Nullcon 2024 Berlin

EV Charging Stations Security
- Free Of Charge

Stephan Gerling

Senior Security Researcher ICS CERT

kaspersky

kaspersky

EV charging stations & security

free of charge

Stephan Gerling

Senior Security Researcher

Kaspersky ICS-CERT

Stephan.Gerling@Kaspersky.com

@ObiWan666

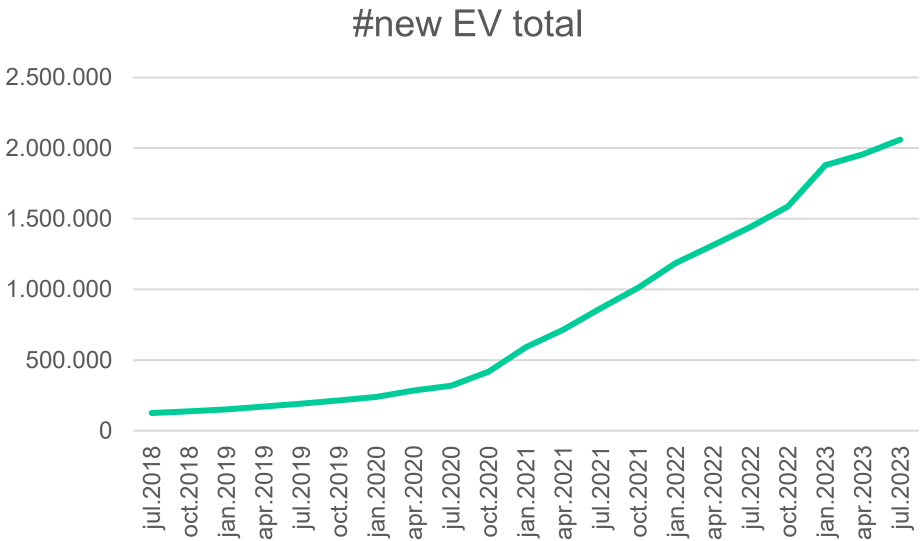
Electric mobility

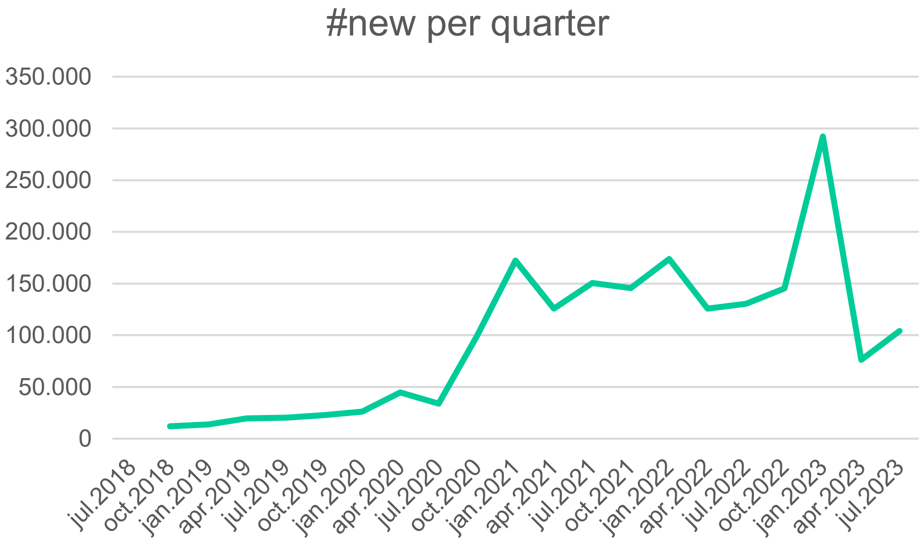
EV charging industry challenges

Electromobility

- Exponential Market Growth
- Fast Evolving Market
- Ensuring EV Drivers’ Satisfaction and Loyalty

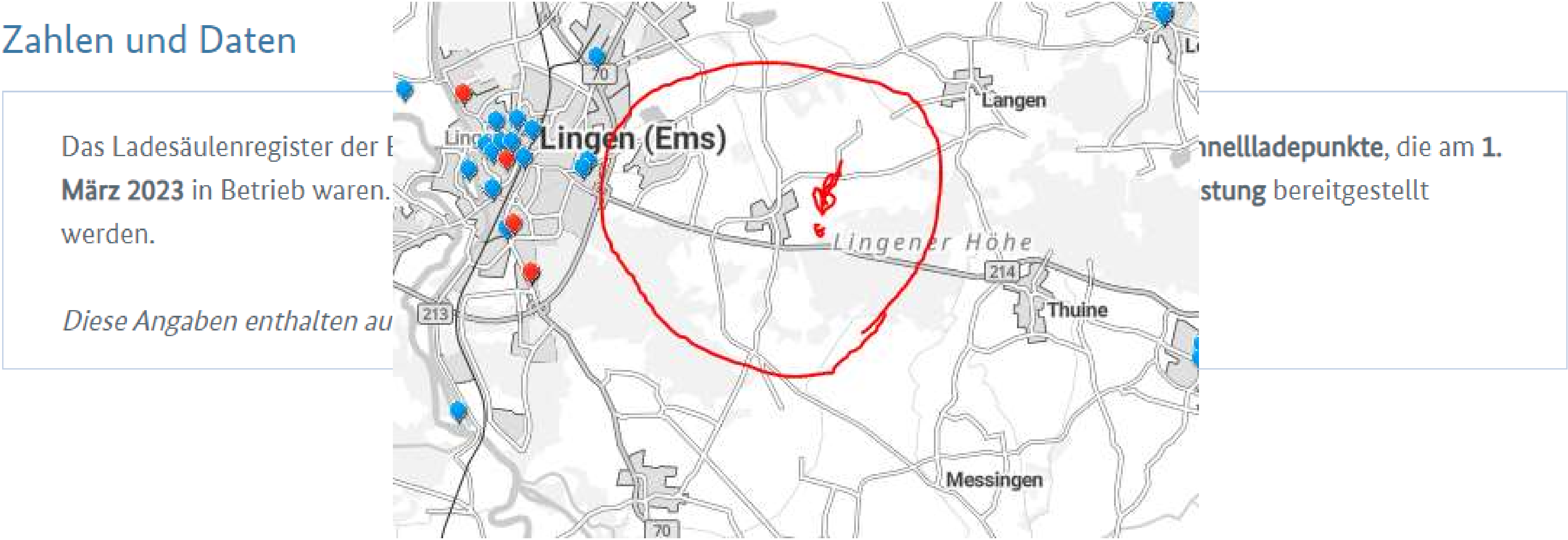
challenge #1 EV acceptance





challenge #1 charging infrastructur

“charging must be as easy as refueling”



Zahlen und Daten

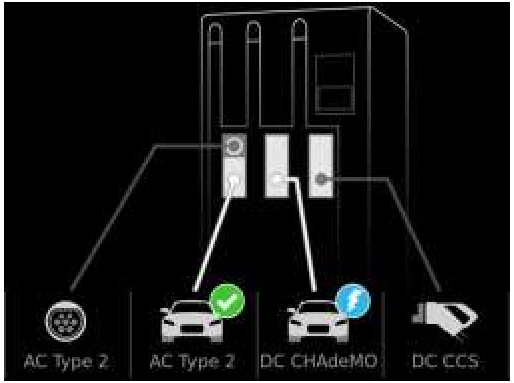
Das Ladesäulenregister der B nellladepunkte, die am 1.
März 2023 in Betrieb waren. stung bereitgestellt
werden.

