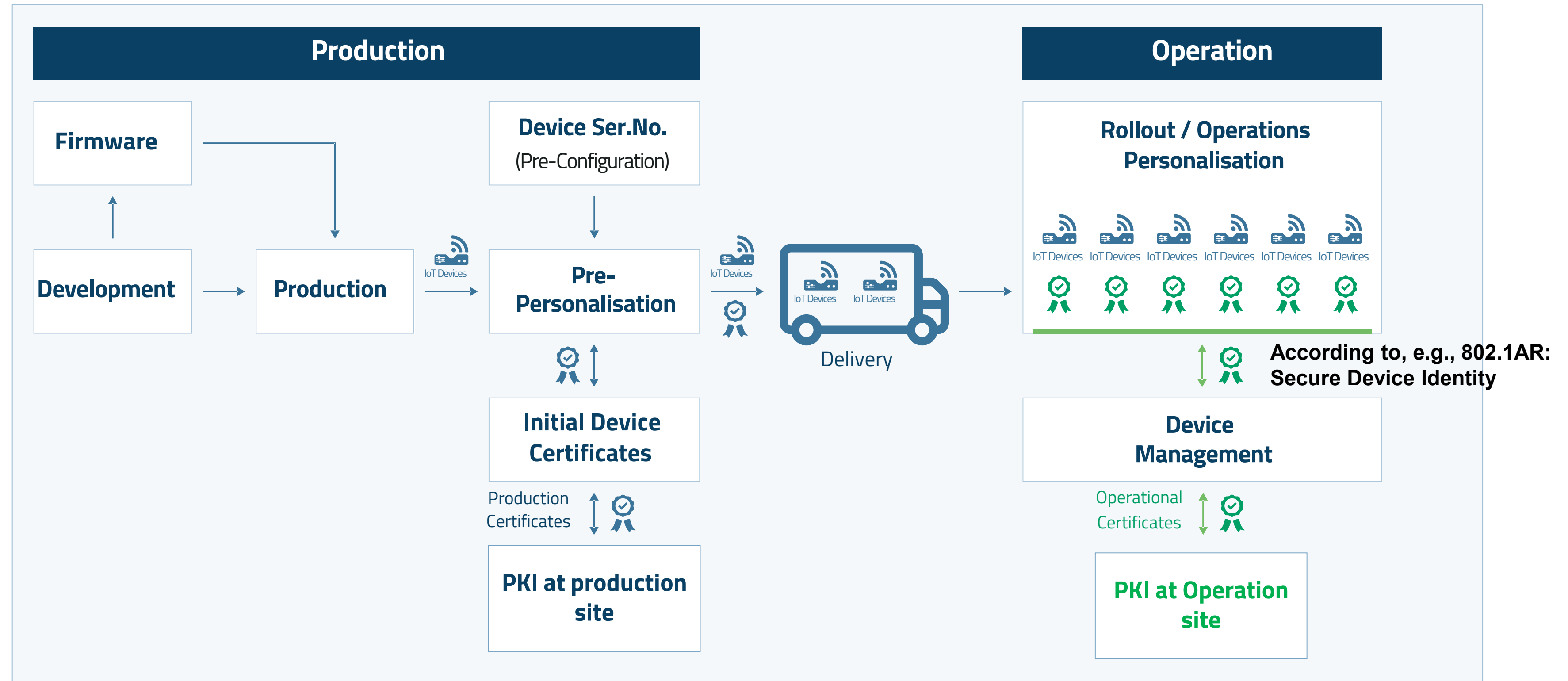


Notwendigkeit von PKI, die Zertifikate ausstellt, verteilt und verwaltet.

