

# TeleTrust-EBCA "PKI-Workshop" 2019

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Berlin, 18.06.2019

## Die besonderen Herausforderungen an PKI-Lösungen im IoT-Umfeld

Björn Jansen, secunet Security Networks AG

**secunet**

# Was genau bedeutet PKI?

**Sicherheitsgerüst für den Identitätsnachweis  
in der digitalen Welt**

**Digitale Zertifikate werden eingesetzt, um**

- Nutzer und technische Komponenten online zu authentisieren
- Elektronische Daten und Nachrichten zu signieren und zu verschlüsseln
- Beim Online-Banking oder -Shopping für Vertraulichkeit und Integrität bei der Datenübertragung zu sorgen.



# PKI – ein alter Hut?

Vom Gefühl her sicherlich schon so alt...



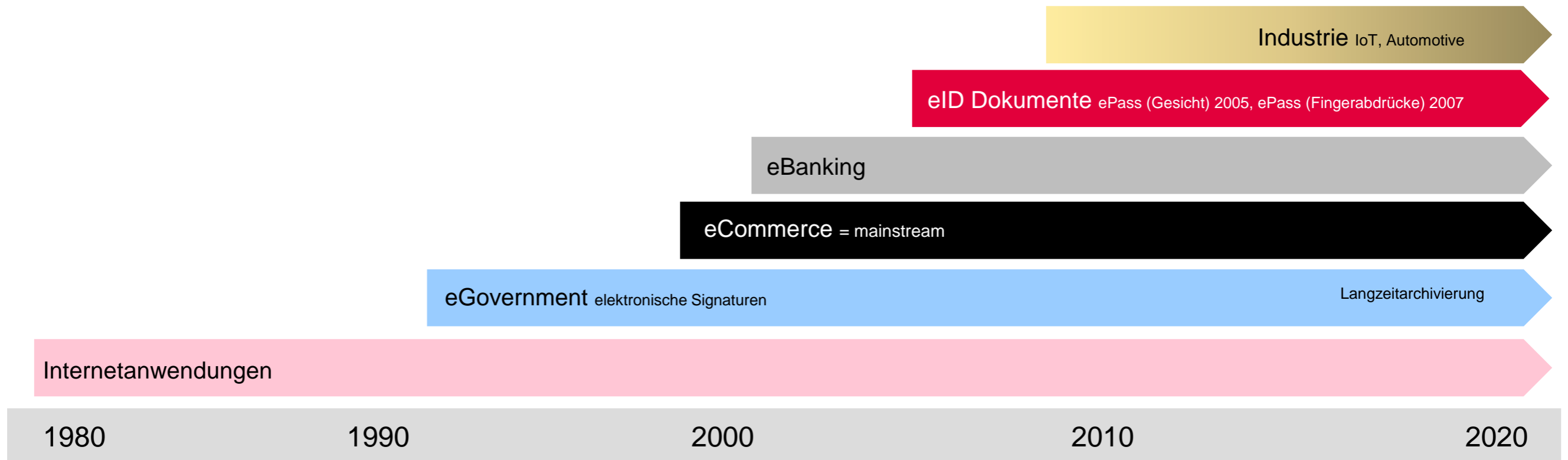
[https://de.wikipedia.org/wiki/Humphrey\\_Bogart](https://de.wikipedia.org/wiki/Humphrey_Bogart)

... tatsächlich aber ein Thema aus dieser Zeit.



