TeleTrusT-EBCA "PKI-Workshop" 2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Berlin, 18.06.2019

Die besonderen Herausforderungen an PKI-Lösungen im IoT-Umfeld

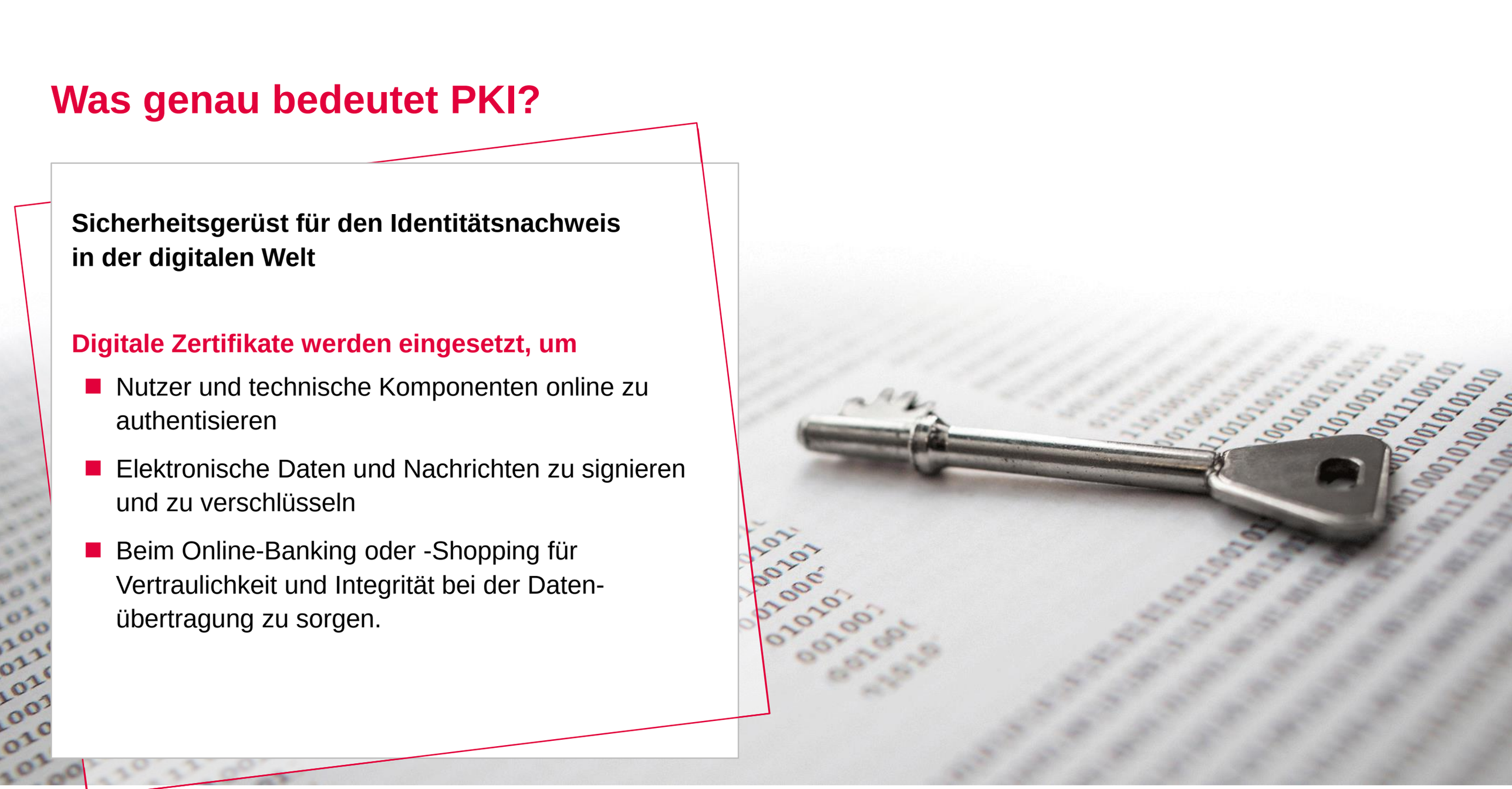
Björn Jansen, secunet Security Networks AG

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 Daten-übertragung zu sorgen.



secunet

PKI – ein alter Hut?

