

IT/OT Certificate Lifecycle Management

Automatisiert und kryptoagil

Klaus Schmeh, Simon Ulmer
Eviden Digital Identity





**Hello
everybody!**

大家好

**Bonjour tout
le monde!**

**Hallo
zusammen!**

**Du hast die falsche
Sprache konfiguriert.**

**Simon Ulmer, Head of
Digital ID Cybersecurity
Products bei Eviden**



**Klaus Schmeh, Editor
Marketing bei Eviden**



**Eviden Digital Identity,
Home of cryptovision
und IDnomic**

**Wir schützen elektronische
Identitäten mit
kryptografischen Lösungen.**



EVIDEN

Heute geht
es um CLM.



Was ist
das?

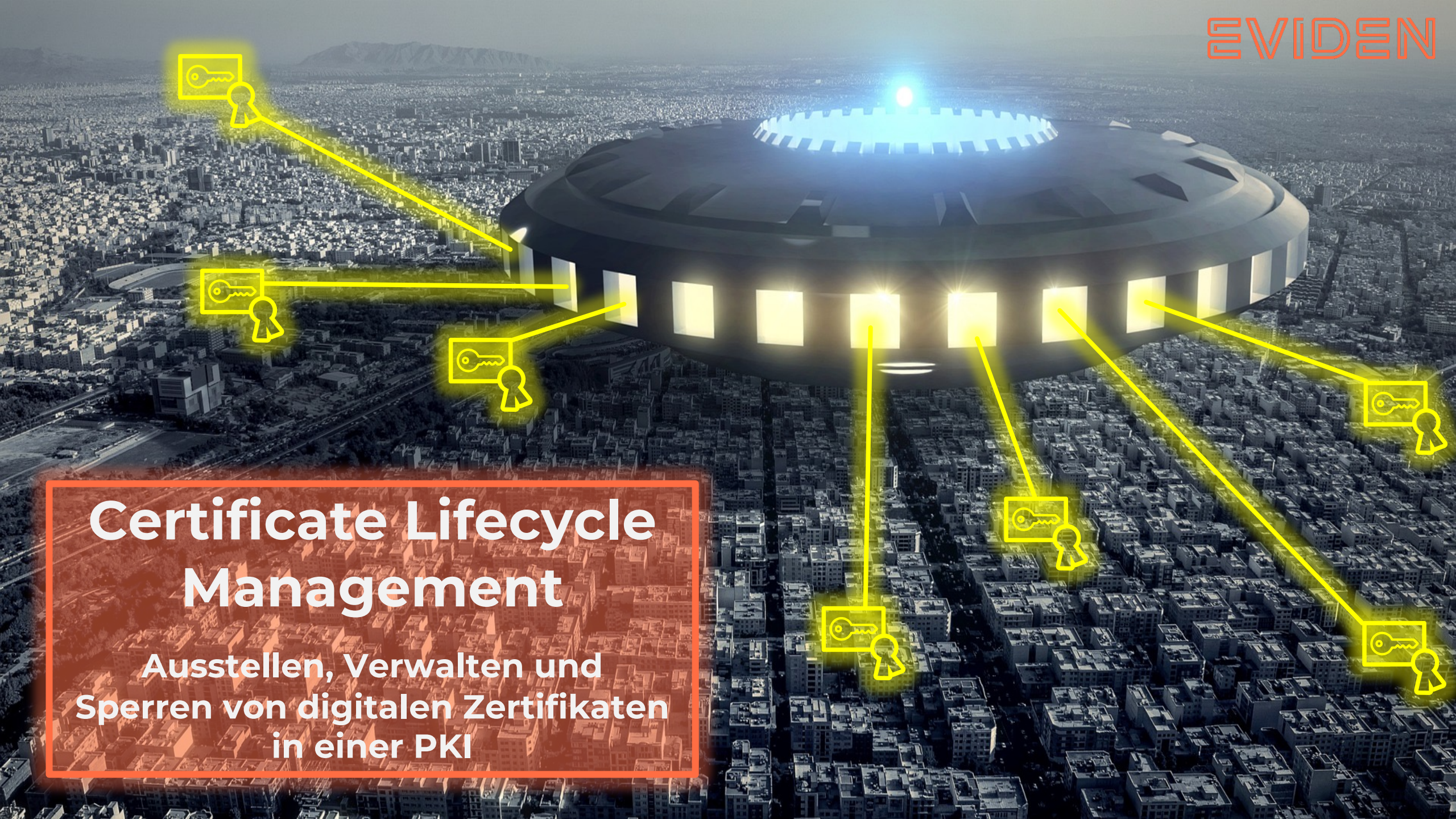




**Public-Key-
Infrastruktur (PKI)**
Infrastruktur zur Verwaltung von
digitalen Zertifikaten

Certificate Lifecycle Management

Ausstellen, Verwalten und Sperren von digitalen Zertifikaten in einer PKI



Eviden CLM-Ansatz

Ende-zu-Ende
Certificate
Lifecycle
Management



Nutzen

IDnomic Sign: Signaturlösung
GreenShield: E-Mail- und Dateiverschlüsselung

Verteilen

CardOS: Kartenbetriebssystem
SCinterface: Smartcard-Middleware
ID RA, ID CMS: Credential-Management

Generieren

ID CA: Certification Authority

Zu CLM gibt es
einiges zu erzählen.



Schauen wir auf
die Agenda.



Agenda

Automatisierung

Inventarisierung

Action

Agenda

Automatisierung

Inventarisierung

Action

**Automatisierung
in einer PKI ist
doch ein alter Hut.**



**Teilweise
schon.**





**Ziele der
Automatisierung**

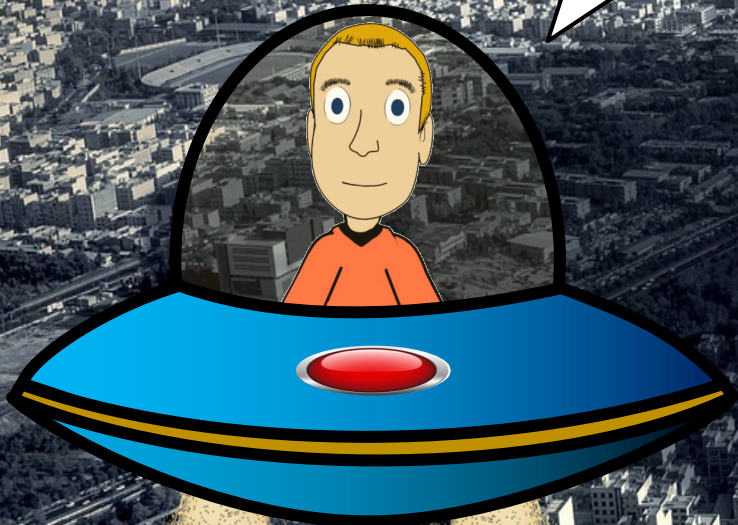


Administration einer PKI vereinfachen

**Umgang mit Zertifikaten für
Anwender vereinfachen**

**Administration von Servern, VPN-
Konzentratoren usw. vereinfachen**

Mittel der Automatisierung



Bulk-Registrierung

User Self Service

Auto-Enrollment

ACME

SCEP

CMP

EST

PKI-Client

Automatische

**Zertifikats-
erneuerung**

OCSP

**Automatisierung
ist also nicht neu.**



**Es gibt aber neue
Herausforderungen: früher
Personen, heute IoT.**



**Micro Segmentation
Zero Trust
Integrität im OT-Bereich
Brücke zwischen IT und OT
IEC 62443
ZTO**

Was ist
ZTO?



Zero Touch
Onboarding.