<https://www.cambridgelivetrust.co.uk/tickets/events/enchanted-cinema-presents-blues-brothers-15>

# Meilensteine in der „PKI-Evolution“



# Wo stehen wir heute?

## Die klassischen Einsatzgebiete:

- Qualifizierte Elektronische Signaturen
  - >> Trust Center stellen den Betrieb ein
- S/MIME
  - >> Aufwändig und ungeliebt (technische Rückschläge)
- Zwei-Faktor-Authentisierung
  - >> Notgedrungen akzeptiert
  - >> Smartcards oder Token (kontinuierlich im PC)
- HTTPS
  - >> Erfolgsgeschichte (mit Rückschlägen)
- VPN
  - >> Erfolgreich (wo vom Nutzer unbemerkt)



**PKI in rein technischen Prozessen hat sich bewährt.**

- Authentisierte Kommunikation wird immer wichtiger
- Angriffe auf technische Systeme mehren sich

# Wohin entwickelt sich der Markt?

## Was sind die neuen Einsatzgebiete?

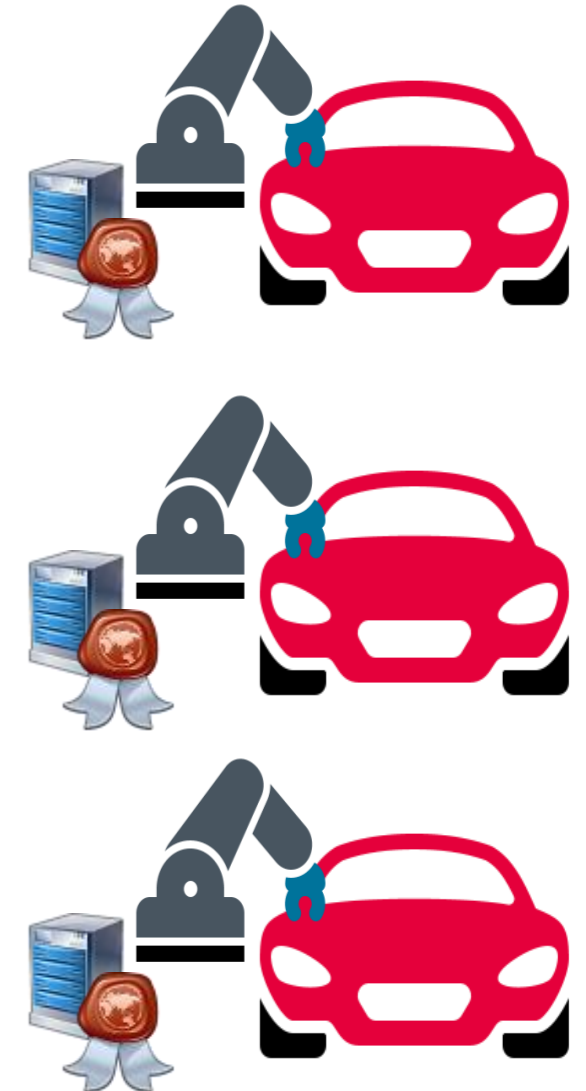
- Updateprozesse
- Einspielen von Konfigurationen
- (Fern-)Wartungszugriffe
- Absicherung von Mehrwertdiensten
  - >> Wetterdaten, Kartenupdates ... im Fahrzeug
  - >> Rezepte und mehr für andere Geräte
- Konformität zwischen Schnittstellen
- Risikoschutz