02

PKI in der Gebäudeautomatisierung

Austausch Herstellerzertifikate



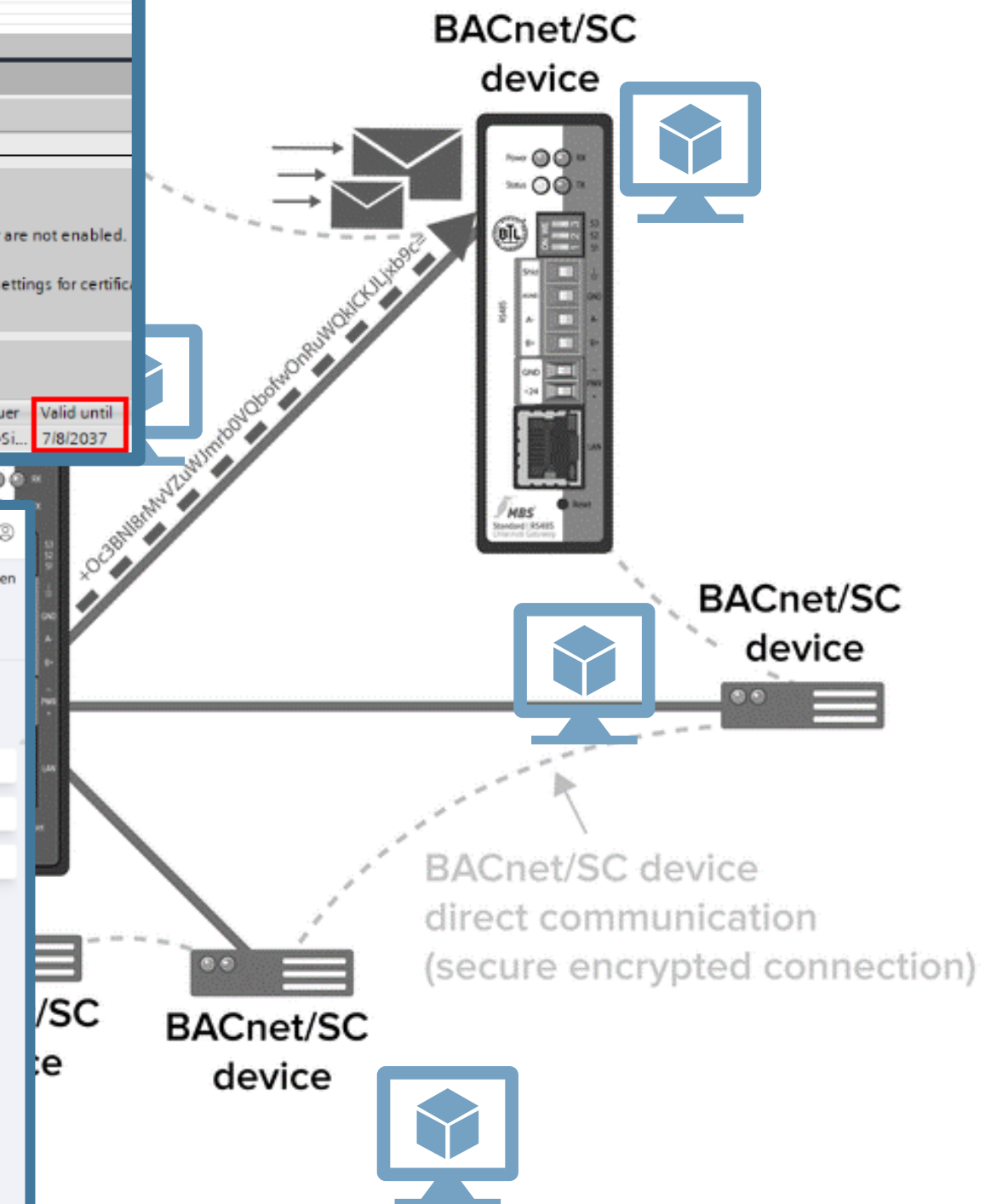
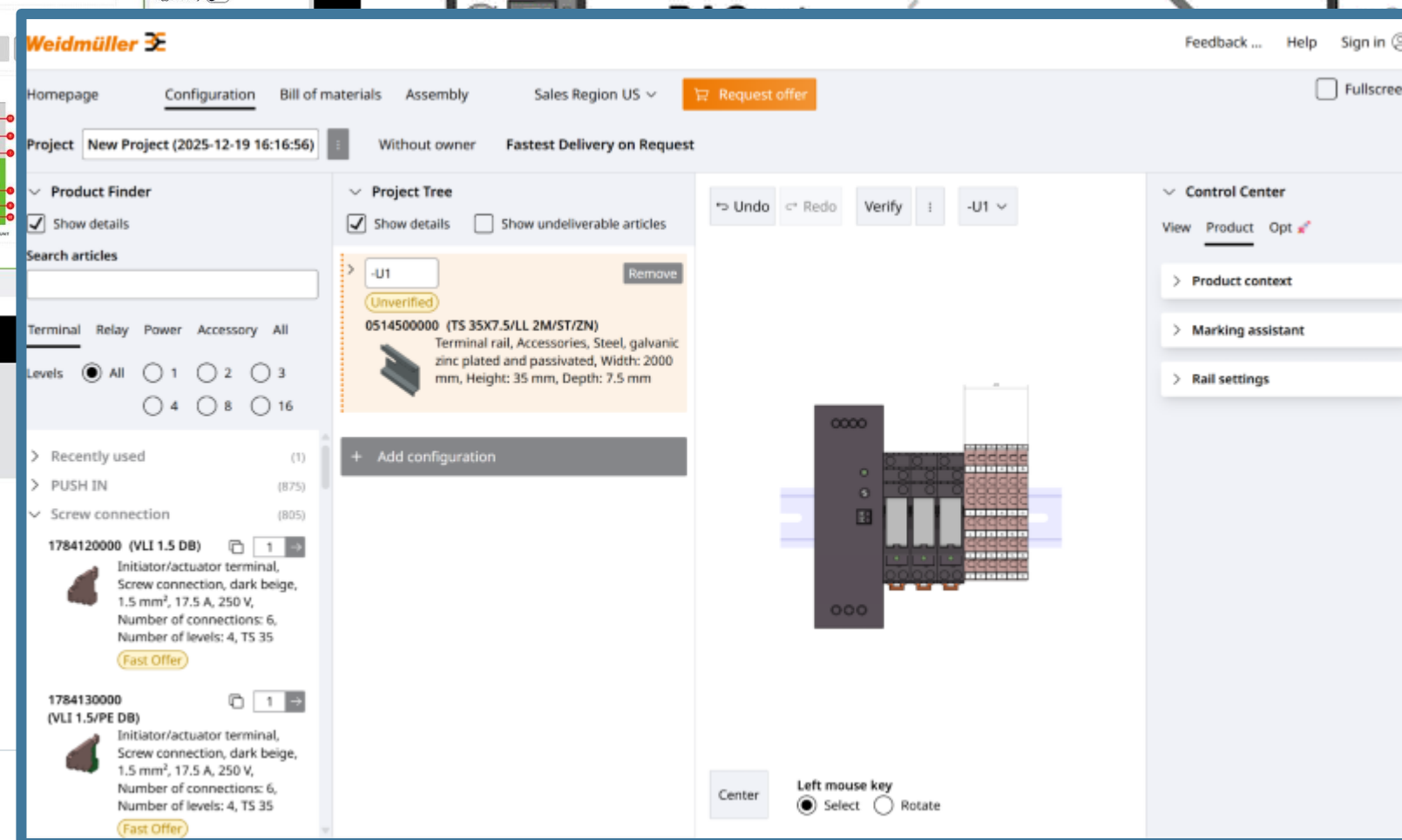