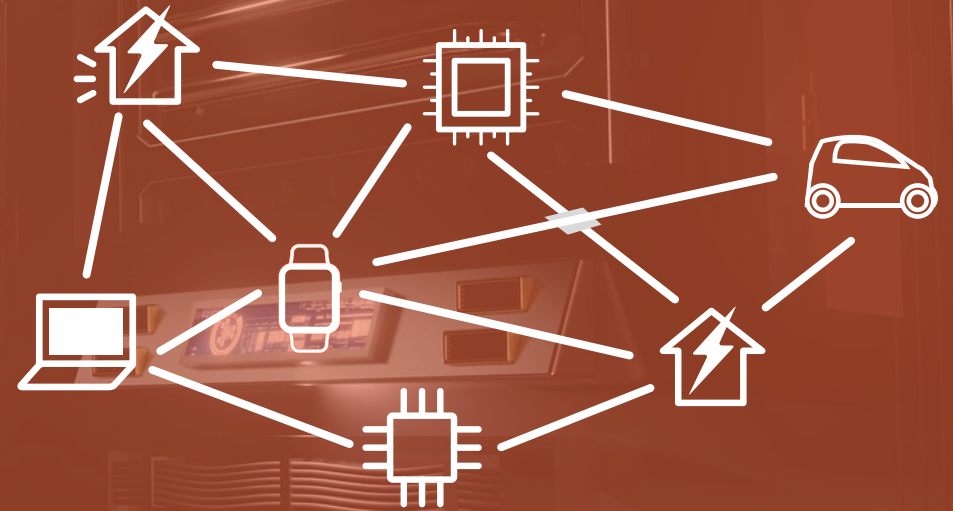


Zero-Touch-Onboarding

Hersteller



Kunde



Zero-Touch-Onboarding

Hersteller

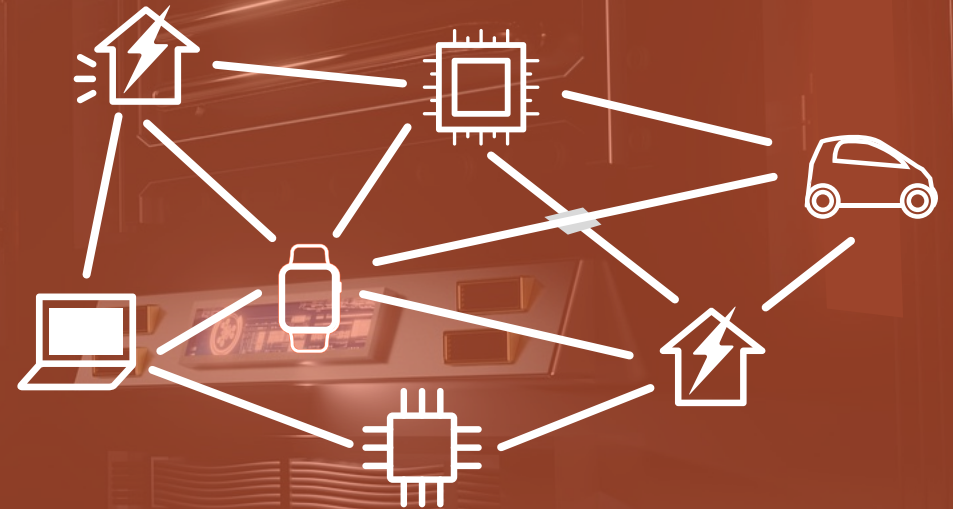


Hersteller-
PKI

ZTO-Dienst



Kunde



Kunden-
PKI

Zero-Touch-Onboarding

Hersteller



Neue
Komponente



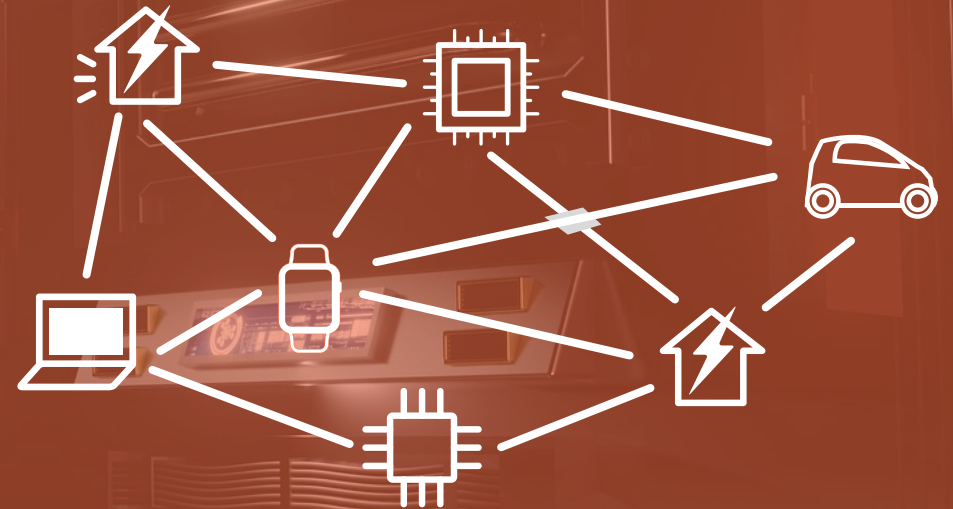
Hersteller-
PKI

Vergibt digitales
Zertifikat

ZTO-Dienst



Kunde



Kunden-
PKI

Zero-Touch-Onboarding

Hersteller



Neue
Komponente



Hersteller-
PKI