# Herausforderung Ökosystem

## CA Betriebsumgebung

- Lokal, verteilt jeweils an den Provisionierungspunkten

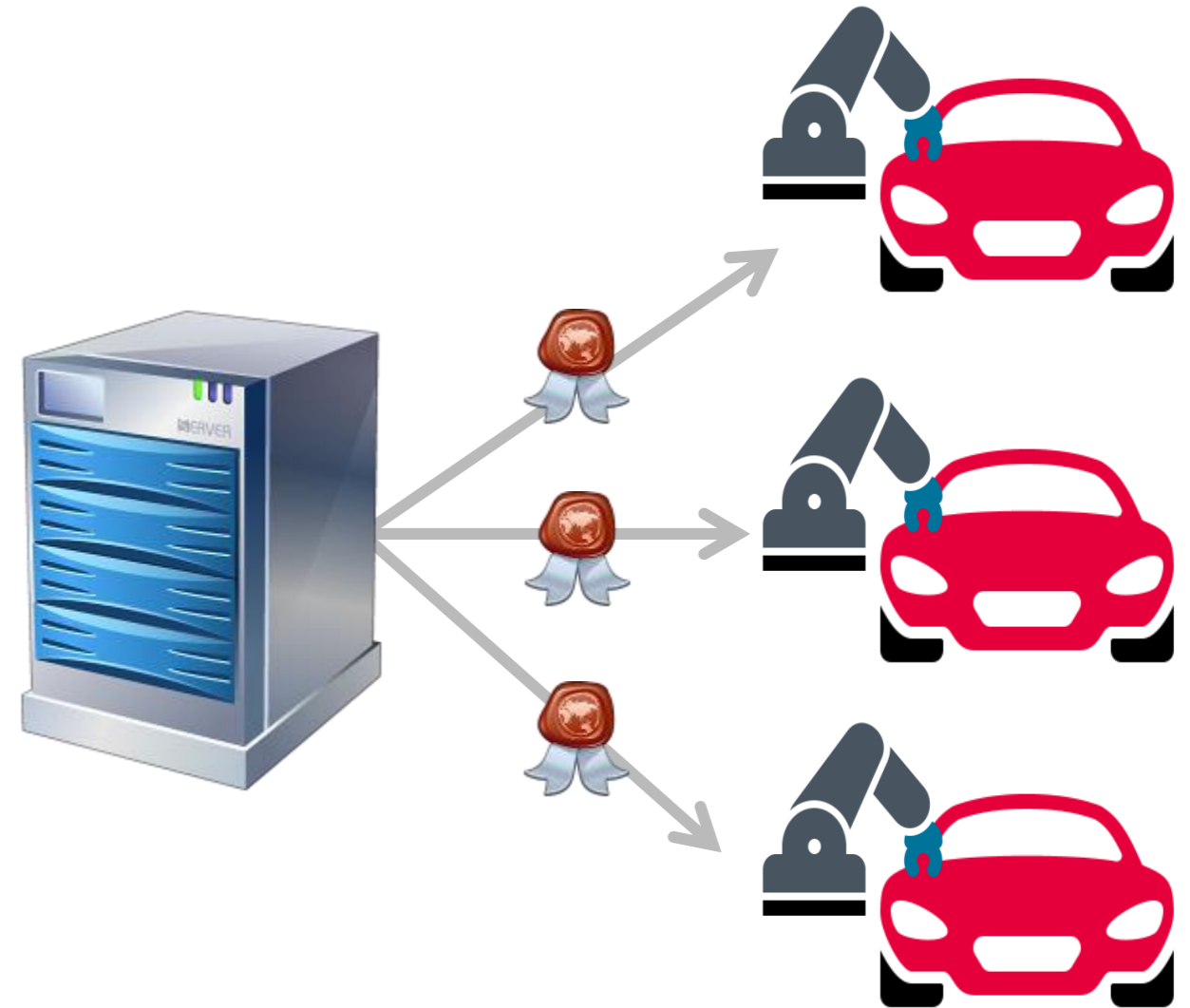




# Herausforderung Ökosystem

## CA Betriebsumgebung

- Lokal, verteilt jeweils an den Provisionierungspunkten
- Remote / als Service (intern/extern)

