Cyber Security

im Öffentlichen Verkehr

Security-Massnahmen in der Umsetzung

Basile Bluntschli, Head Engineering & Operations, onway

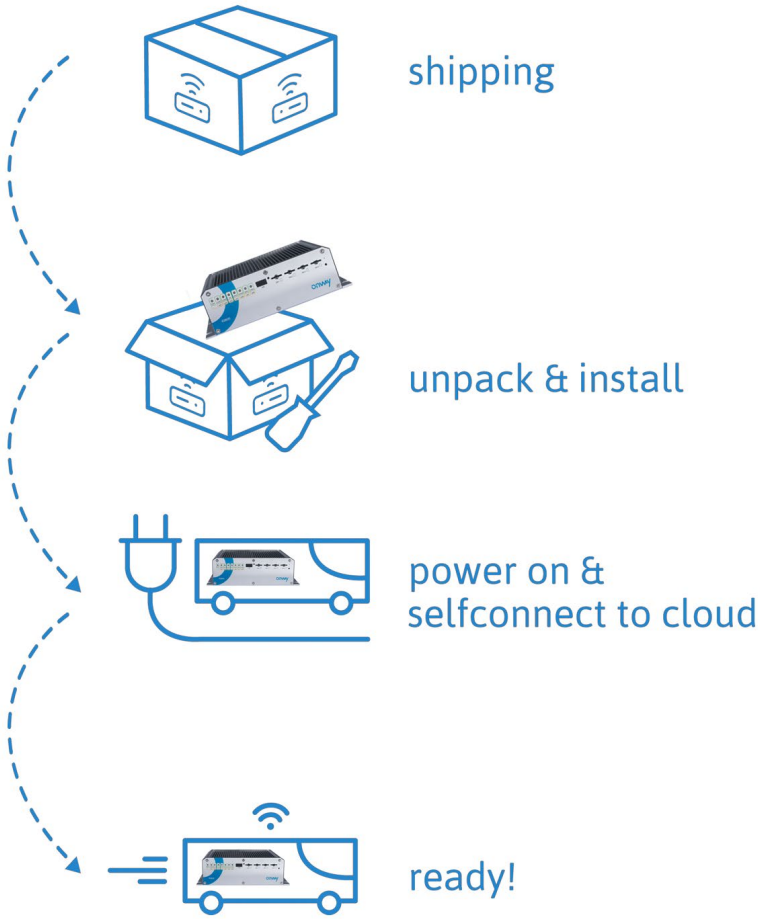
25.10.2023

Wer spricht denn hier?

Basile Bluntschli

- Head Engineering & Operations
- 10+ Years at onway
- Projektumsetzungen
- onway Cloud Services

onway mobile router



onway mobile router

shipping

unpack & install

p
s

ready!

Habitat mobile router

- Die Router werden in unsicheren Netzen eingesetzt
- Operativer Aktivismus versus Sicherheitsüberlegungen
- Komplexität ist der Feind der Sicherheit [Bruce Schneier 1999]
- Kennt ihr die Kollegen?

onway CARLOS

(Cloud-based Advanced Router Linux Operating System)

- Start mit Software Daemon auf Drittsystemen
- Heute eigenes OS, basierend auf Linux LTS Kernel
- Entwicklung der notwendigen Funktionalitäten und Protokolle
- Schlank, um die 30MB

Bootstrapping mobile router

1 CARLOS Image ab Werk installiert

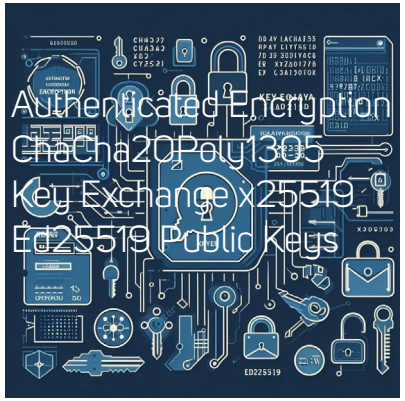
2 Key Generierung bei Inbetriebnahme

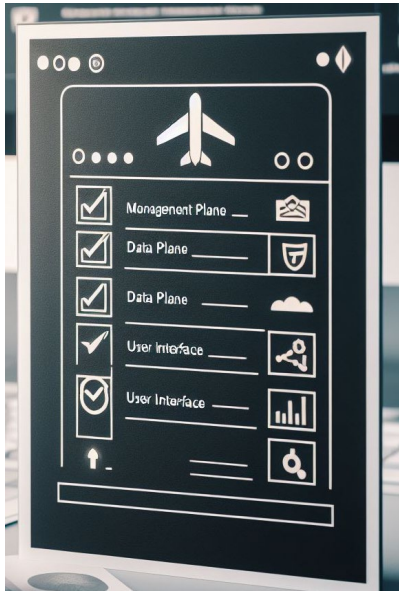
3 onway “Telefonbuch” Anfrage durch mobile router