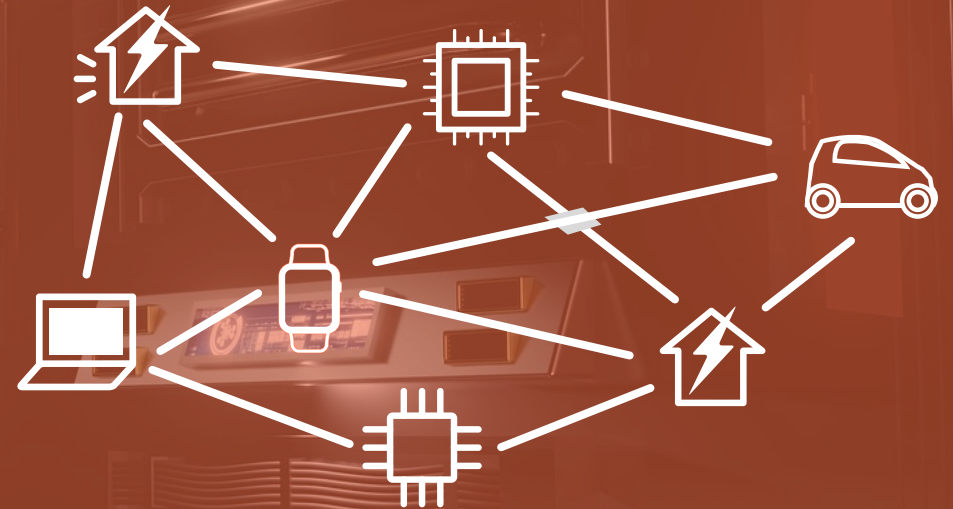
ZTO-Dienst



Authentifiziert
sich



Kunde



Kunden-
PKI



Zero-Touch-Onboarding

Hersteller

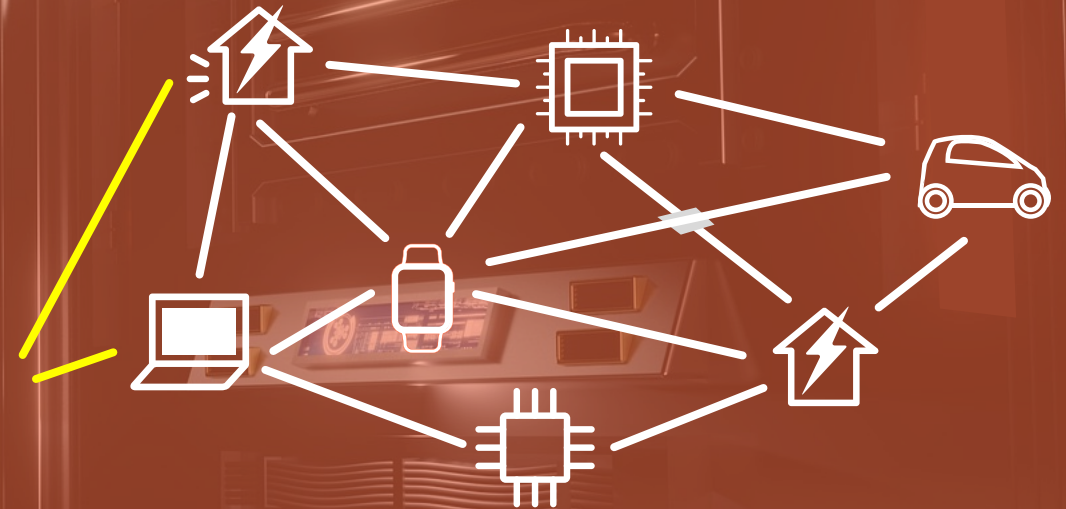


Hersteller-
PKI

ZTO-Dienst



Kunde



Kunden-
PKI

Zero-Touch-Onboarding

Hersteller



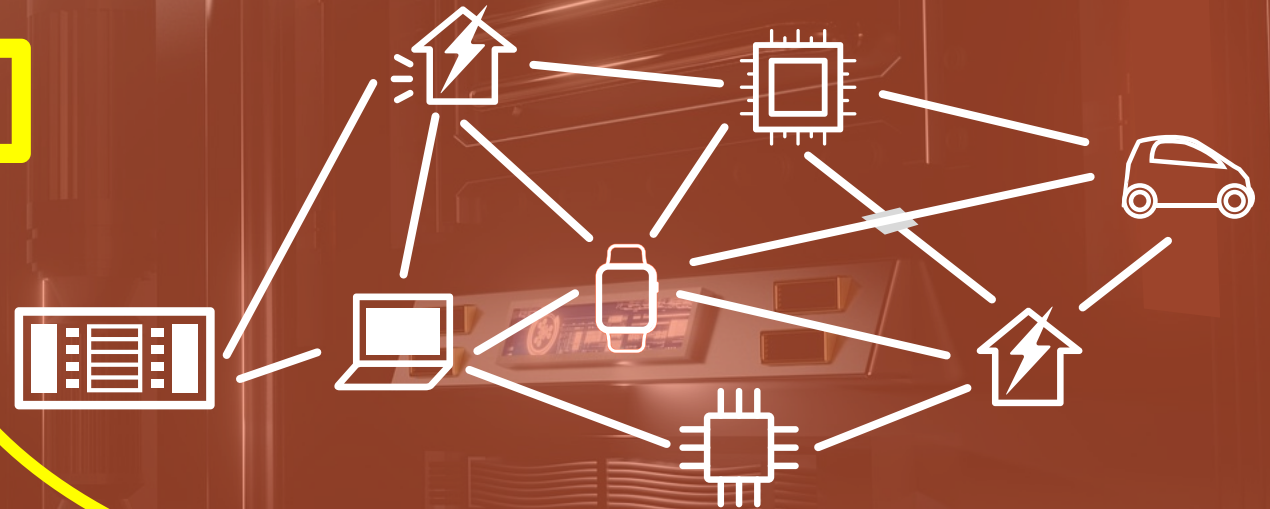
Hersteller-
PKI

ZTO-Dienst



Überträgt
Identität und
Informationen

Kunde



Kunden-
PKI

Zero-Touch-Onboarding

Hersteller



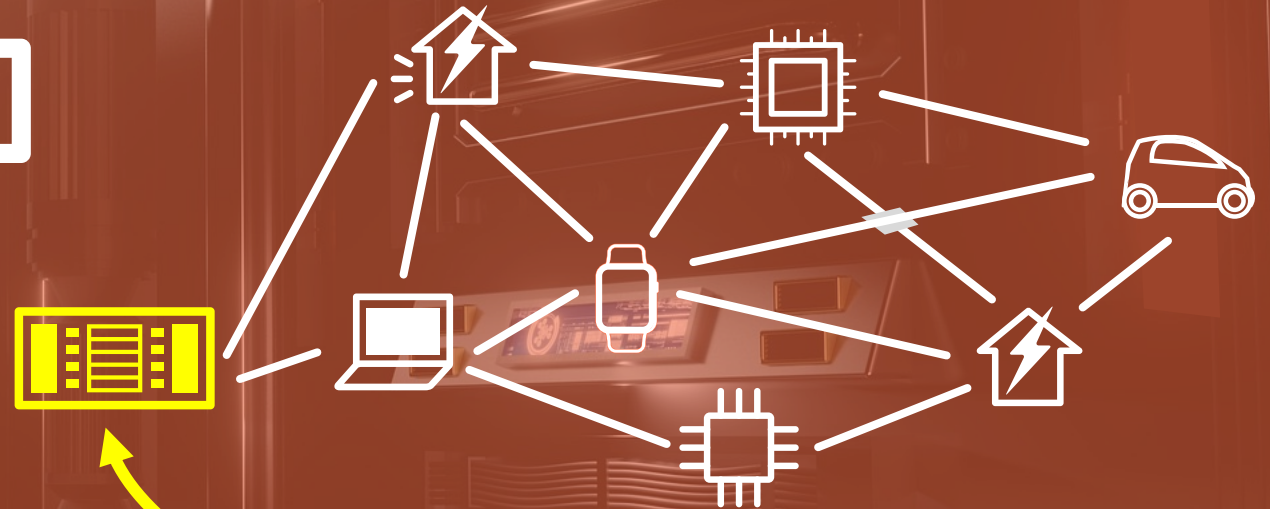
Hersteller-
PKI

ZTO-Dienst