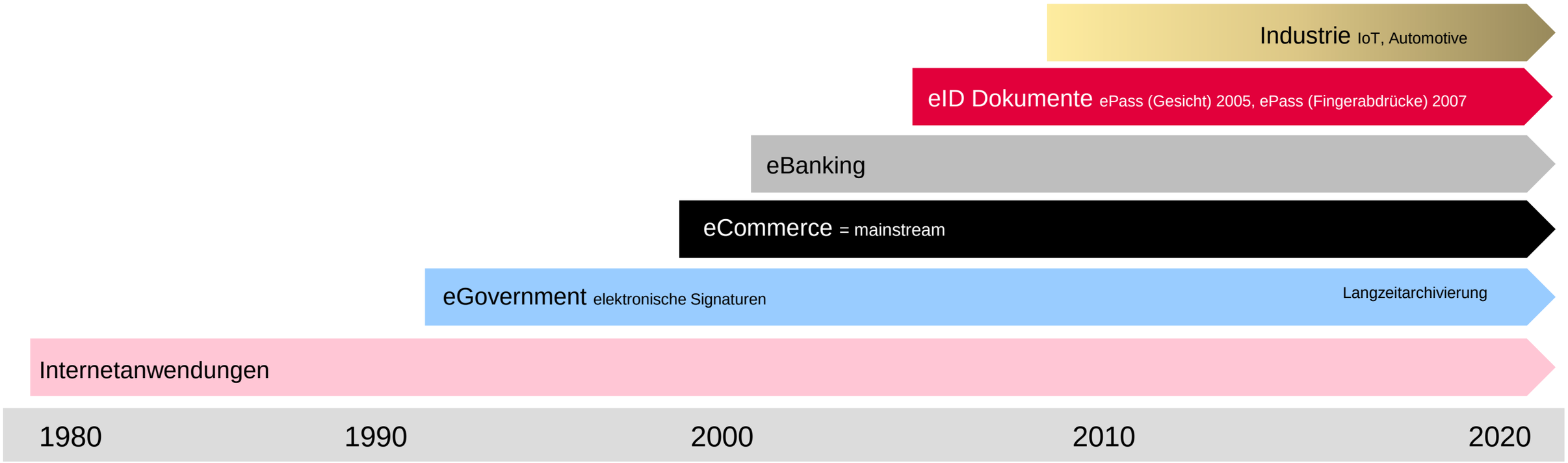
Vom Gefühl her sicherlich schon so alt…

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 stellten 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?

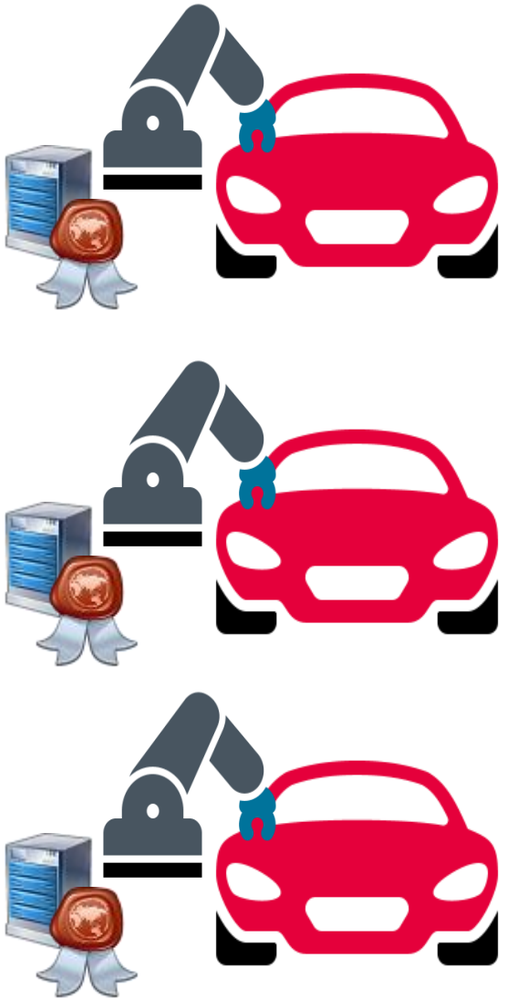
- Updateprozesse
- Einspielen von Konfigurationen
- (Fern-)Wartungszugriffe
- Absicherung von Mehrwertdiensten
  - Wetterdaten, Kartenupdates ... im Fahrzeug
  - Rezepte und mehr für andere Geräte
- Konformität zwischen Schnittstellen
- Risikoschutz