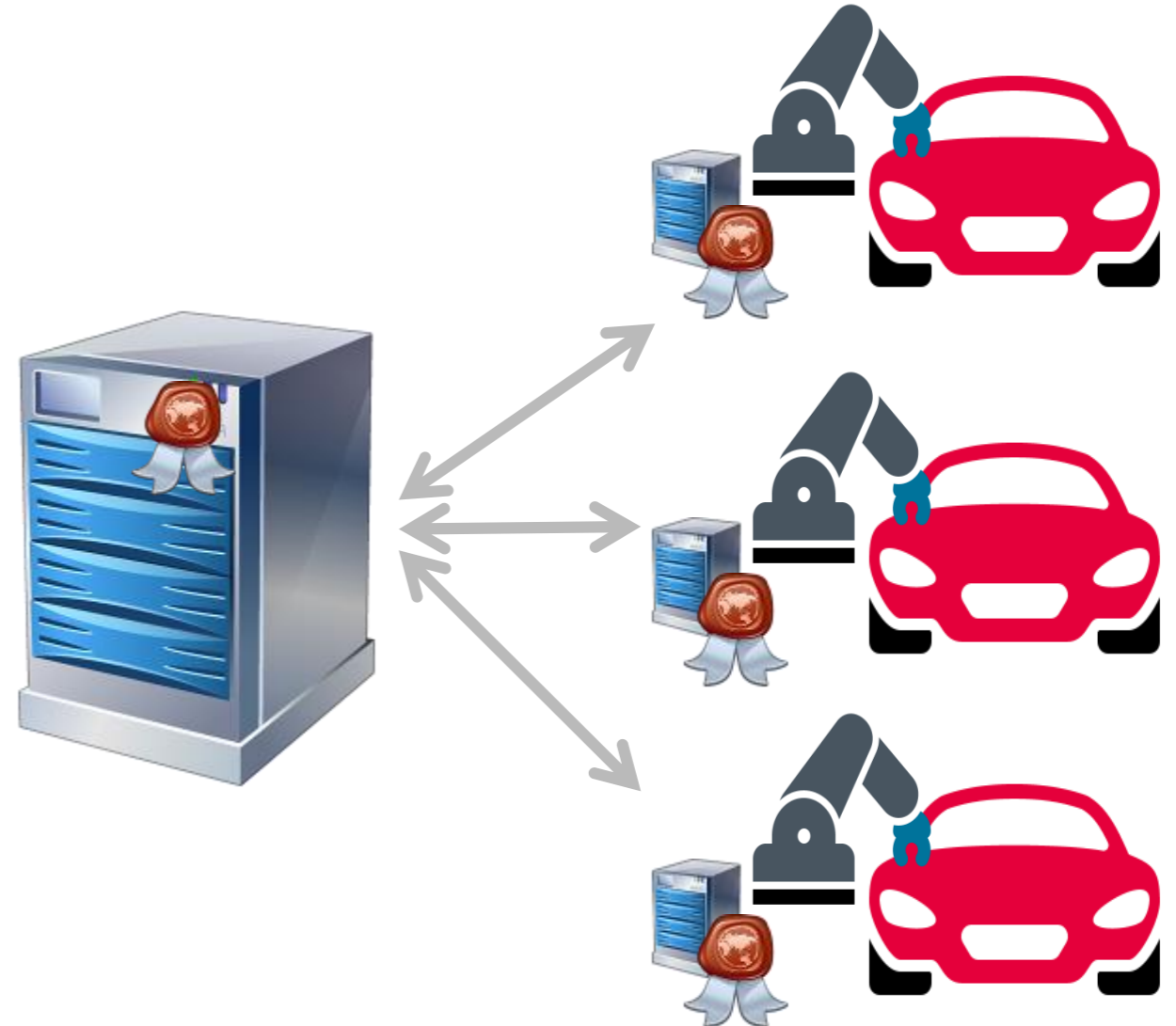




# Herausforderung Ökosystem

## CA Betriebsumgebung

- Lokal, verteilt jeweils an den Provisionierungspunkten
- Remote / als Service (intern/extern)
- Hybrid (nicht zu 100% online, aber sync notwendig)



# Herausforderung Ökosystem(zeit)



Geregelte Umgebung (Netze mit Zeitquelle)

- Client/Server
- Telecom (mobile)



Ungeregelte Umgebung (IoT)

- Vernetzt / autonom
- Systemstart bei  $T=0$

# Gemeinsame Herausforderung - Workshop

## Besonderheiten in Bezug auf IoT

Beispielpunkte:

- Beantragungswege
- Zertifikatsträger
- Zertifikatstypen
- Anwendungsszenarien
- Zeit(kritikalität)
- Konzepte (Laufzeiten, Betrieb, ...)