Vergibt digitales
Zertifikat

Kunde



Kunden-
PKI

Zero-Touch-Onboarding

Hersteller



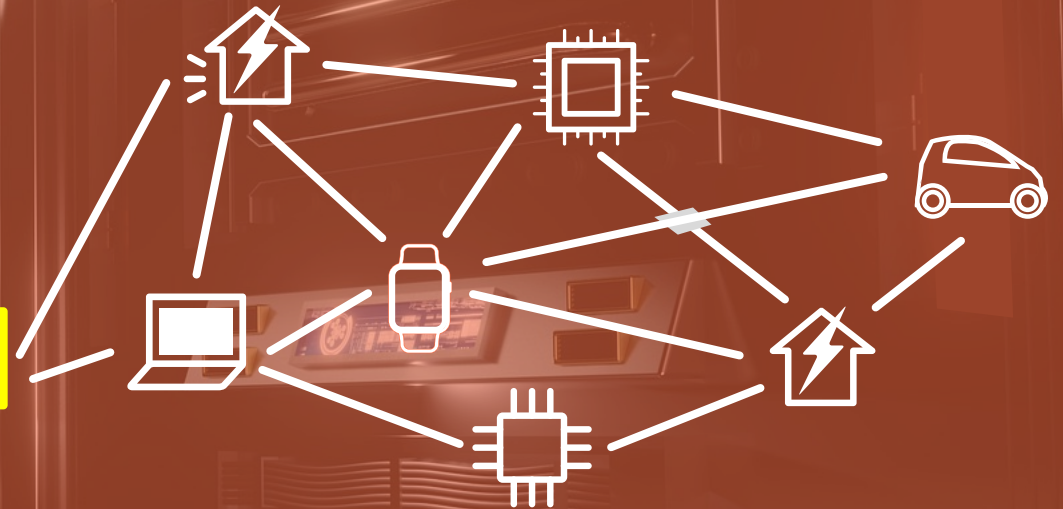

Hersteller-
PKI

ZTO-Dienst



Erhält Zugriffsrechte
und Konfiguration auf
Basis des Zertifikats

Kunde




Kunden-
PKI

Zero-Touch-Onboarding

Hersteller



Hersteller-
PKI

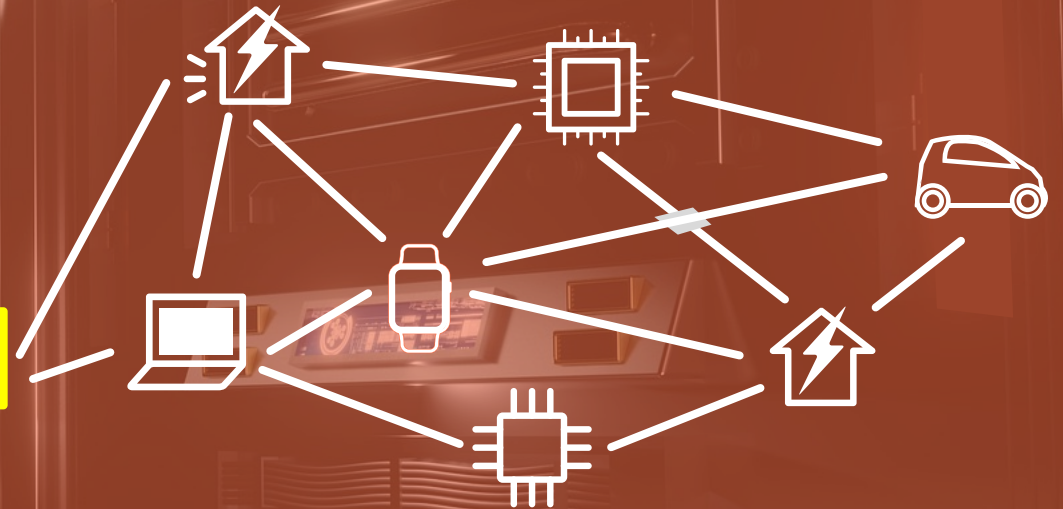
ZTO-Dienst



Wird Teil des
Kundennetzes



Kunde



Kunden-
PKI

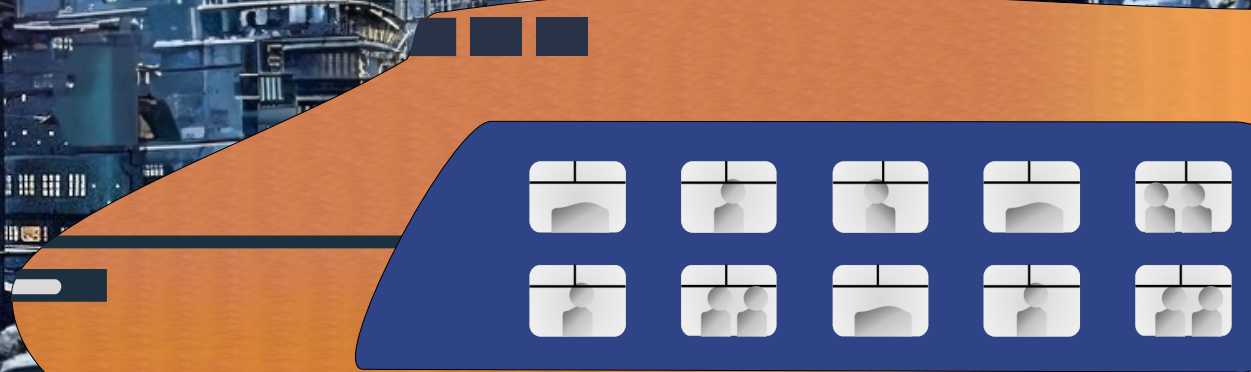
Ich kenne ein
Beispiel?

In Paris?