secunet

Herausforderung Ökosystem

CA Betriebsumgebung

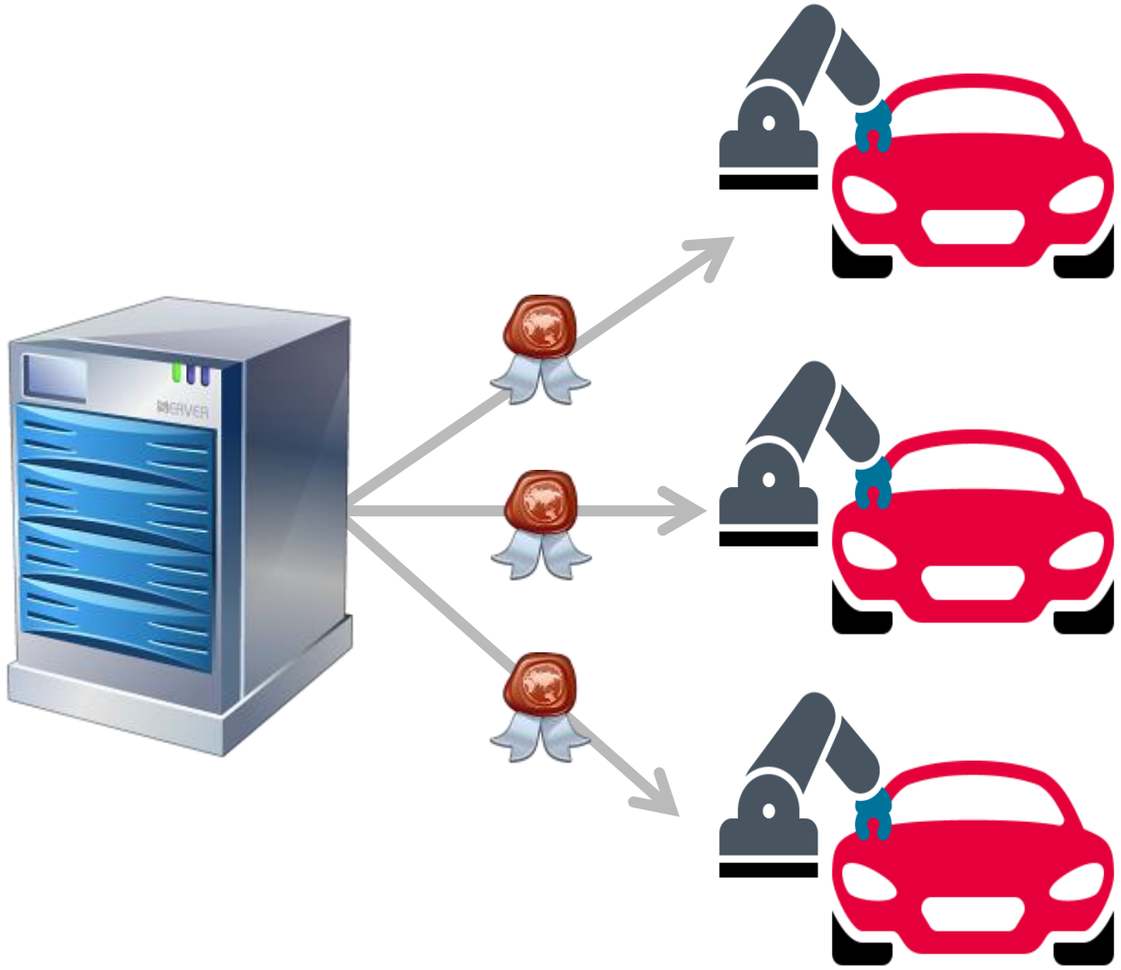
- Lokal, verteilt jeweils an den Provisionierungspunkten



