

# Wenn Hacker Kirchenglocken läuten lassen

## **Sichere Identitäten im IoT**

Simon Ulmer  
Global VP Digital Identity  
21/01/2025

**EVIDEN**





**Simon Ulmer**  
Head of Digital ID  
Cybersecurity Products

## **Eviden Digital Identity**

Sichere elektronische  
IDentitäten und  
benutzerfreundliche  
Kryptografie

*Home of cryptovision  
and IDnomic*



IoT-Sicherheit 2015

# Sicherheitslücke im Kühlschrank

verrät



\*\*\*\*\*

# Gmail-Zugangsdaten

Smart Refrigerator mit Schwächen



Spektakulärer Hack 2018

**Spielcasino gehackt:**  
**Angreifer nutzen IoT-**  
**Sicherheitslücke im**  
**Aquarium**

Zahlreiche Kundendaten erbeutet





IoT-Skandal in den USA (2021)

**Hacker zapfen**

**150.000**

**Überwachungskameras an**

Krankenhäuser, Gefängnisse, Schulen und Polizeireviere betroffen





IoT-Panne im Jahr 2022

# Hacker ließ Glocken des Stephansdoms läuten



Unsichere Internetverbindung zwischen Kathedrale und  
Glockenfirma als Einfallstor



# Jede Komponente im Internet of Things (IoT) ist eine potenzielle Gefahrenquelle

IoT-Sicherheit 2015

**Sicherheitslücke im Kühlschrank verrät Gmail-Zugangsdaten**



Smart Refrigerator mit Schwächen

Spektakulärer Hack 2018

**Spielcasino gehackt: Angreifer nutzen IoT-Sicherheitslücke im Aquarium**



Zahlreiche Kundendaten erbeutet

IoT-Skandal in den USA (2021)

**Hacker zapfen 150.000 Überwachungskameras an**



Krankenhäuser, Gefängnisse, Schulen und Polizeireviere betroffen

IoT-Panne im Jahr 2022

**Hacker ließ Glocken des Stephansdoms läuten**



Unsichere Internetverbindung zwischen Kathedrale und Glockenfirma als Einfallstor

## Das Thema ist nicht neu



# OT-Angriffe in Zahlen

**+9900%**

Zunahme der OT-Angriffe zwischen 2022 and 2027

**15,000**

Betriebsstillstände verursacht von OT-Angriffen 2027

**74%**

Anzahl der OT-Angriffe mit kommerziellem Hintergrund



# Gesetzgeber hat reagiert

## IEC 62443

Sicherheit für  
industrielle  
Netze



## NIS2

Stärkung der  
Cyberresilienz



## Cyber Resilience Act (CRA)

Cybersicherheit  
von Produkten  
mit digitalen  
Elementen



## KRITIS-Gesetz

Schutz für  
kritische  
Infrastrukturen





# Beispiel: Grand Paris Express





# Grand Paris Express

Geplantes U-  
Bahn-Netz  
im Raum Paris

Erster Teil bis zu den Olympischen  
Spielen 2024 fertiggestellt



# Grand Paris Express

Überwachungs-  
kamera

Belüftungsgerät

Fahrkarten-  
Automat

Notruf-  
Telefon

Fahrstuhl

U-Bahn-Stationen sind  
mit Internet of Things  
ausgestattet

Jede IoT-Komponente  
ist potenzielle  
Gefahrenquelle



## Lösung: Jede IoT-Komponente erhält eigene Identität

### Jede Identität ...

- erhält Schlüsselpaar, digitales Zertifikat, Rechte (Device Onboarding / Provisioning)
- kann sich authentisieren, verschlüsseln, signieren
- erhält bei Bedarf geänderte Schlüssel, Zertifikat, Rechte
- wird überwacht
- kann terminiert werden