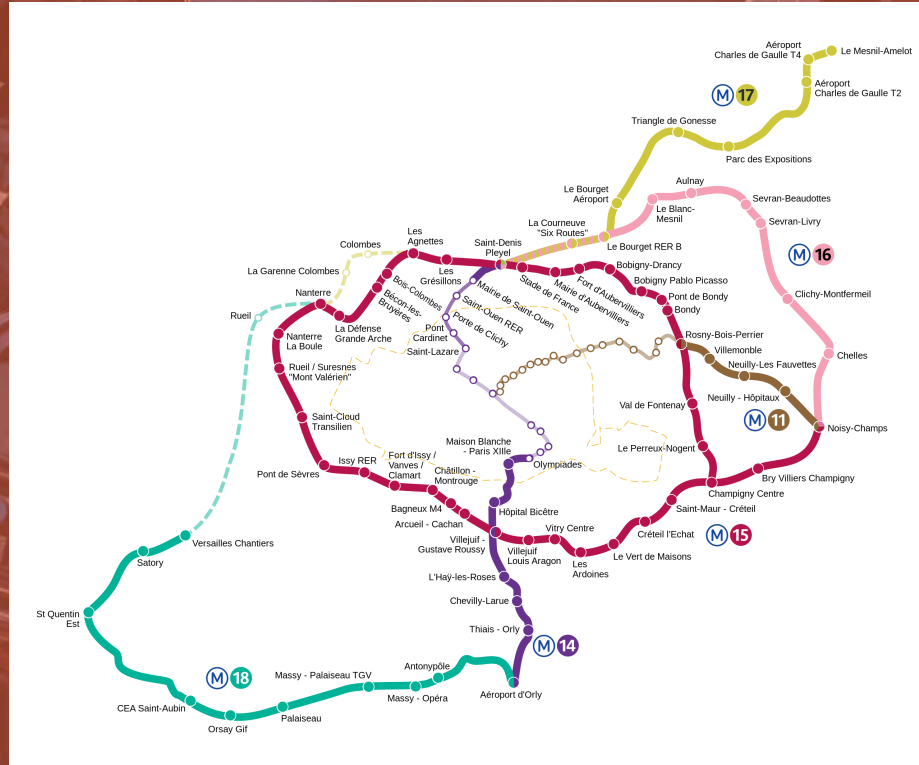


Grand Paris Express

Geplantes U-Bahn-Netz im Raum Paris

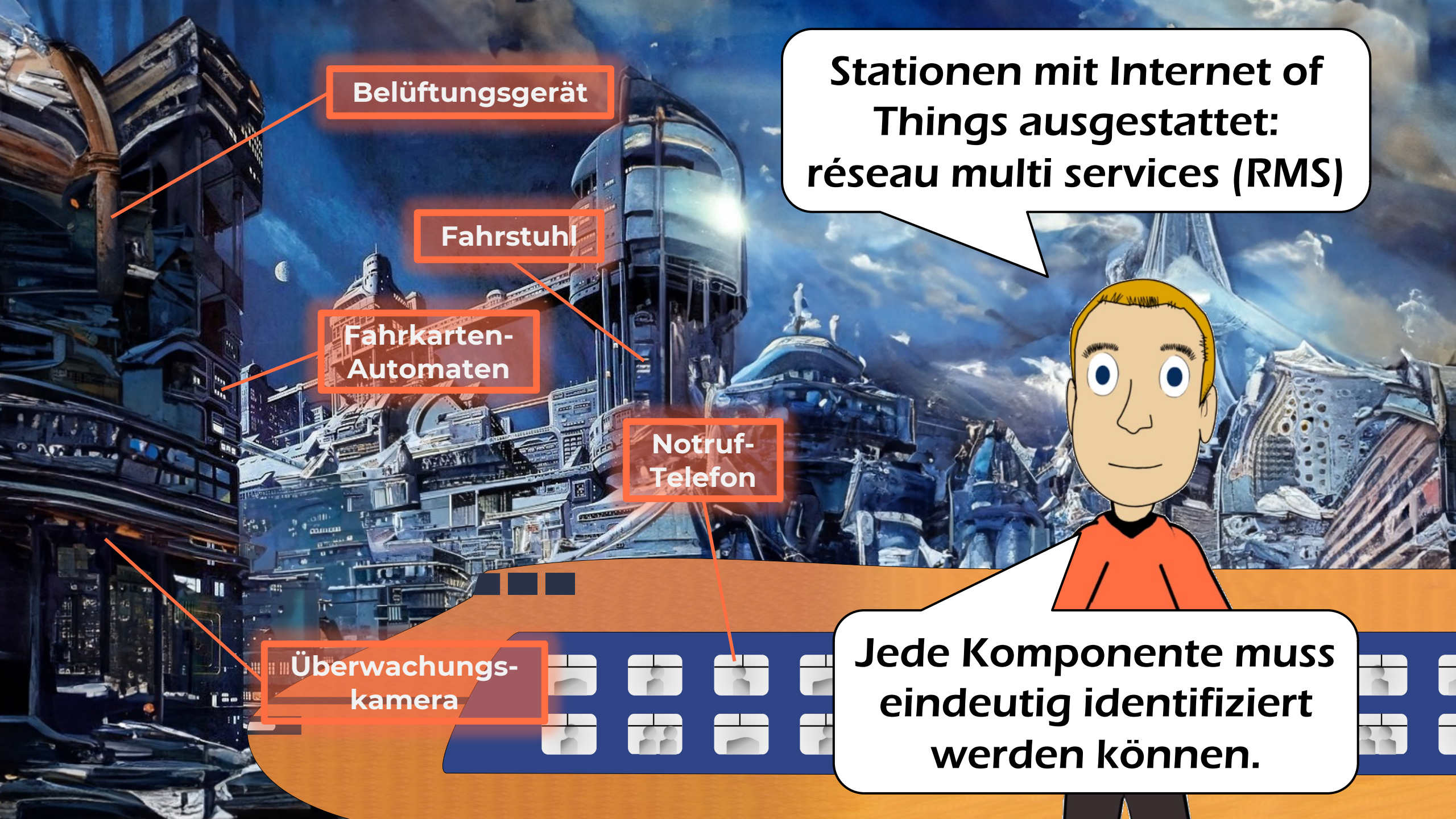


Grand Paris Express



Erster Teil soll bis zu den Olympischen Spielen 2024 fertiggestellt sein.





Belüftungsgerät

Fahrstuhl

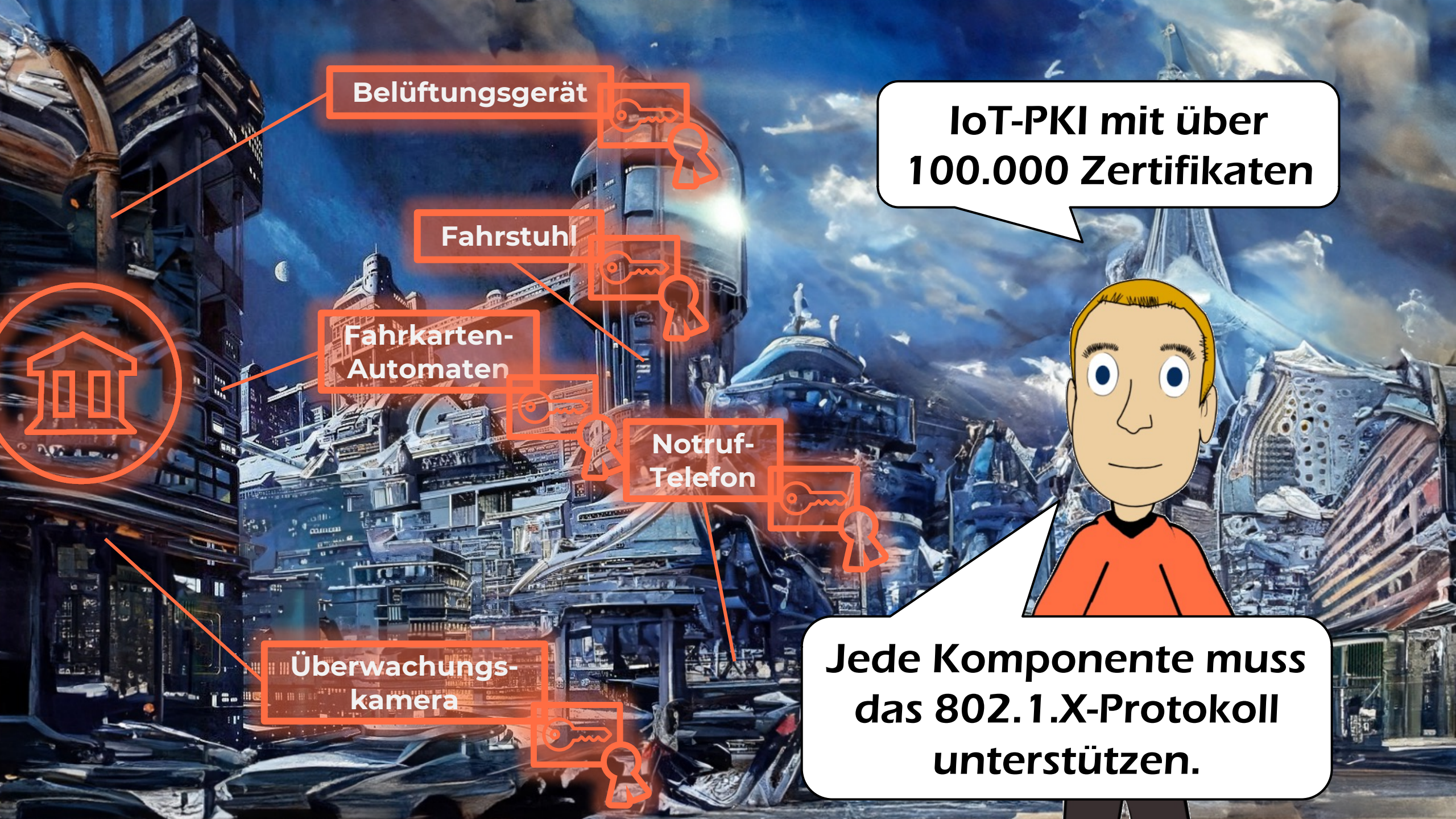
Fahrkarten-Automaten

Notruf-Telefon

Überwachungs-kamera

Stationen mit Internet of Things ausgestattet: réseau multi services (RMS)

Jede Komponente muss eindeutig identifiziert werden können.