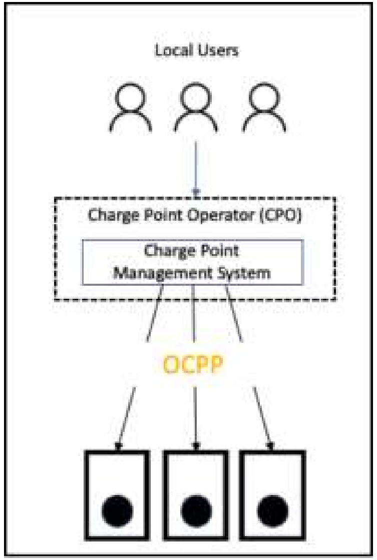
Diese Angaben enthalten au

https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/E-Mobilitaet/start.html

OCPP System architecture

- communications path between charger and Charging Station Management Systems (CSMS)
- CSMS often cloud based platform.
- communication between the charger and the CSMS is done with Web Sockets (WS), a bi-directional HTTP-like protocol.
- Secure Web Socket (WSS) are available





Open Charge Point Protocol - OCPP

One Charging station (CS) can have multiple charging points (CP)

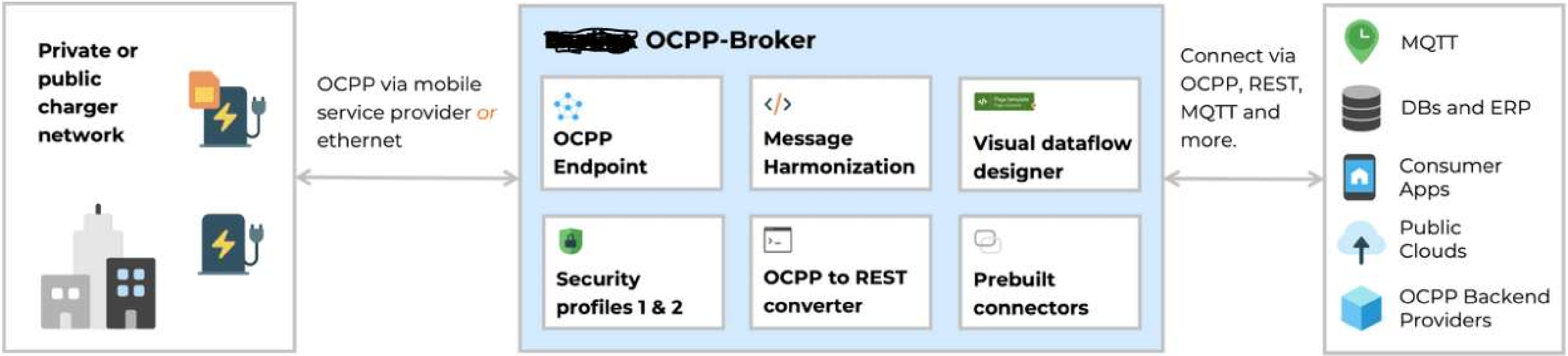
AC or DC

Minimum requirement of the German LSV (Ladesäulenverordnung) for Ad-hoc charging requires at least one of these methods (vgl. § 4 LSV)

1. Free usage or chash payment
2. Card payment or creditcard payment

• bevore 1. Juli 2023:	with cardpayment or web based paymentsystem
• after 1. Juli 2023:	via Credit- or Debit card

Open Charge Point Protocol - OCPP



Private or public charger network

OCPP via mobile service provider *or* ethernet

[redacted] **OCPP-Broker**

OCPP Endpoint

Message Harmonization

Visual dataflow designer

Security profiles 1 & 2

OCPP to REST converter

Prebuilt connectors

Connect via OCPP, REST, MQTT and more.

MQTT

DBs and ERP

Consumer Apps

Public Clouds

OCPP Backend Providers

Open Charge Point Protocol - OCPP

OCPP 1.6

OCPP 1.5

SOAP and JSON

Smart Charging support for load balancing and use of charge profiles

(Local) list management support

Additional status

Message sending requests such as CP time or status at the CP

OSCP 2.0

Communicate prediction of local available capacity for production and generation
Fitting production and generation of flexibility resources to grid capacity
Acts between Flexibility Providers and Capacity Providers
Applicable for site owners, utilities and more

OCPP 2.0.1

OCPP 1.6 plus added functionalities

Device Management

Improved Transaction handling

Added Security

Added Smart Charging functionalities

Support for ISO15118

Display and messaging support

additional improvements requested by the EV charging community

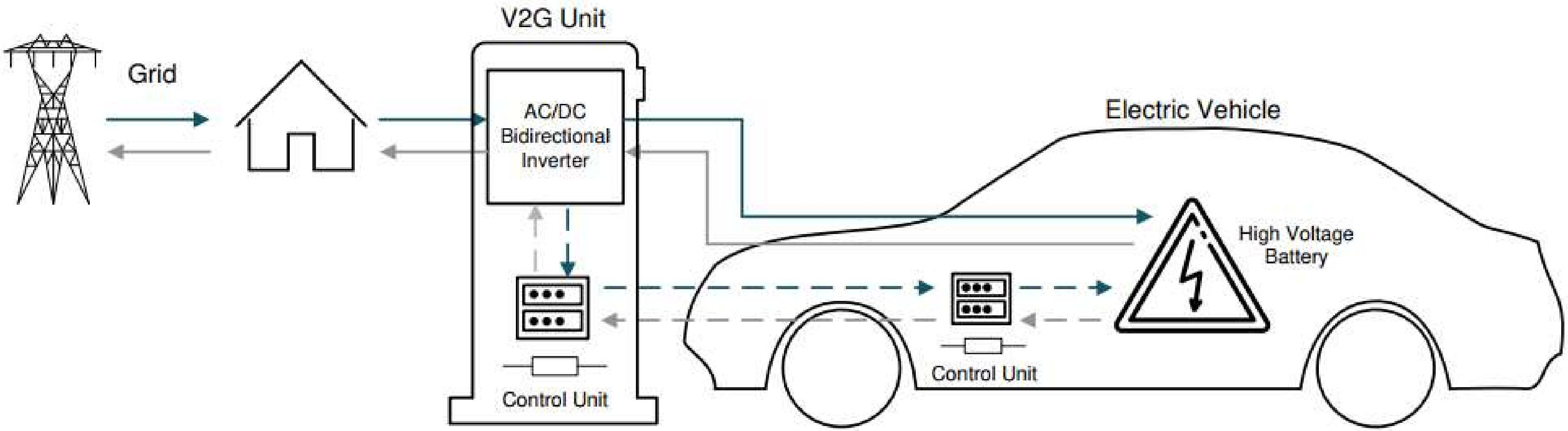
Open Charge Point Protocol - OCPP

Problem:
communication between CP and backend mostly unencrypted

Version 2.0.1 (march 2020) includes first Security Implementations

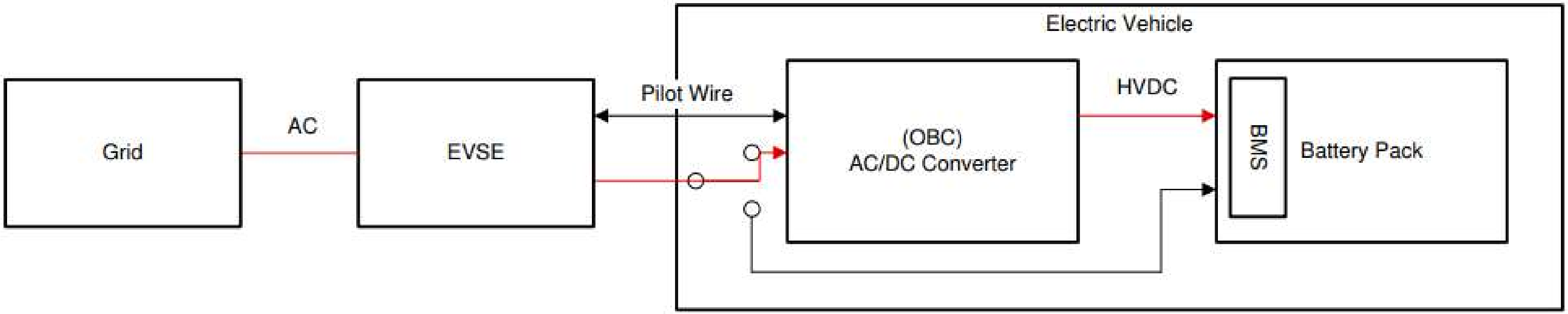
Minimum requirement still Version 1.6
Once in place, no need to upgrade to secure protocol

How works a CS ?