Zero Touch Onboarding

Zero Trust Security



# ZTO - ZTS



**Zero Touch  
Onboarding**

**Zero Trust  
Security**



## Lösung: Jede IoT-Komponente erhält eigene Identität

### Jede Identität ...

- erhält Schlüsselpaar, digitales Zertifikat, Rechte (Device Onboarding / Provisioning)
- kann sich authentisieren, verschlüsseln, signieren
- erhält bei Bedarf geänderte Schlüssel, Zertifikat, Rechte
- wird überwacht
- kann terminiert werden

Identity  
Management



# Device Onboarding heute

EVIDEN

Hersteller



Auslieferung 

Betreiber

## Onboarding

- Manuelle Prüfung der Lieferung
- Lokale Registrierung
- Eintrag in Management-Tool
- Manuelles Profilieren

**Prozess ist unsicher, aufwändig, fehleranfällig, keine Supply-Chain-Sicherheit**



The background is a vibrant orange-toned illustration. It features a central semi-circular window showing a city skyline with a prominent tower. Surrounding this are various digital and network-related icons: server racks, laptops, tablets, a cloud with a gear, a globe, and various circular symbols representing different types of data or devices. The overall aesthetic is futuristic and tech-oriented.

**Device Identity  
Management ist  
notwendig**



# Grand Paris Express

Überwachungs-  
kamera

Belüftungsgerät

Jedes Gerät erhält Identität,  
Schlüsselpaar und digitales  
Zertifikat

Notruf-  
Telefon

PKI notwendig

Fahrkarten-  
Automat

Onboarding-Prozess notwendig



# Zero Touch Onboarding

Prozess, der Komponenten sicher und einfach im Netz registriert

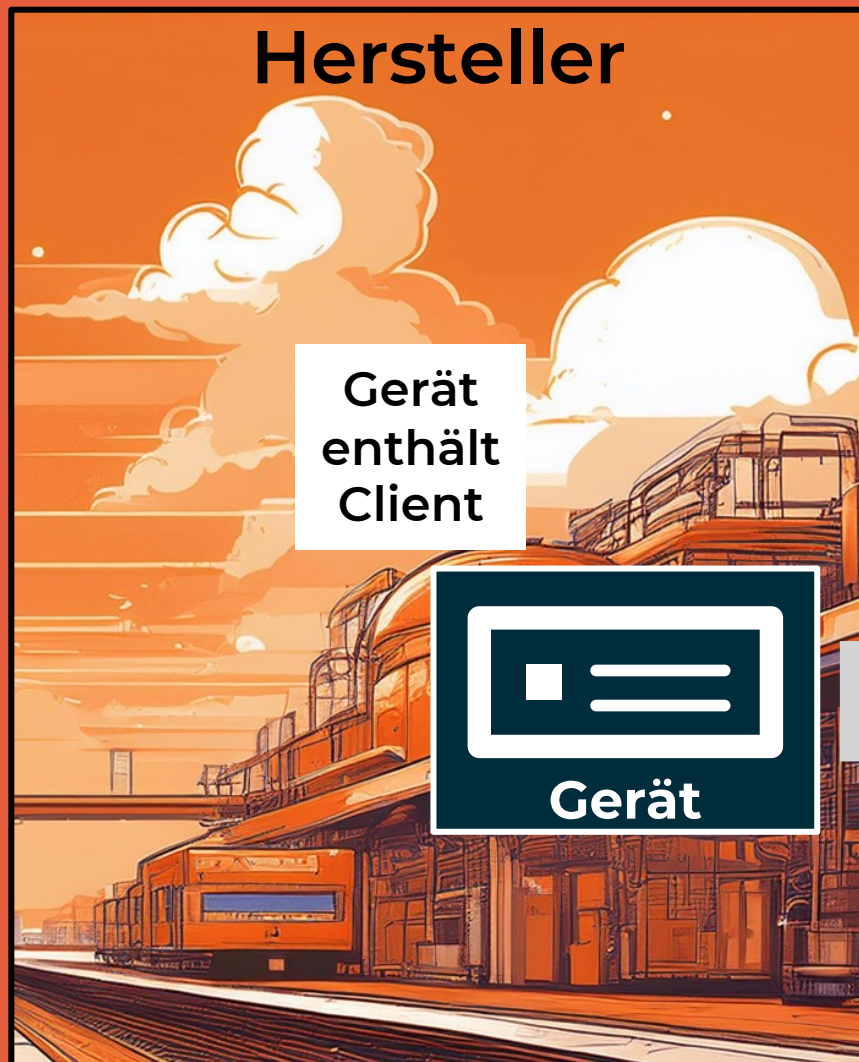
PKI-basiert

Hersteller wird einbezogen  
(Supply Chain Security)