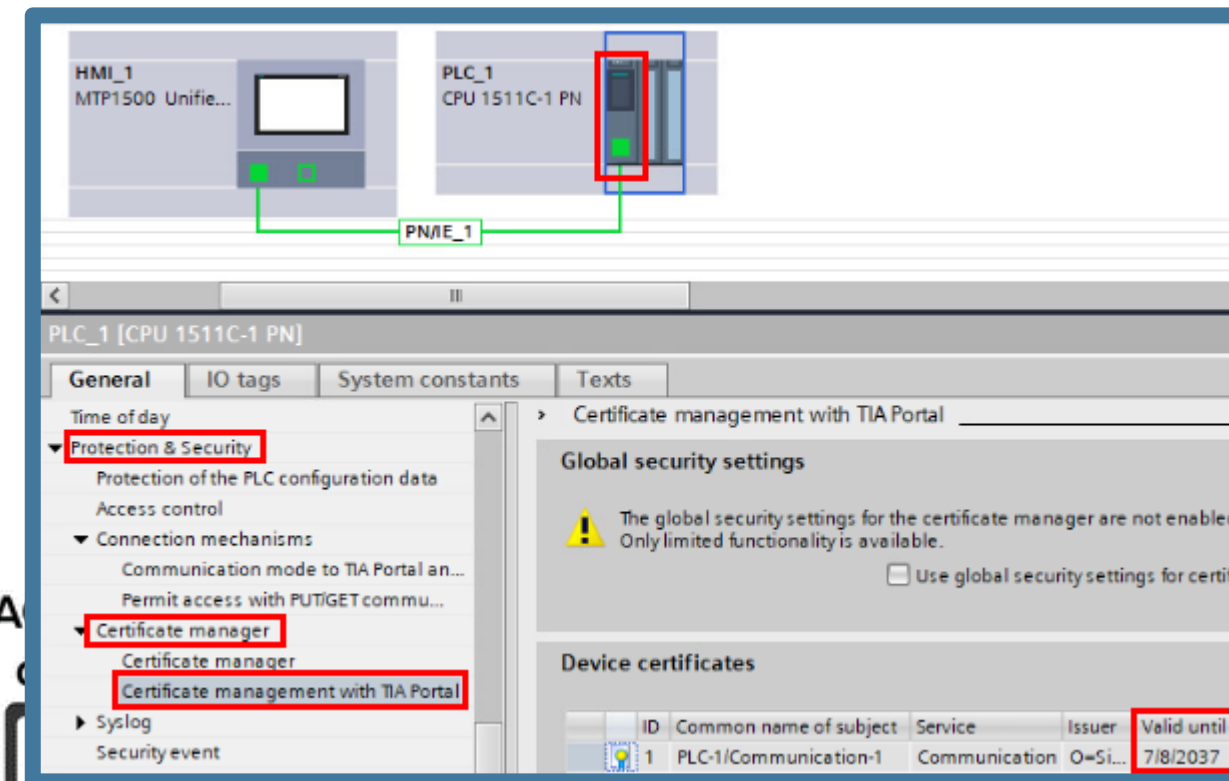
2. PKI Use-Case