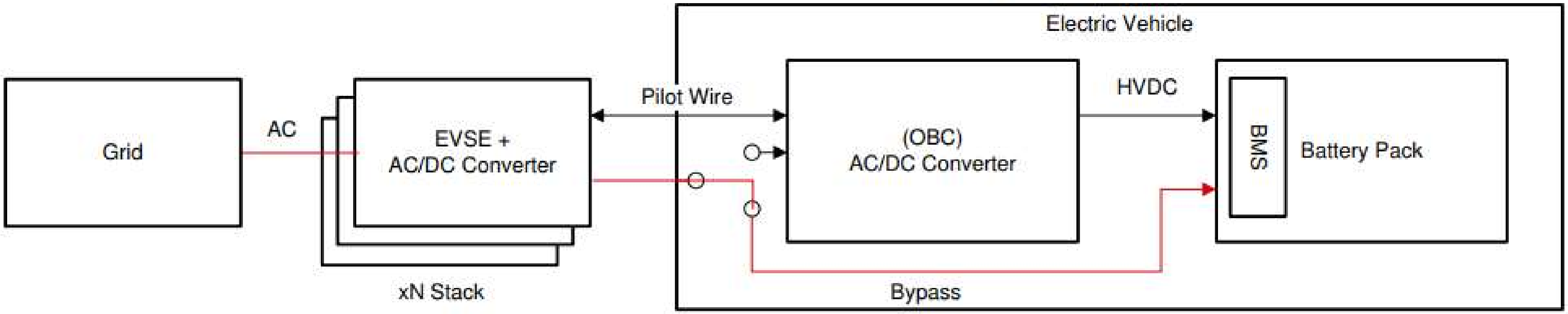


How works a CS ?

AC Charging System Power Flow

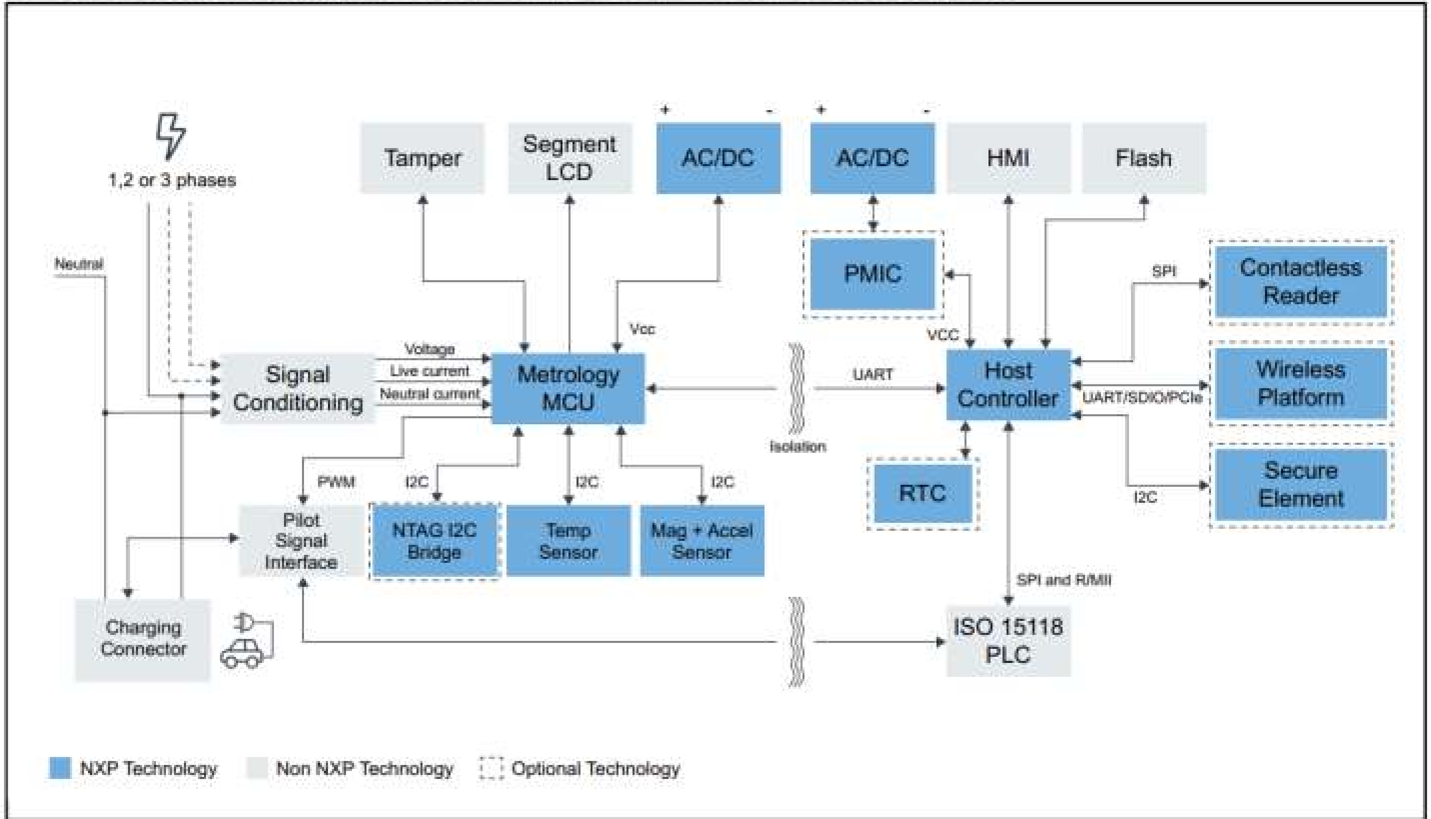


DC Charging System Power Flow



How works a CS

AC Residential Charging Station (Level 1,2 or 3) Block Diagram



Recommended Products for AC Residential Charging Station (Level 1,2 or 3)

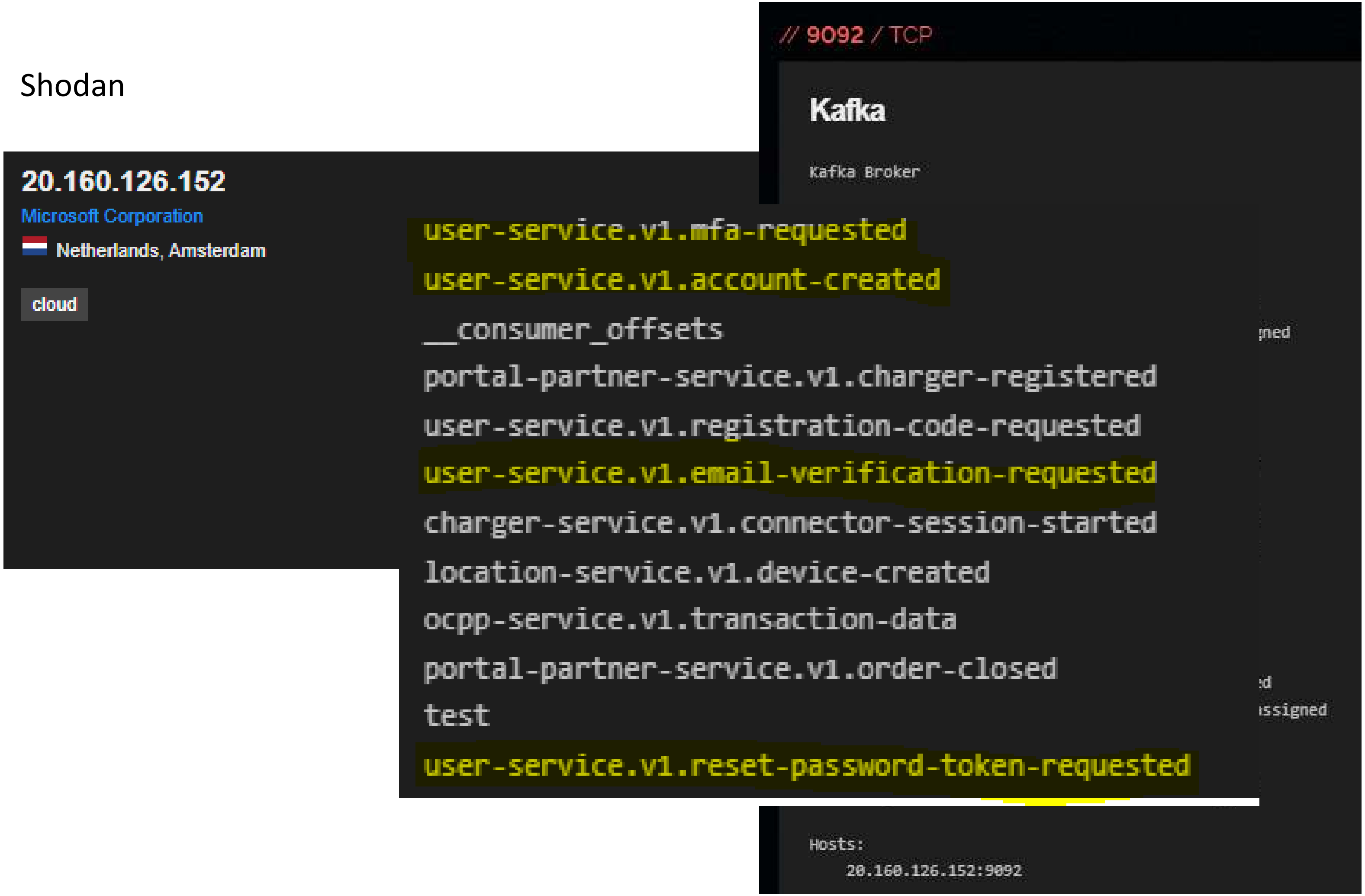
https://www.nxp.com/assets/block-diagram/en/EVChargingStation_EV-CHARGER-STATION.pdf