ZTO Client notwendig



# ZTO Client und TTP





# Standards



## **SZCP (RFC 8572)**

Secure Zero Touch Provisioning



## **FIDO Device Onboard (FDO)**

Automatic onboarding protocol



## **EST (RFC 7030)**

Enrollment over Secure Transport



## **802.1x**

Network authentication

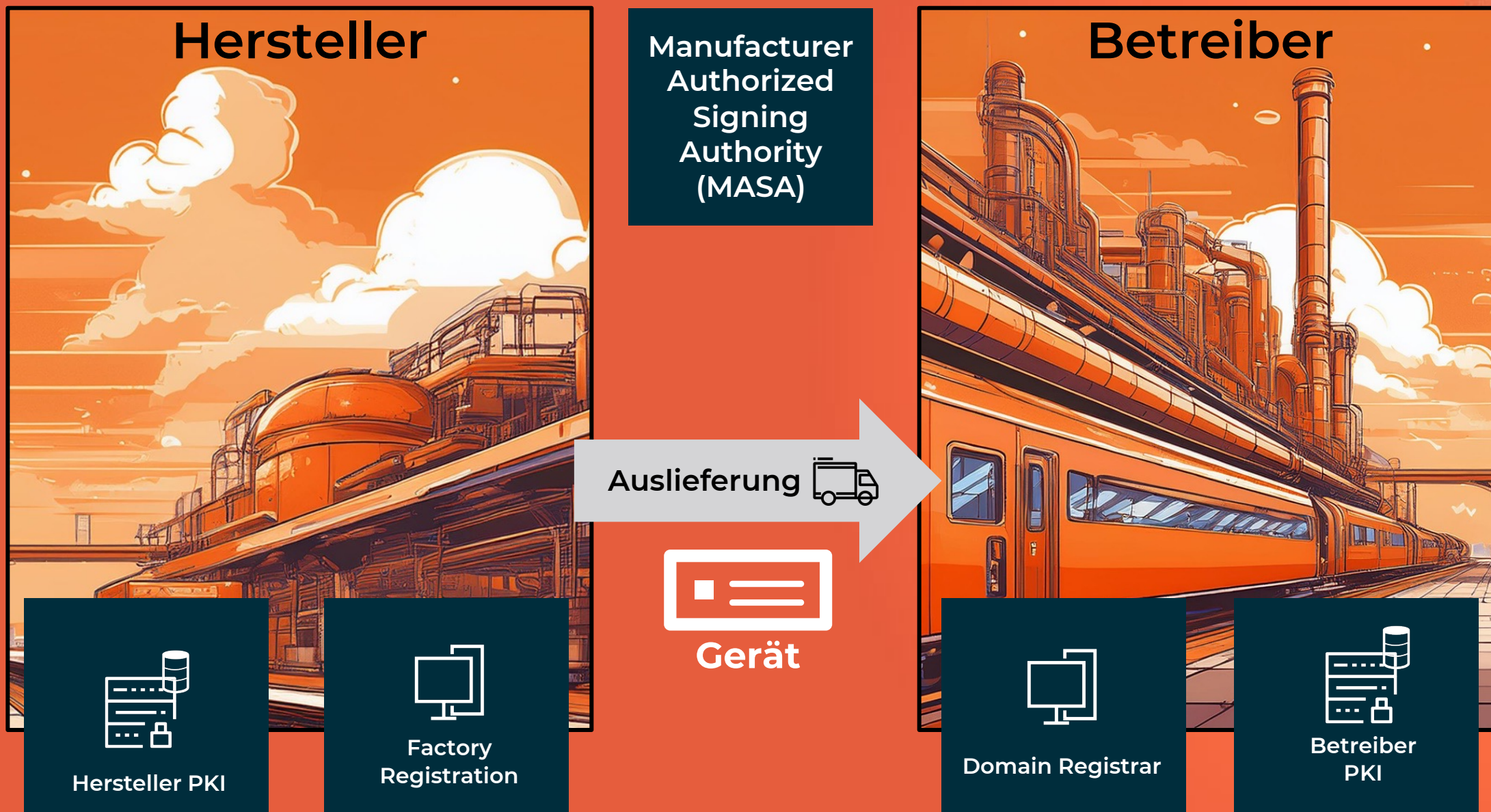


## **BRSKI (RFC 8995)**

Bootstrapping Remote Secure Key Infrastructure



# Weitere Komponenten








## OHNE ZTO

## MIT ZTO




## HERSTELLER

 Gerät ohne Identität

-  ZTO-Client-Installation
-  Registrierung bei Trusted Third Party

Lieferung

## BETREIBER

-  Manuelle lokale Registrierung
-  Manuelle Konfiguration
-  Manuelles Enrolment und Renewal (alle zwei Jahre)

-  Vollständiges, automatisiertes Certificate Lifecycle Management
-  Nachvollziehbarkeit vom Hersteller bis zum Nutzer



# Betrieb mit ZTO

Jede Komponente kann sich  
authentifizieren, verschlüsseln,  
signieren und  
Authentifizierungen vornehmen



# Grand Paris Express

A stylized illustration of a high-speed train in Paris. The train is sleek and aerodynamic, moving from left to right on a track. In the background, the Eiffel Tower is visible on the left, and a large, arched bridge spans the tracks. The sky is a warm orange color with white clouds and streaks of light, suggesting a sunset or sunrise. The overall style is graphic and modern.