Belüftungsgerät

Fahrsstuhl

Fahrkarten-Automaten

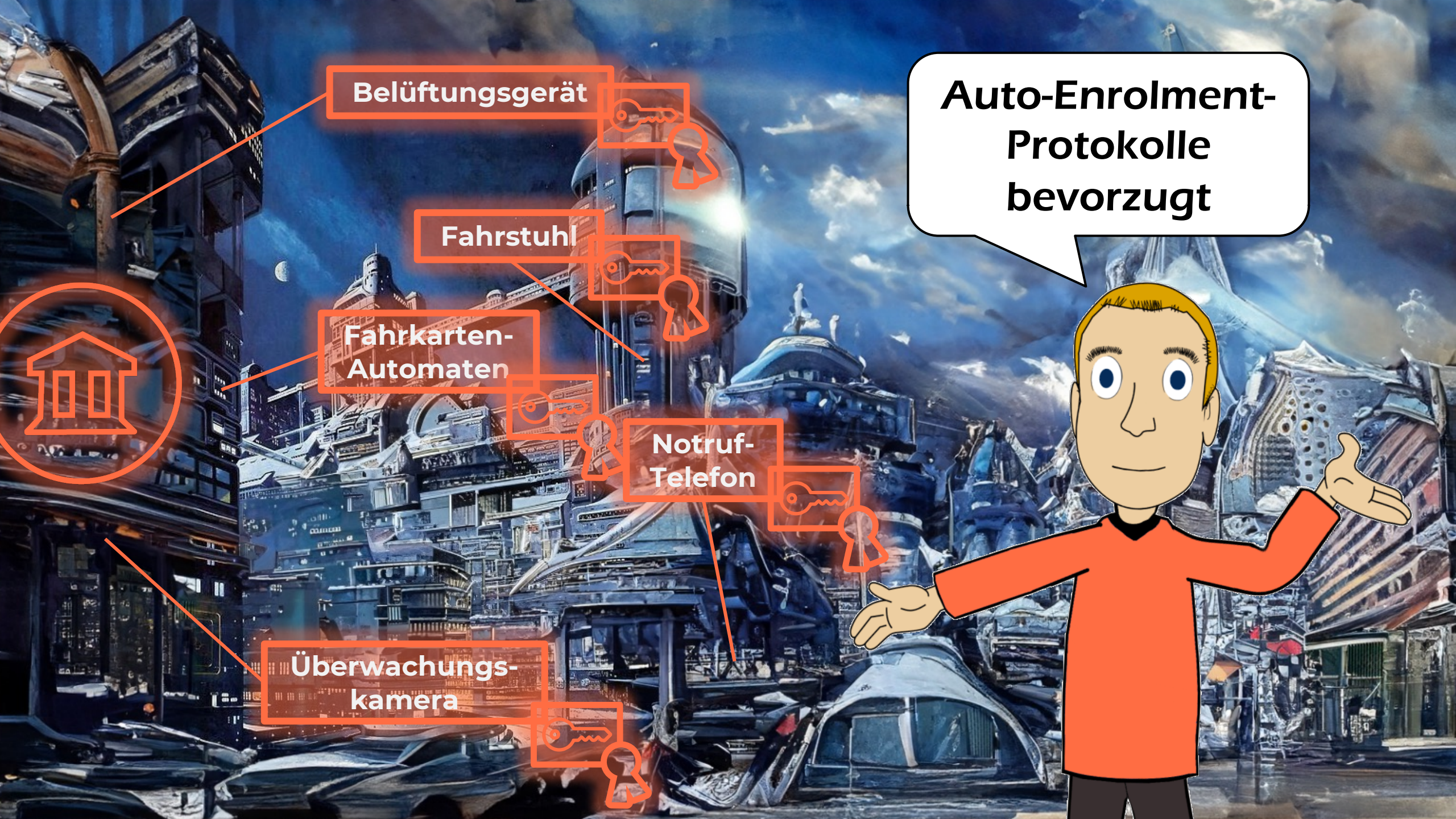
Notruf-Telefon

Überwachungs-kamera

IoT-PKI mit über 100.000 Zertifikaten

Jede Komponente muss das 802.1X-Protokoll unterstützen.





Belüftungsgerät

Fahrstuhl

Fahrkarten-Automaten

Notruf-Telefon

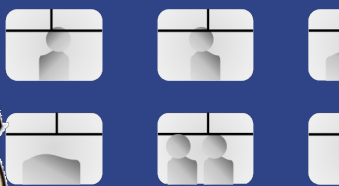
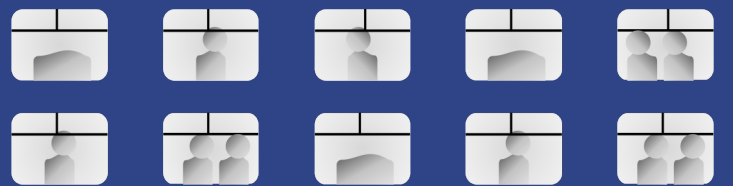
Überwachungs-kamera

Auto-Enrolment-Protokolle bevorzugt



**IoT-PKI mit über
100.000 Zertifikaten**

**Mangel an Unterstützung von
Protokollen festgestellt. Bisher
alles manuell implementiert.**



Zukünftig wird Zero Touch Onboarding (ZTO) angestrebt.



Agenda

Automatisierung

Inventarisierung

Action

Worum geht es hier?



Der Betreiber eines IT-Systems will wissen, wo und wie digitale Zertifikate eingesetzt werden.



**Es sollte sein wie in einem
Cockpit: ein Dashboard
bzw. Single Pane of Glass**





Certificates

Alerts

Compliance



Own CA

External

MS-PKI

X.509

Card-verifiable

PGP



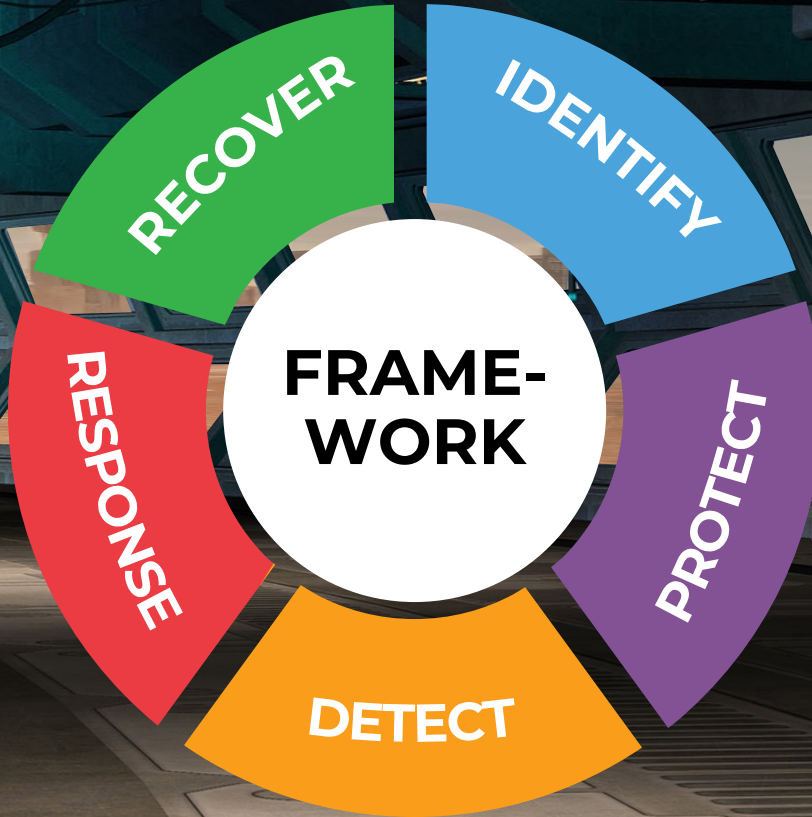
Krypto-Inventar

ID	Anwendungsbereich	Krypto-Lösung	Krypto-Verfahren	Status
259	Sicherer Zugriff auf Webseiten	Firefox TLS	AES-256 SHA-384 ECDH P-256	PQC-readiness plan
260	Datei-Verschlüsselung für USB-Speichersticks	VeraCrypt	AES-256 SHA-512	PQC-ready
263	E-Mail-Verschlüsselung in Controlling-Abteilung	Outlook 2021 auf Windows	AES-256 SHA-384 RSA-2048	PQC-readiness plan
264	E-Mail-Verschlüsselung in Entwicklungsabteilung	Outlook 2021 auf Windows	AES-256 SHA-384 RSA-2048	PQC-readiness plan
267	E-Mail-Krypto-Gateway	ABC Secure Mail Gate	AES-256 SHA-384 RSA-2048	PQC-readiness plan
269	VPN-Client	ABC VPN	AES-128 SHA-1 RSA-1024	PQC-option
270	E-Mail-Signatur	Mail-Sign	AES-256	PQC-readiness plan

Schwachstellen entdecken

Sichtbarkeit erhöhen

NIST Framework Cybersecurity 2.0



Was gibt es zu tun?