Geräte-Management über GUIs

- TLS-Zertifikate für jedes Feldgerät, Switch, Controller, etc.



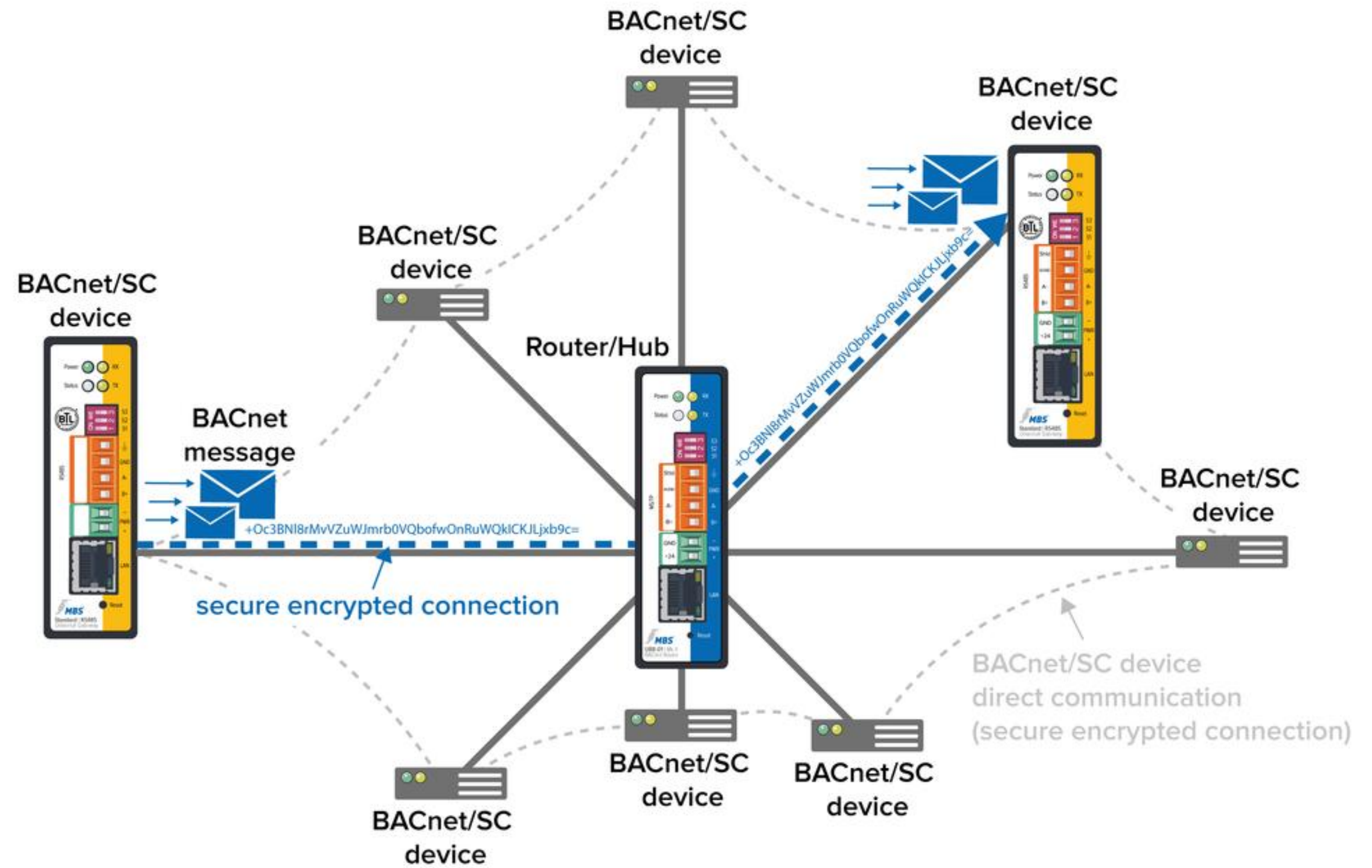
MTG



3. PKI Use-Case

BacNect/SC (Secure Connect)

- TLS (1.3) -basiertes Protokoll über TCP/IP
- Devices können Client oder Server sein
- **Regelmäßige Zertifikatserneuerung** nötig, ca. alle 1-2 Jahre.