Wrong scope?

Charging Point:

1. Housing defined as „secure„
2. No hardened IIoT because of #1
3. No Charging card security (only UID of mifare cards used)
4. #3 still cloneable and public known since 2017
5. No encryption
6. Searchable on Shodan.IO
7. And many more

Shodan



20.160.126.152

Microsoft Corporation

Netherlands, Amsterdam

cloud

// 9092 / TCP

Kafka

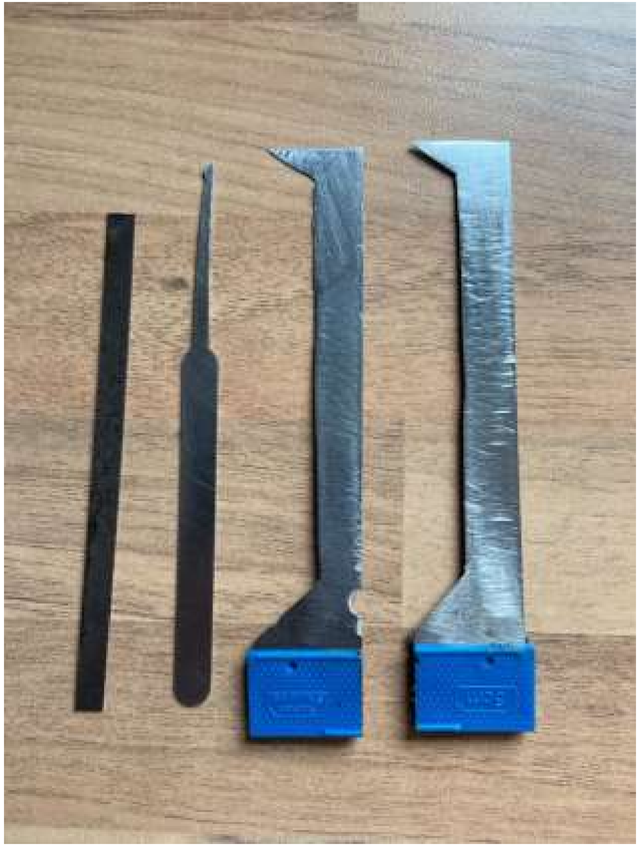
```
Kafka Broker
```

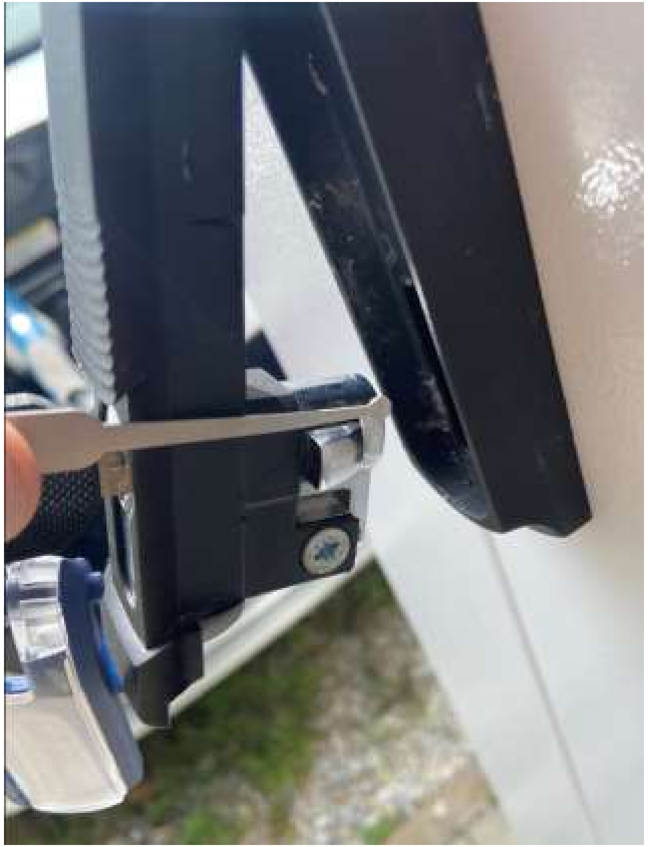
```
user-service.v1.mfa-requested
user-service.v1.account-created
__consumer_offsets
portal-partner-service.v1.charger-registered
user-service.v1.registration-code-requested
user-service.v1.email-verification-requested
charger-service.v1.connector-session-started
location-service.v1.device-created
ocpp-service.v1.transaction-data
portal-partner-service.v1.order-closed
test
user-service.v1.reset-password-token-requested
```

```
ned
d
ssigned
```