4 mobile router redirect zu Kunden System

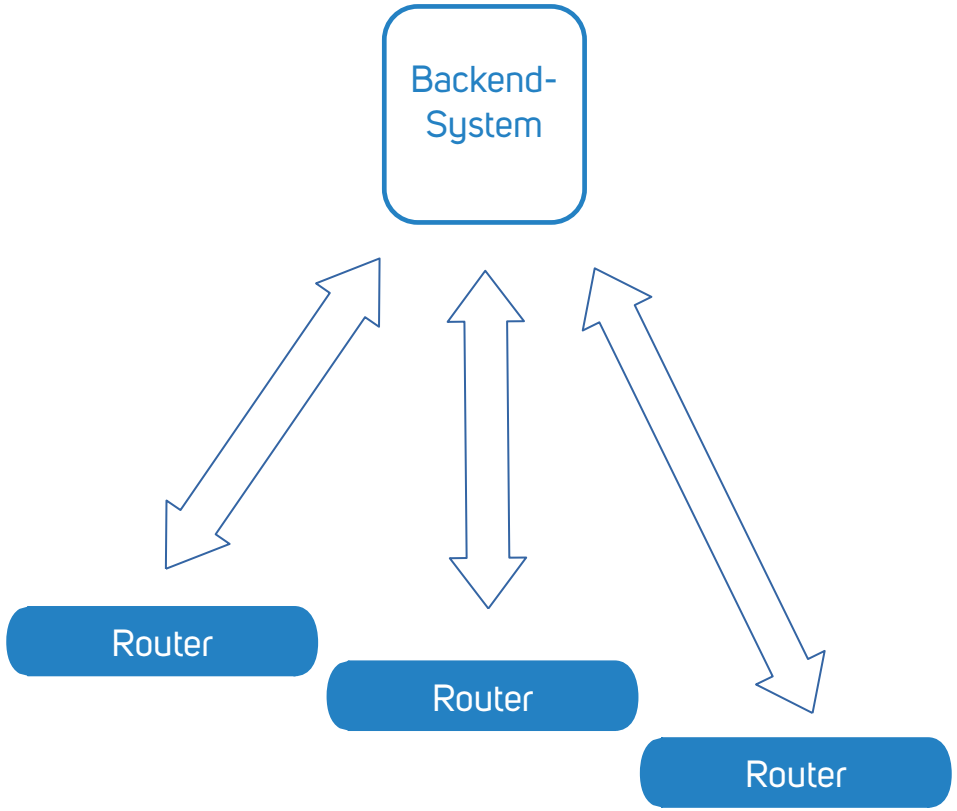
5 Kunden System Kontakt

6 Management Tunnel etabliert





Management Protokoll



Permanente Verbindung Router → Backend

Protokoll, UDP-basiert

- Verschlüsselt Authentisiert
- state-of-the-Art crypto
- Agil über mehrere Uplinks
- Effizientes Encoding, Komprimierung

Multiplexing verschiedener Applikationen

- Telemetrie, Konfiguration, Updates, Remote-Login
- Bidirektionale Kommunikation, Push-Notifications

Backend skalierbar und redundant

- Mandanten-fähig

Get the mobile router ready

Security LAN	enroll NAC
Security IPSEC	enroll certificates
Configuration	push configuration
OS Version	upgrade
Management Plane	established

Upgrade the OS

Integrität

Boottime

Failsafe

Change Configuration

- Atomic Changes
- Failback Mechanism
- Fast Deployment
- No Uncertainty

Tooling made easy

Zentrale Konfiguration im Backend

- Reproduzierbarkeit, Templates, Versionierung
- Zertifikates-Management onway PKI
- Router sind „mgmtless“ aber voll mit lokaler “Intelligenz”

Deployment via GitOps

- Auf ganze Flotten
- Applizierung auf Router in Sekunden(bruchteilen)
- Deployment Pipeline

onway Mixer

Zertifikatsmanagement - Automatisiert

onway EST CA

- EST basierende PKI CA
  - EST = Enrollement over Secure Transport
  - RFC 7030 basiert
- HTTPS REST API für Zertifikatsmanagement
  - Role Based Access
  - Audit Log
  - sBGP IP Addr Block inkludierung
- Voll automatisiert durch den onway Mixer
- Thirdparty Anbindung via HTTPS Rest
- Certificate Revocation List actively deployed and used