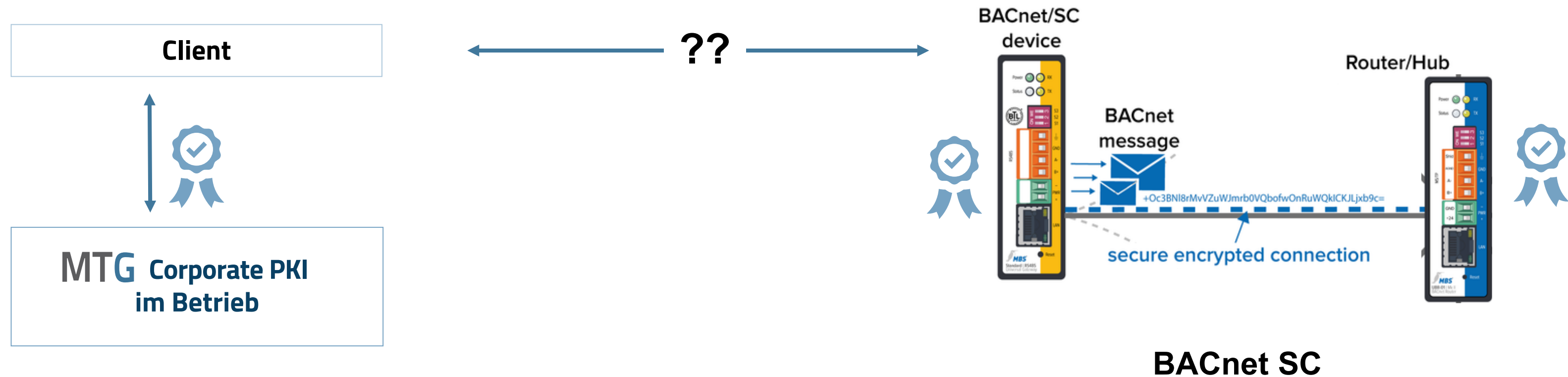


<https://www.mbs-solutions.de/bacnetsc>

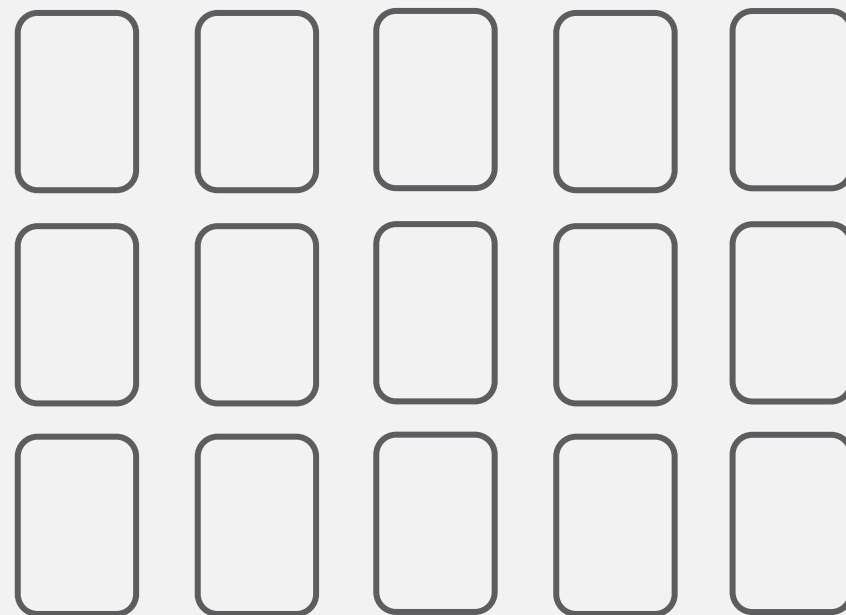
Standardisierungslücke

PKI für Zertifizierungs- und Registrierungsstellen sind in BACnet/SC nicht definiert.

© FCIT/UNIVERSITY OF SOUTH FLORIDA



Mittlere Liegenschaft



100 Geräte

Aufwand manueller Zertifikatswechsel mit kürzeren Laufzeiten

2026

- ✓ 100 Geräte
- ✓ 1 Wechsel alle 2 Jahre
- ✓ 15 Minuten pro Gerät
- ✓ ca. > 650 Minuten
- ✓ **ca. > 10 Stunden**