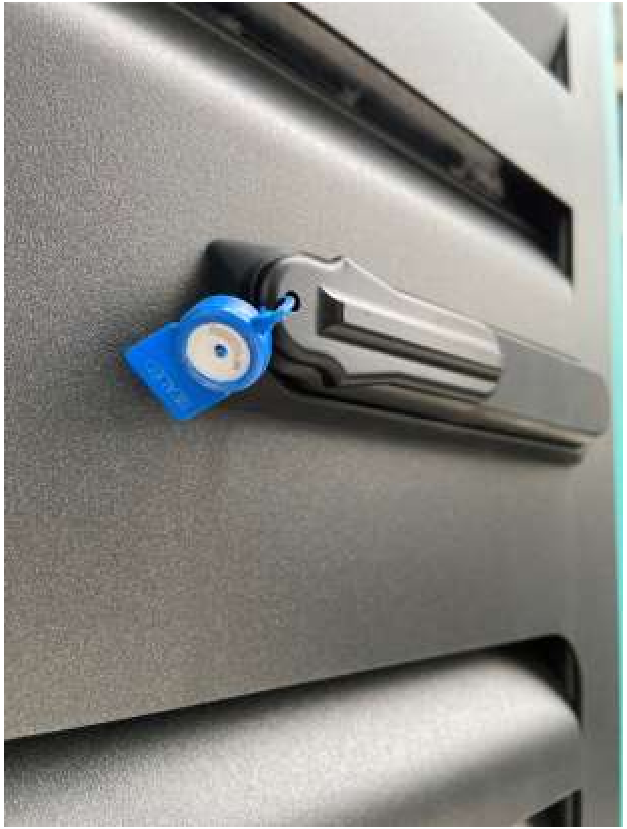
```
Hosts:
    20.160.126.152:9092
```

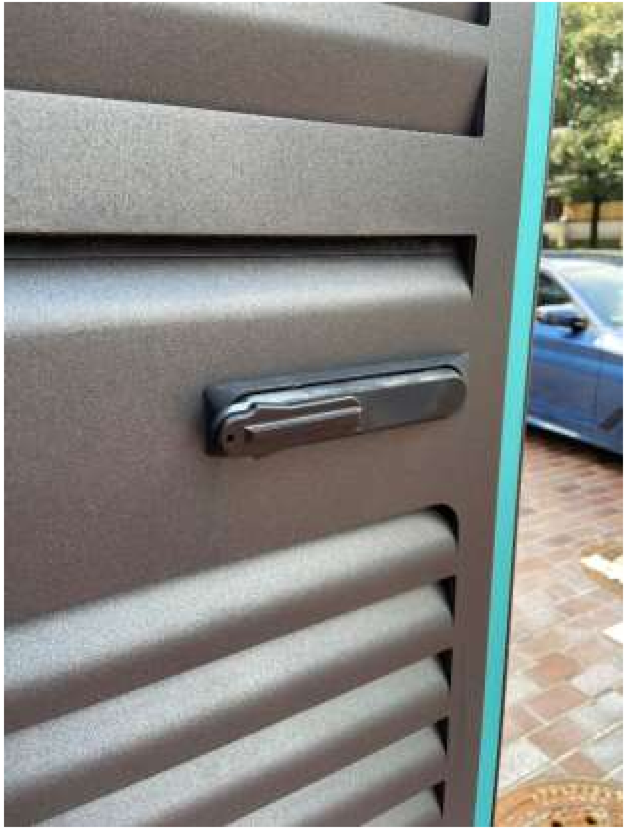
Physical Security fail





Physical Security fail #2





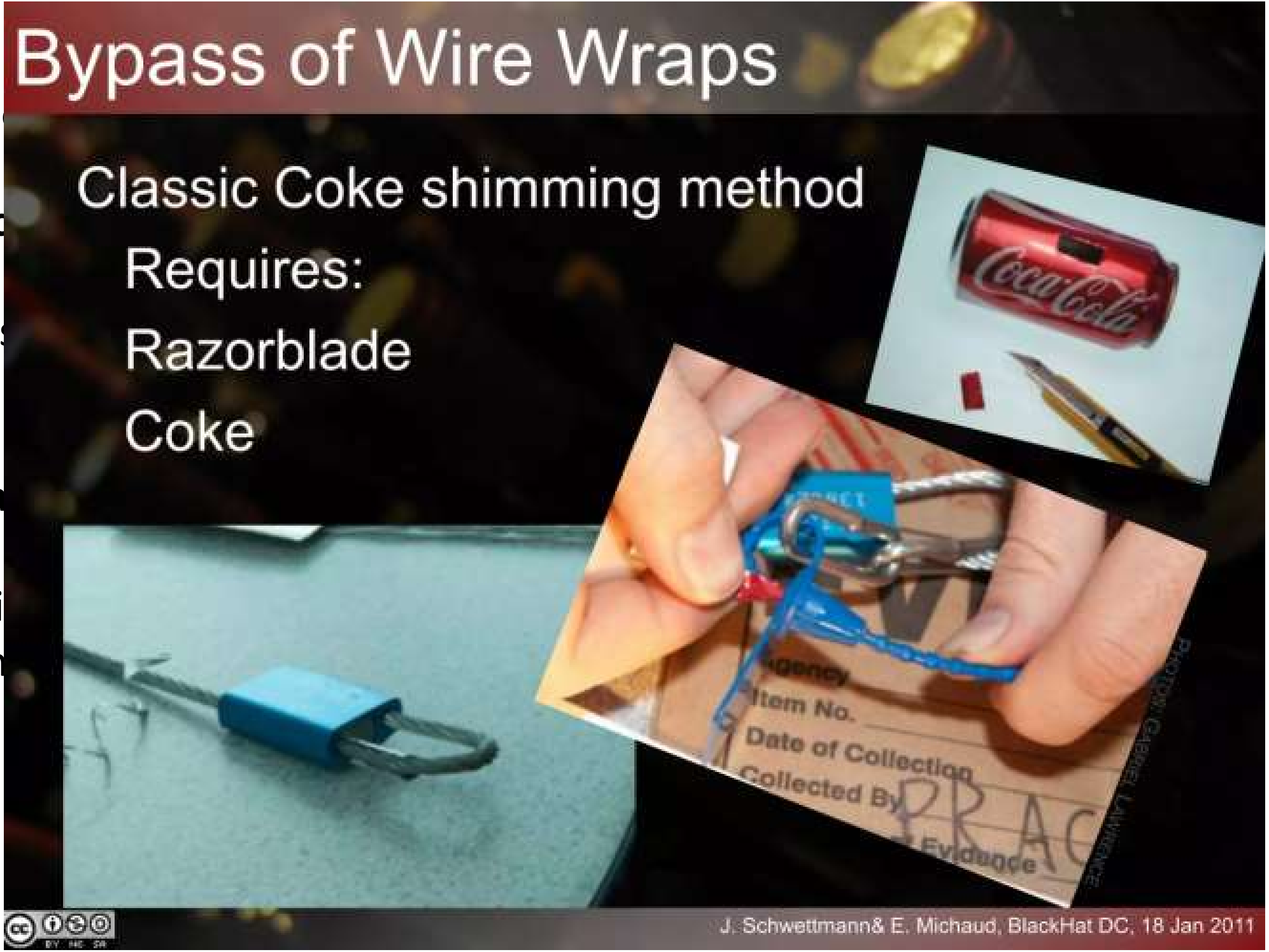
How to bypass the se

Why Use Sec

Security seal
of entry.

How to bypa

Shimming wi
other thechn



Bypass of Wire Wraps

Classic Coke shimming method

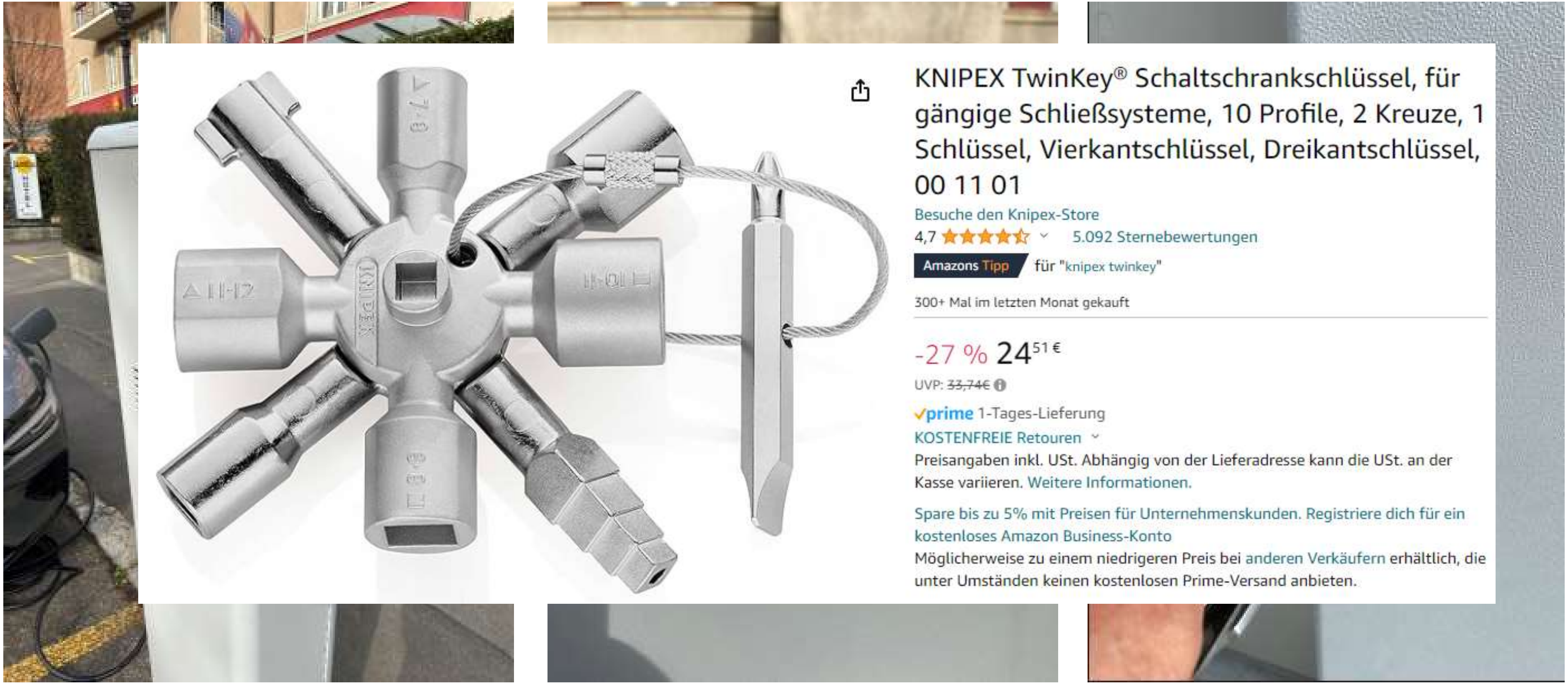
Requires:

Razorblade

Coke

J. Schwettmann& E. Michaud, BlackHat DC, 18 Jan 2011

A Swiss Charging Station



KNIPEX TwinKey® Schaltschrankschlüssel, für gängige Schließsysteme, 10 Profile, 2 Kreuze, 1 Schlüssel, Vierkantschlüssel, Dreikantschlüssel, 00 11 01

Besuche den Knipex-Store

4,7 ★★★★☆ 5.092 Sternebewertungen

Amazons Tipp für "knipex twinkey"

300+ Mal im letzten Monat gekauft

-27 % 24⁵¹ €

UVP: ~~33,74€~~

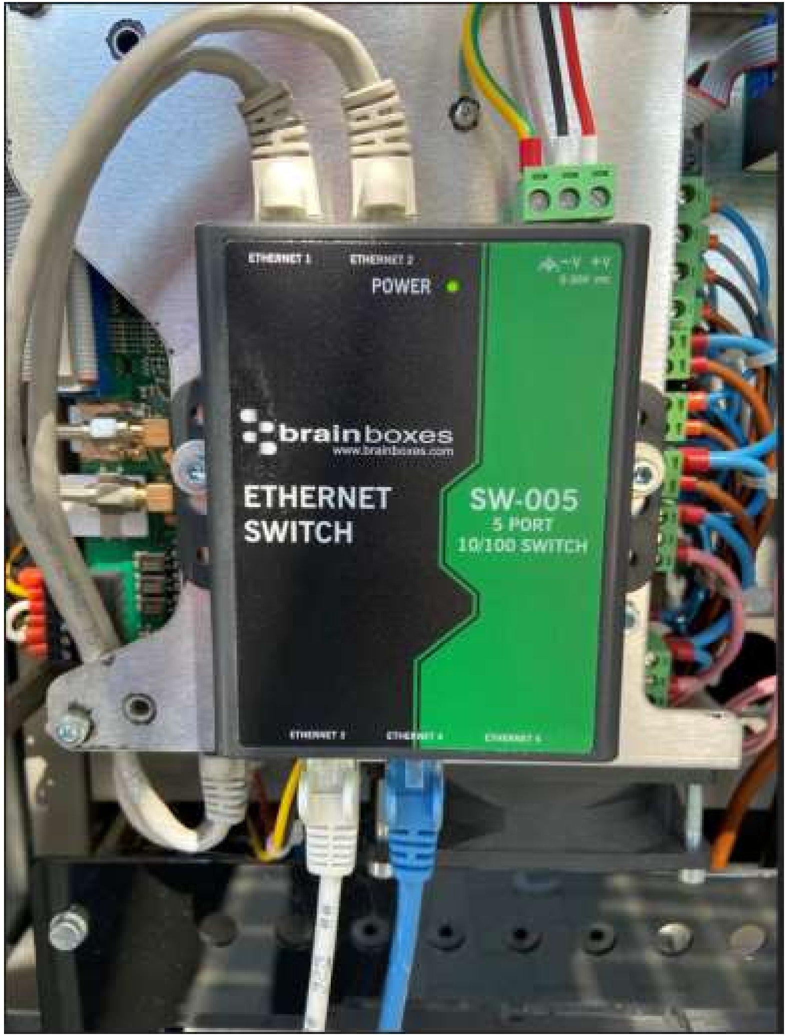
✓prime 1-Tages-Lieferung

KOSTENFREIE Retouren

Preisangaben inkl. USt. Abhängig von der Lieferadresse kann die USt. an der Kasse variieren. Weitere Informationen.

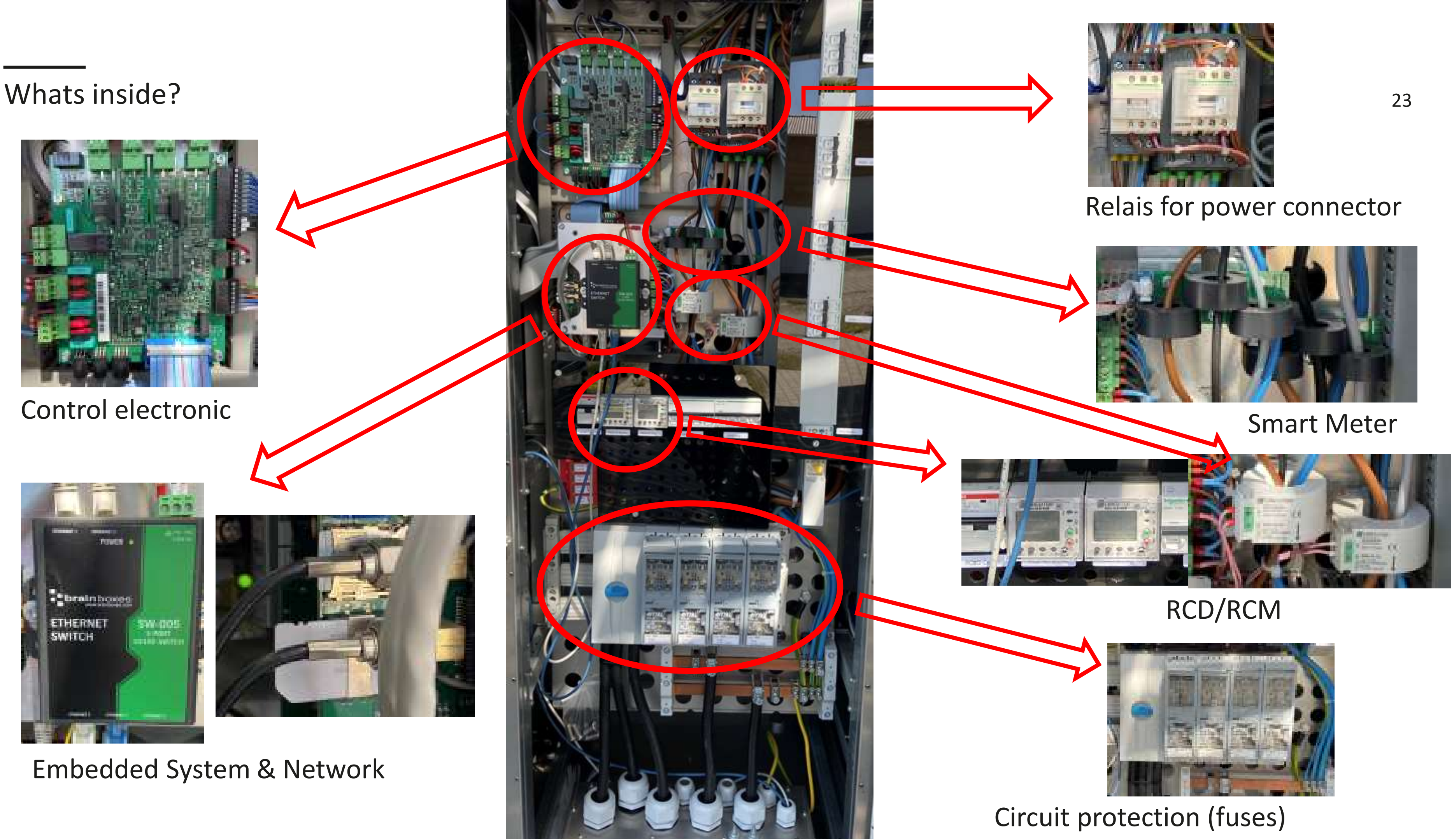
Spare bis zu 5% mit Preisen für Unternehmenskunden. Registriere dich für ein kostenloses Amazon Business-Konto

Möglicherweise zu einem niedrigeren Preis bei anderen Verkäufern erhältlich, die unter Umständen keinen kostenlosen Prime-Versand anbieten.