IoT-PKI mit über  
100.000 Zertifikaten



# Grand Paris Express

An illustration of a modern high-speed train in motion, set against a Parisian cityscape. The Eiffel Tower is visible on the left, and a large bridge with multiple arches spans the background. The scene is rendered in a stylized, sketch-like manner with a warm, orange-toned sky and motion blur lines suggesting speed.

Kunde fordert, dass Komponenten ZTO-  
Protokolle unterstützen

Hersteller müssen zeitnah nachrüsten

Gesamte Supply Chain muss sich anpassen



# Eviden-Offering

**Consulting**

**Eviden ZTO**

ZTO Client

MASA

Domain Registrar

**IDnomic PKI**

**Implementierung**



# Fazit

**IoT, OT können angegriffen werden**

**Identity Management für  
Komponenten als Gegenmaßnahme**

**ZTO ist unverzichtbar**



IoT-Panne im Jahr 2022

# Hacker ließ Glocken des Stephansdoms läuten



Unsichere Internetverbindung zwischen Kathedrale und  
Glockenfirma als Einfallstor

## Lässt sich mit ZTO verhindern



# Noch Fragen?

**Gerätehersteller,  
Systemintegratoren:**  
Kontaktieren Sie uns, wir stellen  
gerne eine Demo zur Verfügung

## Kontakt

Kay Prisille

[kay.prisille@eviden.com](mailto:kay.prisille@eviden.com)



# Whitepaper



[www.cryptovision.com/en/download-access](http://www.cryptovision.com/en/download-access)



Vielen Dank für Ihre  
Aufmerksamkeit!

EVIDEN