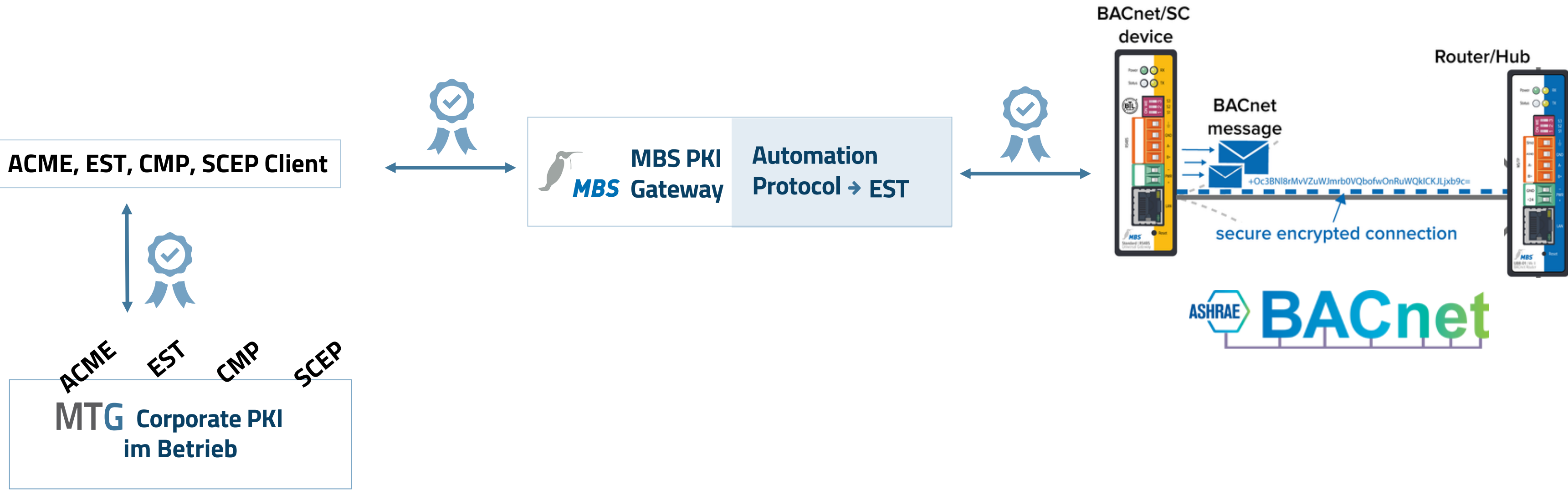
2027

- ✓ 100 Geräte
- ✓ 1 Wechsel pro Jahr
- ✓ 15 Minuten pro Gerät
- ✓ ca. > 1.500 Minuten
- ✓ **ca. > 25 Stunden**

2028

- ✓ 100 Geräte
- ✓ 2 Wechsel pro Jahr
- ✓ 15 Minuten pro Gerät
- ✓ ca. > 3.000 Minuten
- ✓ **ca. > 50 Stunden**

IT für OT



PKI Automatisierungsprotokolle

03

Vom Konzept zur Praxis

Proof of Concept der M&P Gruppe

- Demonstrator um Feldgeräte, Automatisierung und Management sicher zu testen
- Integration von MBS PKI Gateway
- Getestet mit MTG PKI mit Nitrokey HSM
 - Automatisiert für Bacnet/SC Zertifikate
 - TLS Server Zertifikate für GUIs



Learnings aus PoC

- **Kommunikation ist schwierig!**
Gemeinsame Sprache und Verständnis zwischen restriktiven Anforderungen der OT in der Gebäudeautomatisierung und „hohen Sicherheitsbedürfnis“ der IT
- **Kommunikation ist schwierig!**
Trennung in verschiedene Schutzzonen und strikte Trennung von IT und OT Bereichen hat die erste Installation und Kommunikation zwischen den Komponenten herausfordernd gestaltet.
- **Die Lösung ist technisch naheliegend.**

Erweiterungsmöglichkeiten

- **Erweiterung auf komplexere und mächtigere Protokolle**
- **Lösung für bestehende Legacy-Systeme**
 - **Ohne eigene Schlüsselgeneration**
 - **Nur mit BACnet-fähigkeit**
- **Automatisierung der anderen PKI Use-cases**

Danke!