ETHERNET 1
ETHERNET 2
POWER
-V +V
5-30V DC
brainboxes
www.brainboxes.com
ETHERNET
SWITCH
SW-005
5 PORT
10/100 SWITCH
ETHERNET 3
ETHERNET 4
ETHERNET 5

POWER
brainboxes
ETHERNET
SWITCH
SW-005
5 PORT
10/100 SWITCH

Whats inside?



Control electronic

Embedded System & Network

Relais for power connector

Smart Meter

RCD/RCM

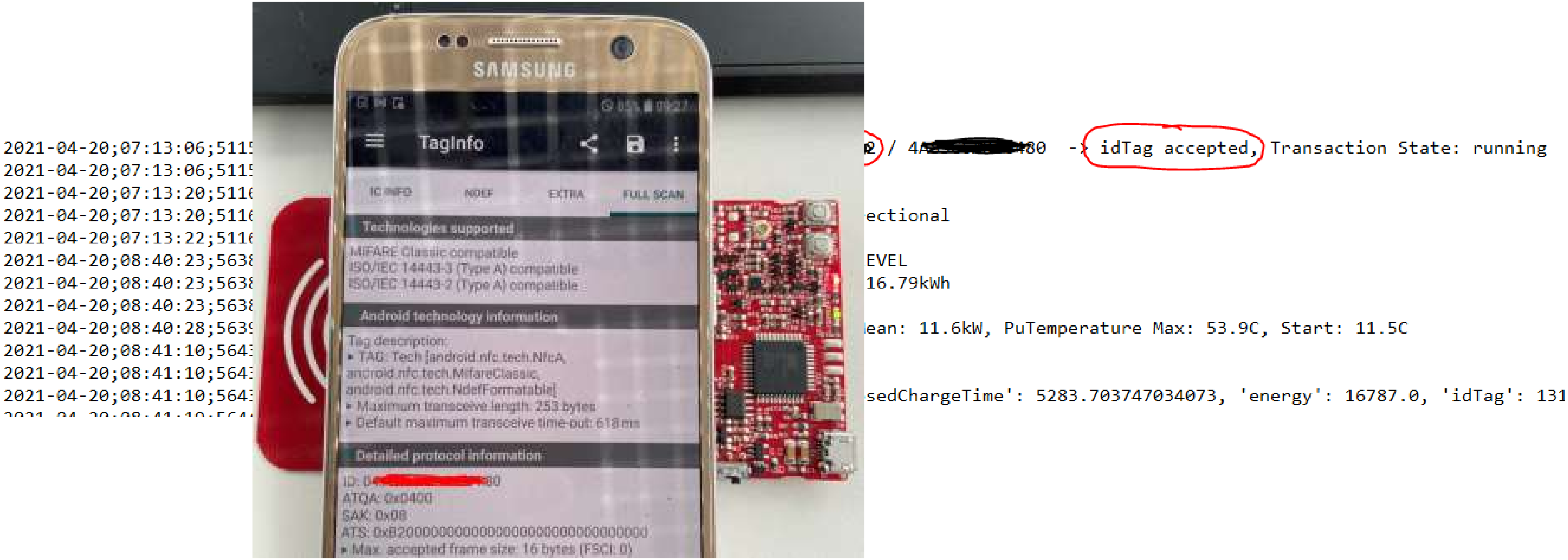
Circuit protection (fuses)

(un)secure charging cards

Charging Cards

- Mifare classic
- Only UID used
- Easy to clone
- Public known since 2017
- Nothing changed

Cloning the Charging Card



```
2021-04-20;07:13:06;511                                                  2 / 4A[redacted]80  -> idTag accepted, Transaction State: running
2021-04-20;07:13:06;511
2021-04-20;07:13:20;511
2021-04-20;07:13:20;511                                                  ectional
2021-04-20;07:13:22;511
2021-04-20;08:40:23;563                                                  EVEL
2021-04-20;08:40:23;563                                                  16.79kWh
2021-04-20;08:40:23;563
2021-04-20;08:40:28;563                                                  ean: 11.6kW, PuTemperature Max: 53.9C, Start: 11.5C
2021-04-20;08:41:10;564
2021-04-20;08:41:10;564
2021-04-20;08:41:10;564                                                  sedChargeTime': 5283.703747034073, 'energy': 16787.0, 'idTag': 131
```

Technologies supported

MIFARE Classic compatible
ISO/IEC 14443-3 (Type A) compatible
ISO/IEC 14443-2 (Type A) compatible

Android technology information

Tag description:
- TAG: Tech [android.nfc.tech.NfcA, android.nfc.tech.MifareClassic, android.nfc.tech.NdefFormatable]
- Maximum transceive length: 253 bytes
- Default maximum transceive time-out: 618 ms

Detailed protocol information

ID: 0[redacted]80
ATQA: 0x0400
SAK: 0x08
ATS: 0xB2000000000000000000000000000000
- Max. accepted frame size: 16 bytes (FSCI: 0)