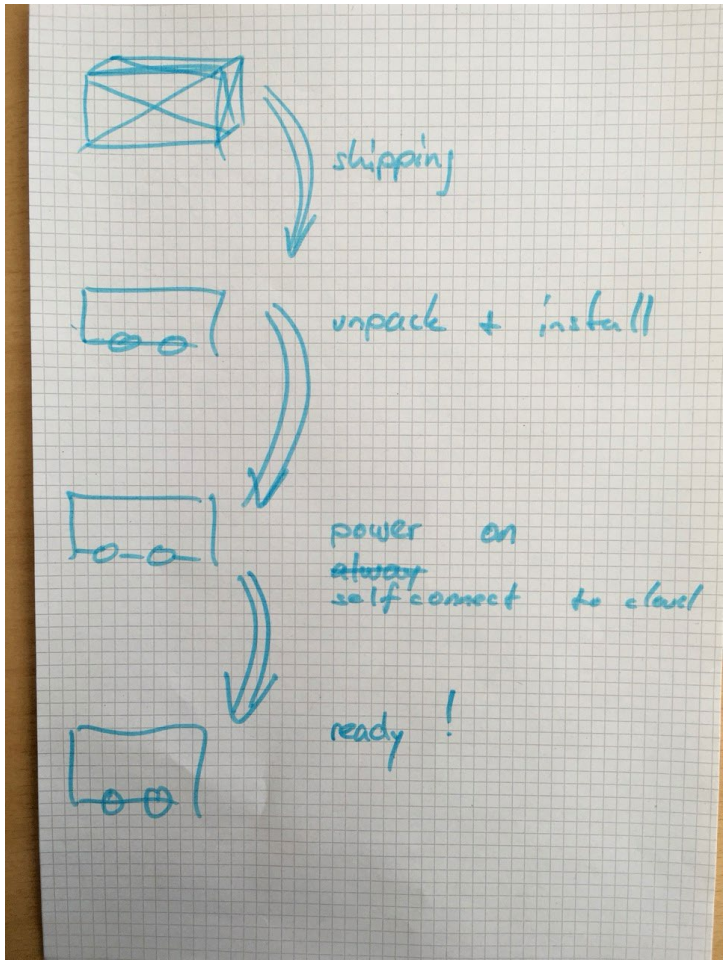
Drei Hauptmerkmale onway Lösung

1. Sinnvolle “Einschränkung” der Sicherhheitseinstellungen

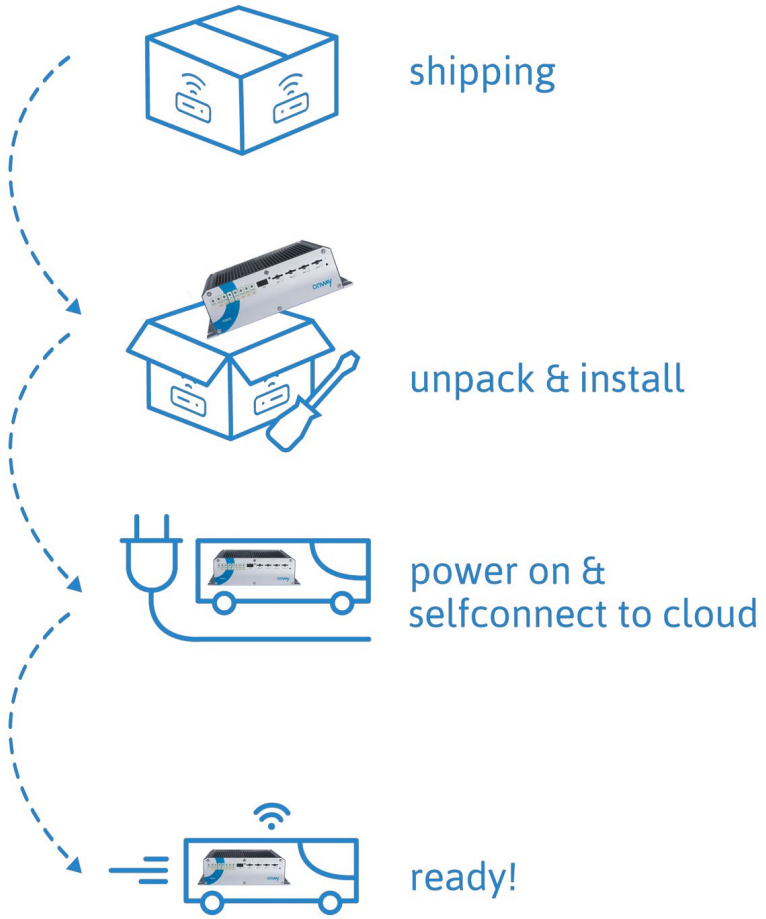
2. Sicherer “always on” Managementkanal mit State of the art cryptography

3. Einfaches Tooling mit Automatisierung und Versionierung aus dem Backend

onway mobile router



onway mobile router



Vielen Dank für Ihre Aufmerksamkeit!

Cyber Security

im Öffentlichen Verkehr

Besten Dank für Ihre Aufmerksamkeit!