Herausforderung Ökosystem

CA Betriebsumgebung

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

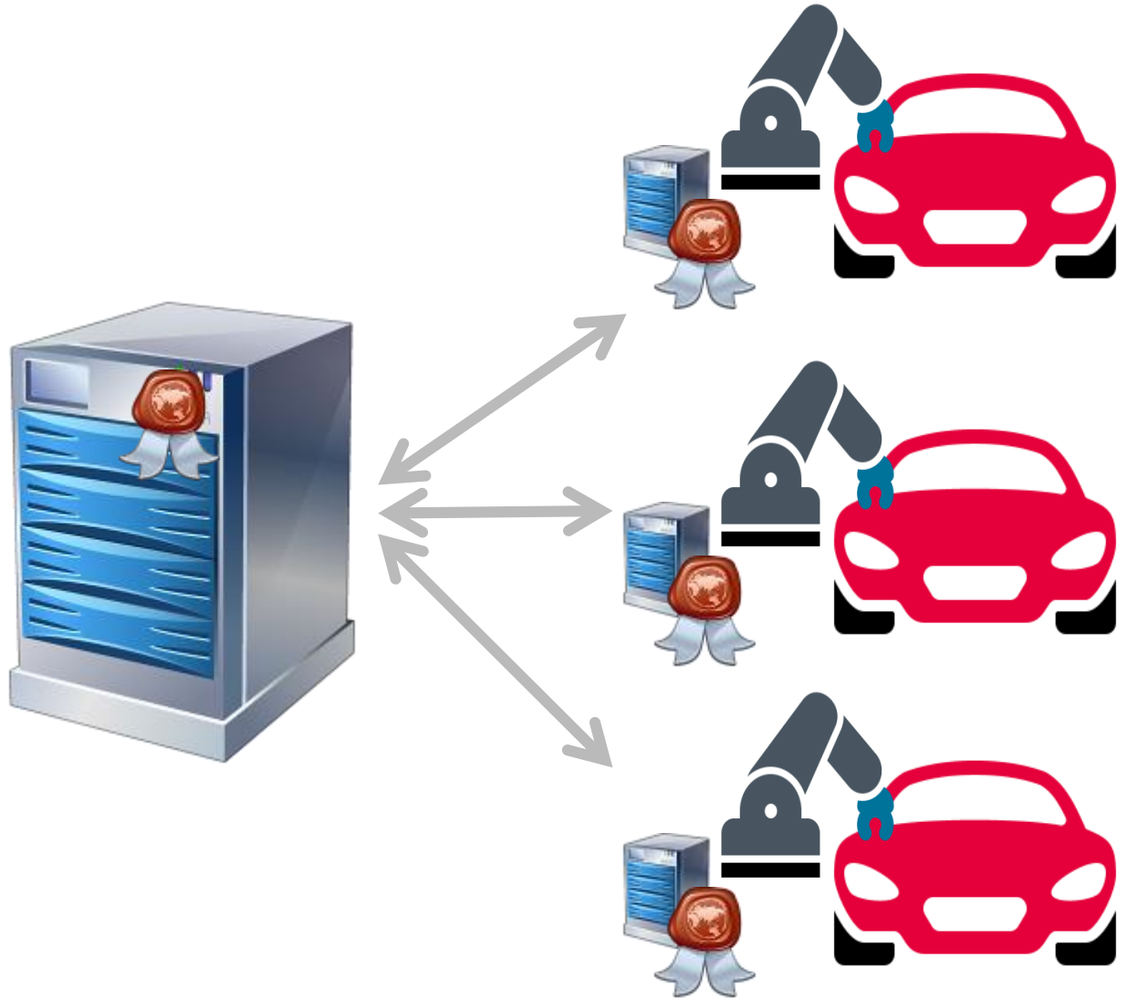


secunet

Herausforderung Ökosystem

CA Betriebsumgebung

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



secunet

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)