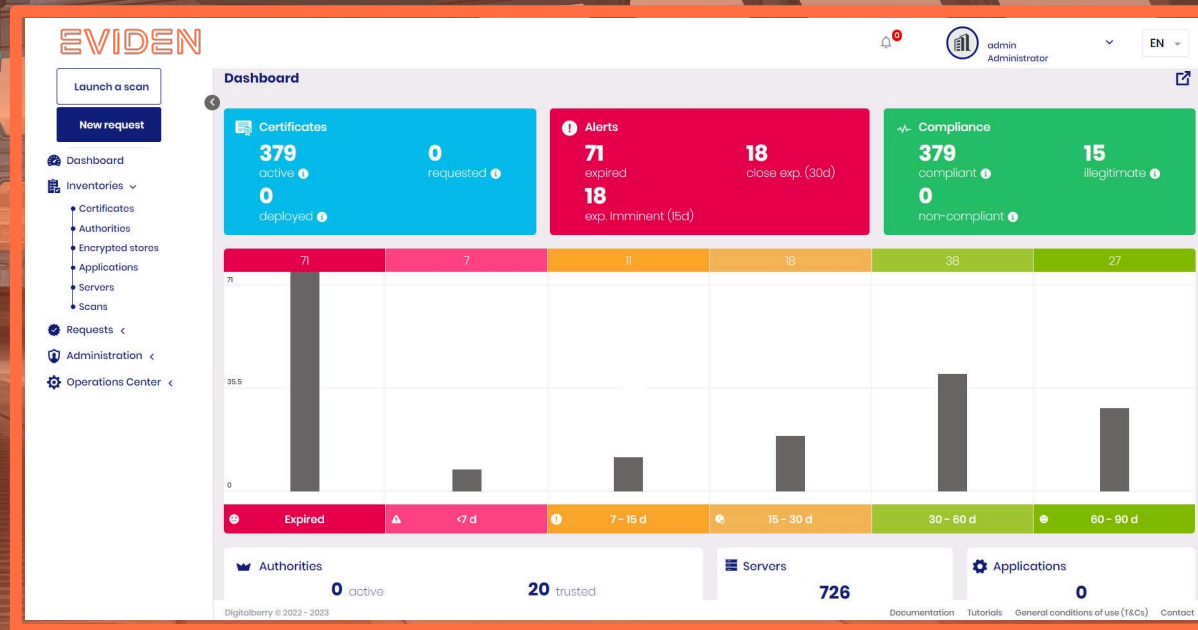


Risikobewertung,
Priorisierung



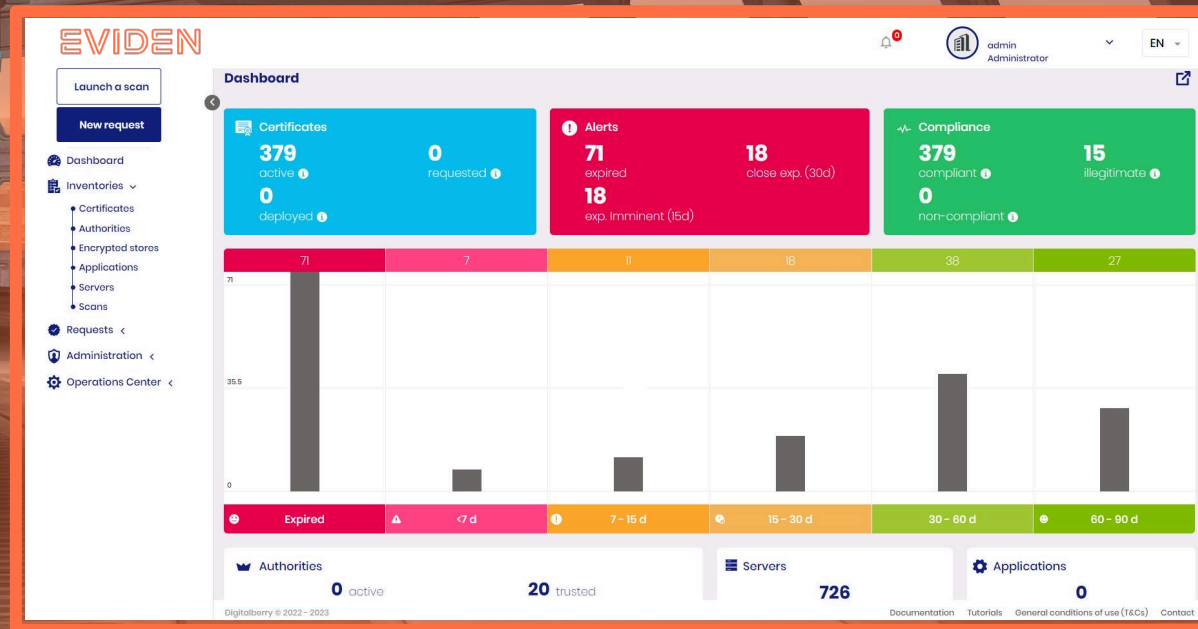
Kann man die
Inventarisierung
automatisieren?

Ja, es gibt
Tools.



Was können diese Tools?

Über Agenten nach Zertifikaten suchen
Webserver anpingen



Agenda

Automatisierung

Inventarisierung

Action

Was gibt es
zu tun?



Einiges.



Action

PKI
vereinheitlichen

PKI
automatisieren

Schwache Krypto-
Verfahren, kurze
Schlüssel ersetzen

Zertifikate
umschreiben, migrieren

Google-Vorgabe
umsetzen: Zertifikate
nur noch 90 Tage gültig

Und was ist mit
Krypto-Agilität.



Die ist besonders
wichtig.



Krypto-Agilität

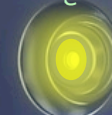


**Unter anderem sind
lange Schlüssel eine
Herausforderung.**

RSA

ECC

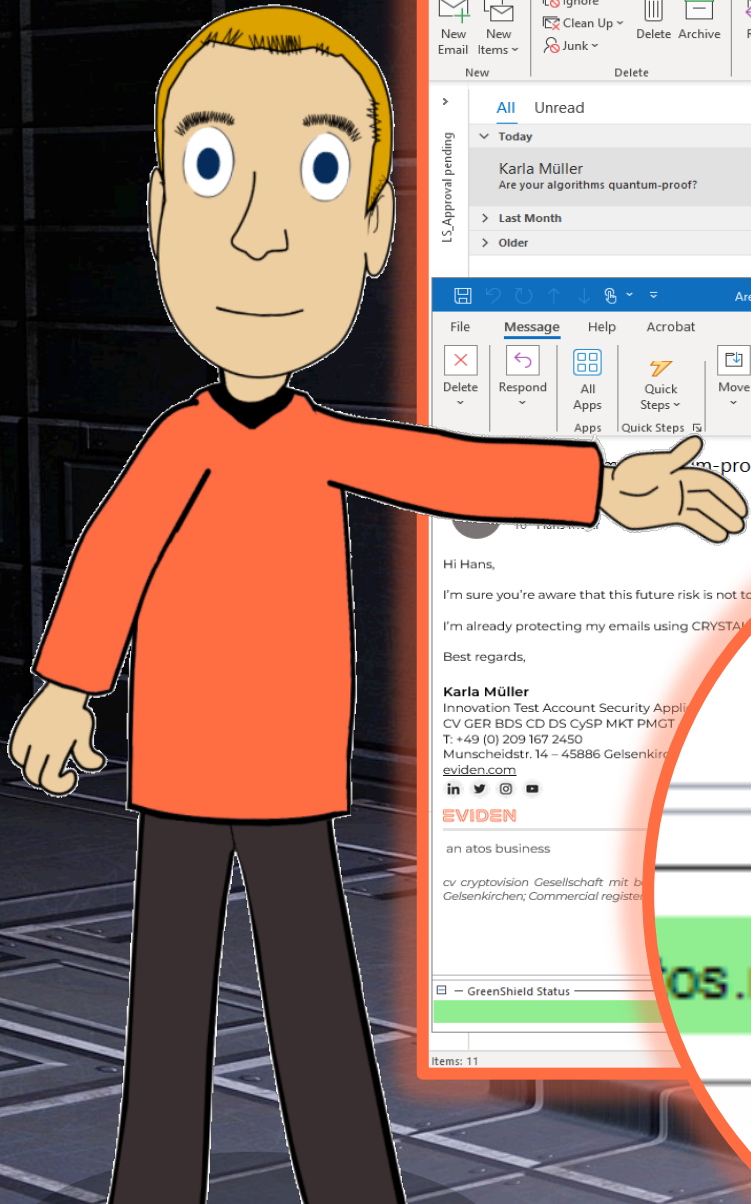
Kyber

Dilithiu
mMcElie
c

Bietet PQC-
Preview-Modul



**cryptovision
GreenShield**
Mail- und File-
Verschlüsselung



The screenshot shows a Microsoft Outlook interface. The main window displays an email titled "Are your algorithms quantum-proof? - Message (HTML)". The email content includes:

Hi Hans,

I'm sure you're aware that this future risk is not to be...