## Gemeinsamkeiten (klassische PKI und IoT PKI)

Beispielpunkte:

- Robustheit?
- Interaktionsfreiheit?
- Skalierbarkeit?
- Flexibilität (Schnittstellen, Prozesse, ...)?
- Globale Verfügbarkeit?
- Zukunftssicherheit?



**Kosten**

# PKI – der Schlüssel für die Zukunft

## The Internet of Things a very short story

The Internet of Things is the network of physical devices, vehicles, buildings and so on embedded with electronics, software, sensors and network connectivity that enable these objects to collect and transmit data via the Internet.

This year, 2016, we will have **4.9 billion** connected things, so get ready, the Internet of Things is here to stay

Companies like **Google** and **Samsung** are investing in home devices and having a connected kitchen could save the food and beverage industry as much as **15%** annually

The global wearable device market has grown **223% in 2015**

ATMs were some of the **first** Internet of Things objects as far back as **1974**

The "Internet of Things" is a phrase that **87%** of people haven't heard of

Back in **2008**, there were already more objects connected to the Internet than people

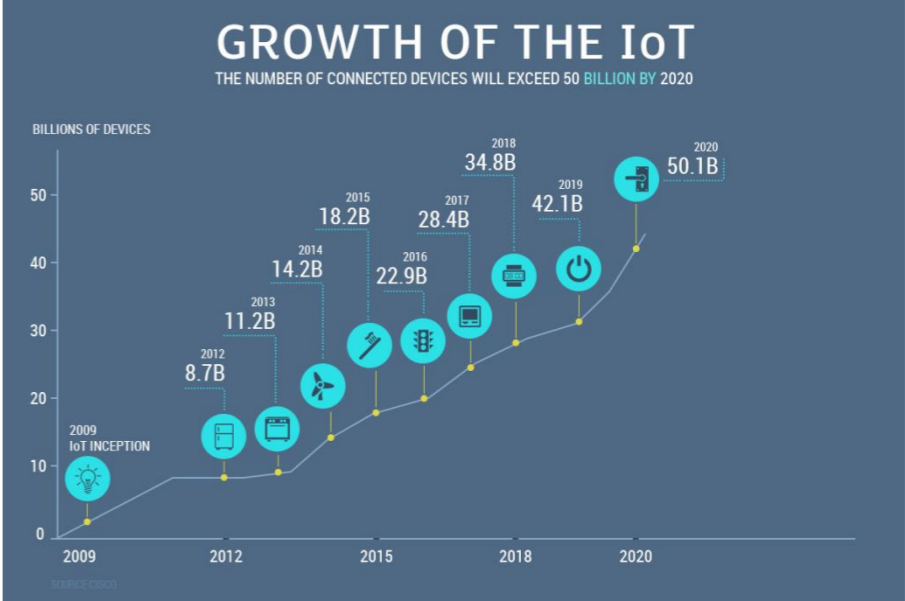
According to some estimates, the Internet of Things will add **USD 10-15 trillion** to global GDP in the next **20 years**

**By 2020, 250K** vehicles will be connected to the Internet

Google's self-driving cars average about **10 000 autonomous miles** per week

Based on "12 Internet of Things Facts Everyone Should Read" by Bernard Marr

Quelle: <https://www.iso.org/news/2016/09/Ref2112.html> , ISO/TC 204



Quelle: <https://www.theuy.nl/portfolio/internet-of-things/iotb/>

The logo for secunet, featuring the word "secunet" in a bold, sans-serif font. The letters "secunet" are black, and the letter "n" is red. The logo is positioned in the upper right corner of the slide.

**secunet**

**Björn Jansen**

Vertrieb

Division Kritische Infrastrukturen

**secunet Security Networks AG**

Kurfürstenstraße 58

45138 Essen

Telefon +49 201 5454-3869

[bjoern.jansen@secunet.com](mailto:bjoern.jansen@secunet.com)