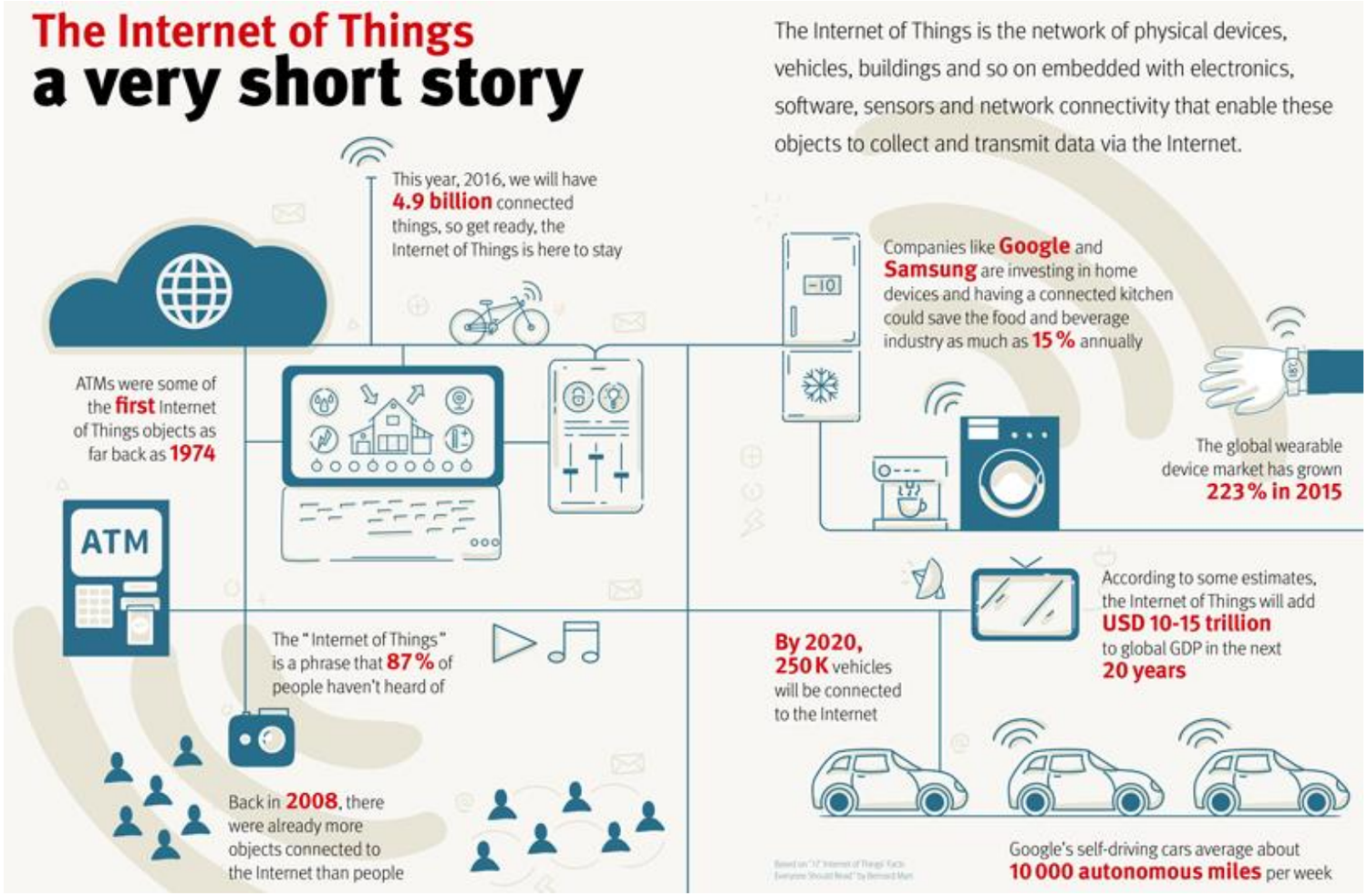
Beispielpunkte:

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

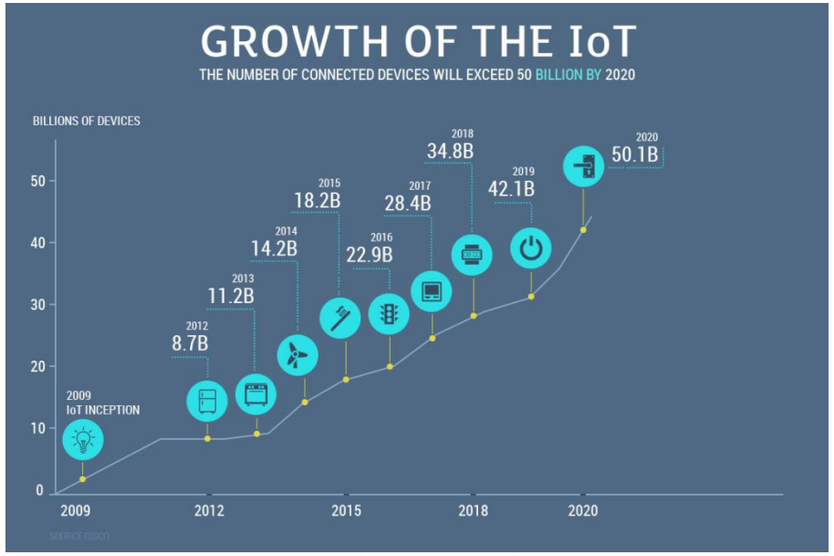
Kosten

secunet

PKI – der Schlüssel für die Zukunft



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



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

secunet

Björn Jansen
Vertrieb
Division Kritische Infrastrukturen

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen
Telefon +49 201 5454-3869
bjoern.jansen@secunet.com