I'm already protecting my emails using CRYSTAL...

Best regards,

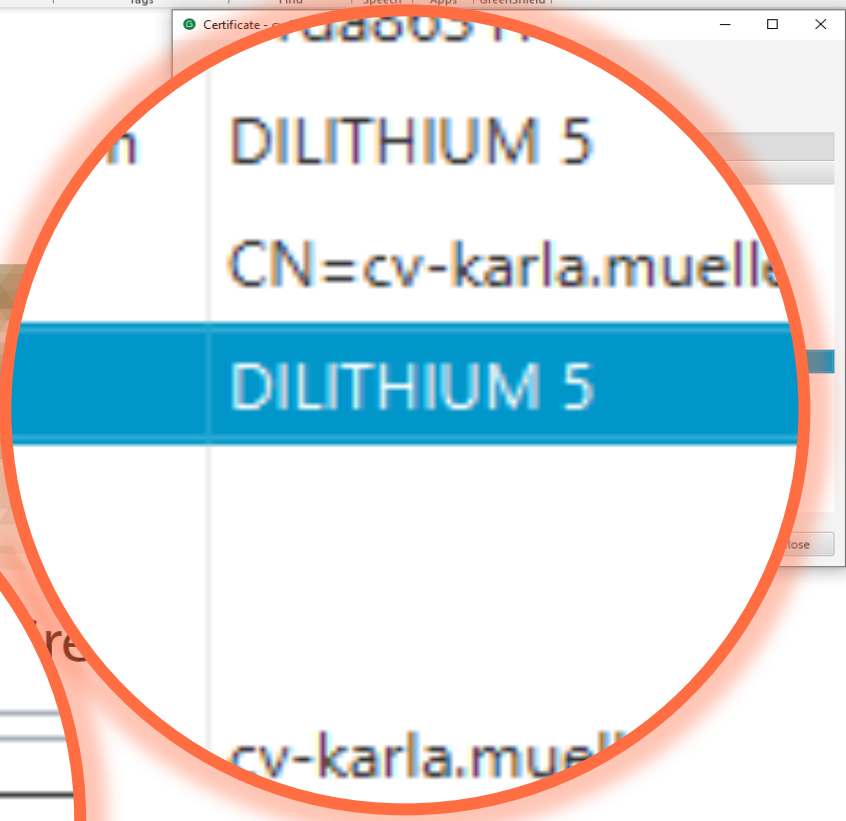
Karla Müller
Innovation Test Account Security Appli...
CV GER BDS CD DS CySP MKT PMCT...
T: +49 (0) 209 167 2450
Munscheidstr. 14 – 45886 Gelsenkir...
eviden.com
in [social media icons]

EVIDEN
an atos business

cv cryptovision Gesellschaft mit b...
Gelsenkirchen; Commercial regist...

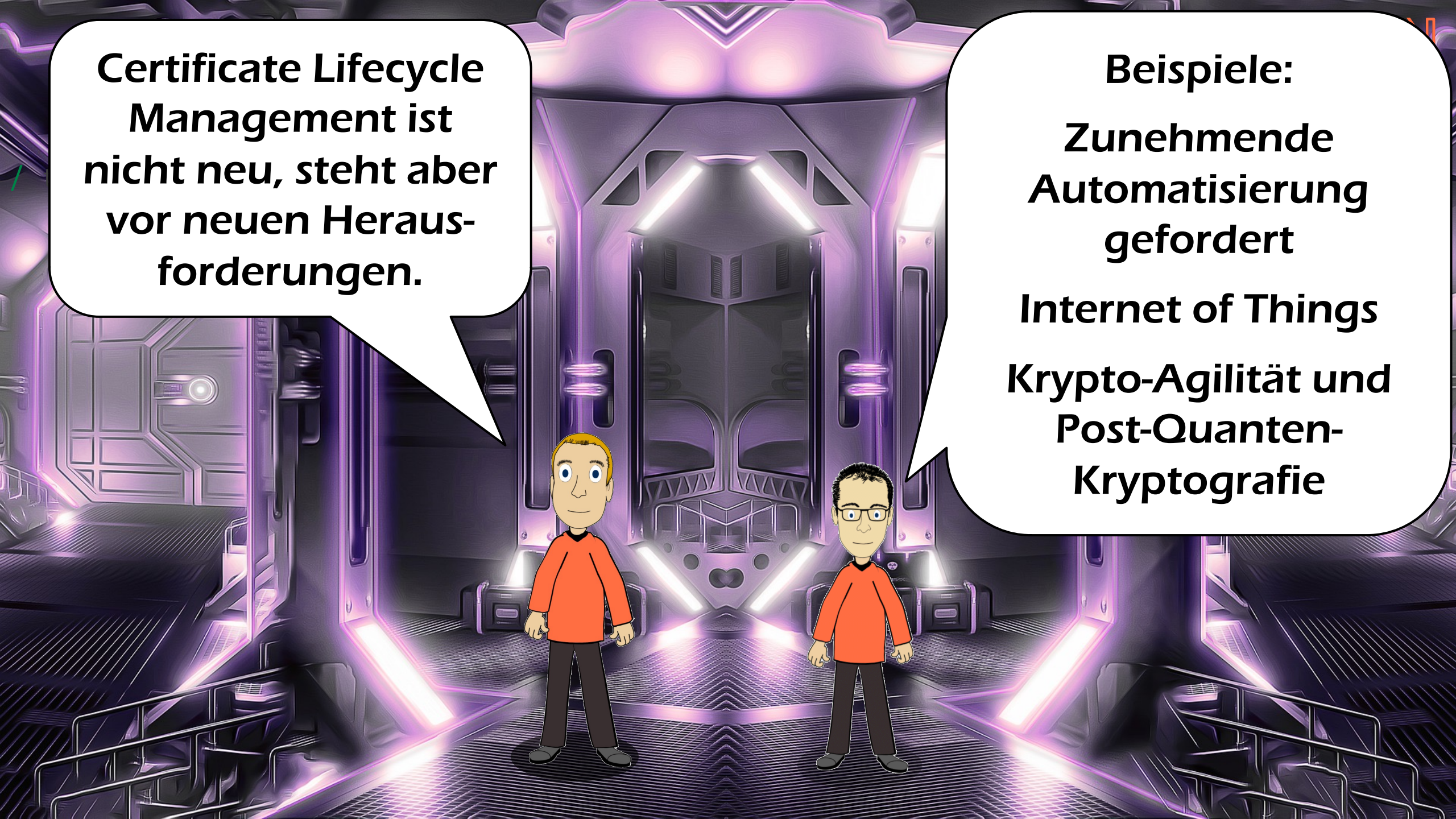
os.net' - DILITHIUM 5

At the bottom of the Outlook window, it says "Items: 11" and "All folders are up to date. Connected to: Microsoft Exchange".



EVIDEN

Fazit



Certificate Lifecycle Management ist nicht neu, steht aber vor neuen Herausforderungen.

Beispiele:
Zunehmende Automatisierung gefordert
Internet of Things
Krypto-Agilität und Post-Quanten-Kryptografie

EVIDEN

EVIDEN