Cloning the Charging Card

Vulnerabilities **KLCERT-21-227**

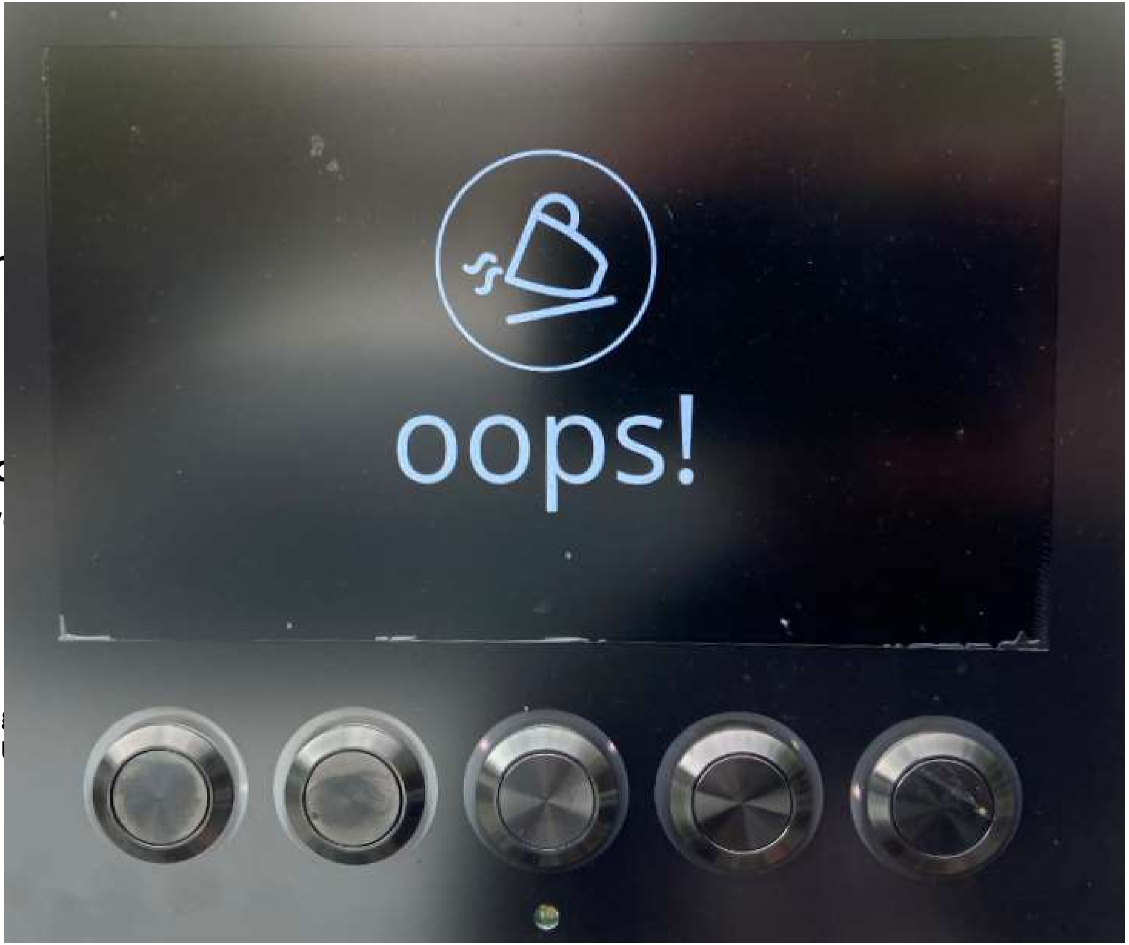
EVTEC espresso&ch

Denial of Service

denial of Service pc

- **nmap aggressive electronic with**
- **Network paket**

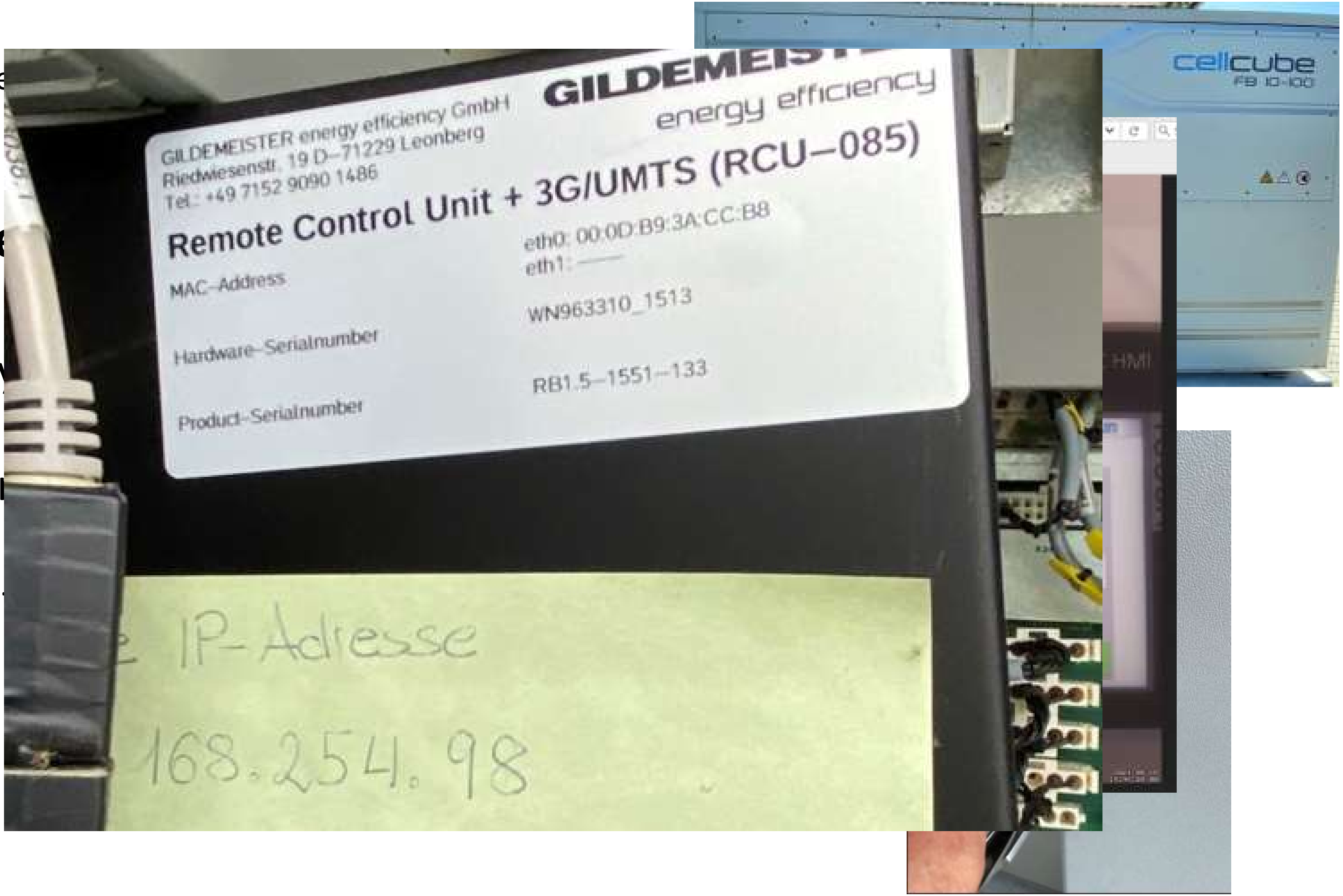
CVSS:3.1 Base score: 7.3 (hi
CVSS:3.1/AV:A/AC:L/PR:N/



Public accessable

Batte

- Phy
- Re
- Ne
- Un



GILDEMEISTER energy efficiency GmbH
Riedwiesenstr. 19 D–71229 Leonberg
Tel.: +49 7152 9090 1486

GILDEMEISTER
energy efficiency

Remote Control Unit + 3G/UMTS (RCU–085)

MAC–Address eth0: 00:0D:B9:3A:CC:B8
eth1: ——

Hardware–Serialnumber WN963310_1513

Product–Serialnumber RB1.5–1551–133

e IP-Adresse
168.254.98

Vulnerabilities **KLCERT-21-228**

EVTEC espresso&charge 4 in 1 EV charging Station

No authentication required to access log files, (log files accessible for public)

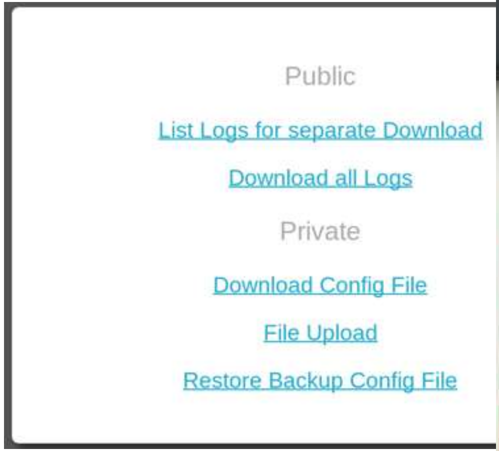
log files accessible for public
http://ip.address.of.charginstation:8888/cgi-bin/public/list-logs

log files contains juicy information's accessible for everyone
List of public readable log files:

> **ACEnergyMeterPlug2.log (105 KB)**
> **………**

CVSS:3.1 Base score: 6.5 (medium)
CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Wrong security decision



Public

List Logs for separate Download

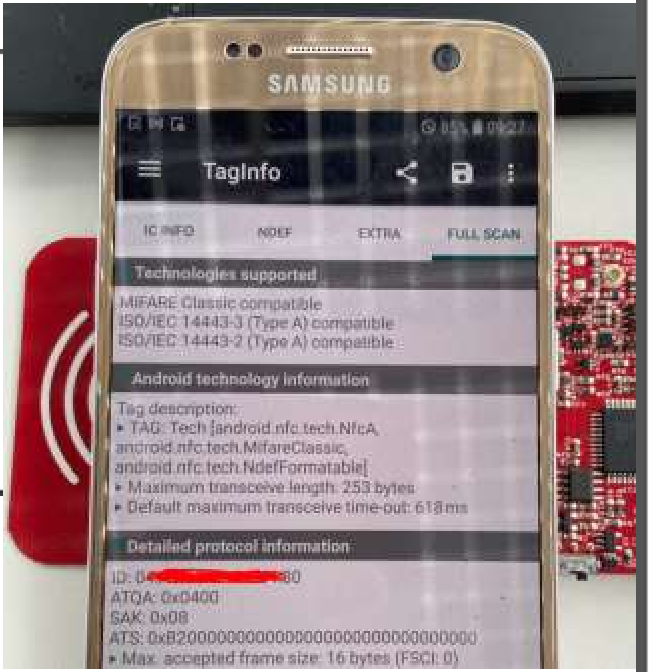
Download all Logs

Private

Download Config File

File Upload

Restore Backup Config File



TagInfo

IC INFO | NDEF | EXTRA | FULL SCAN

Technologies supported

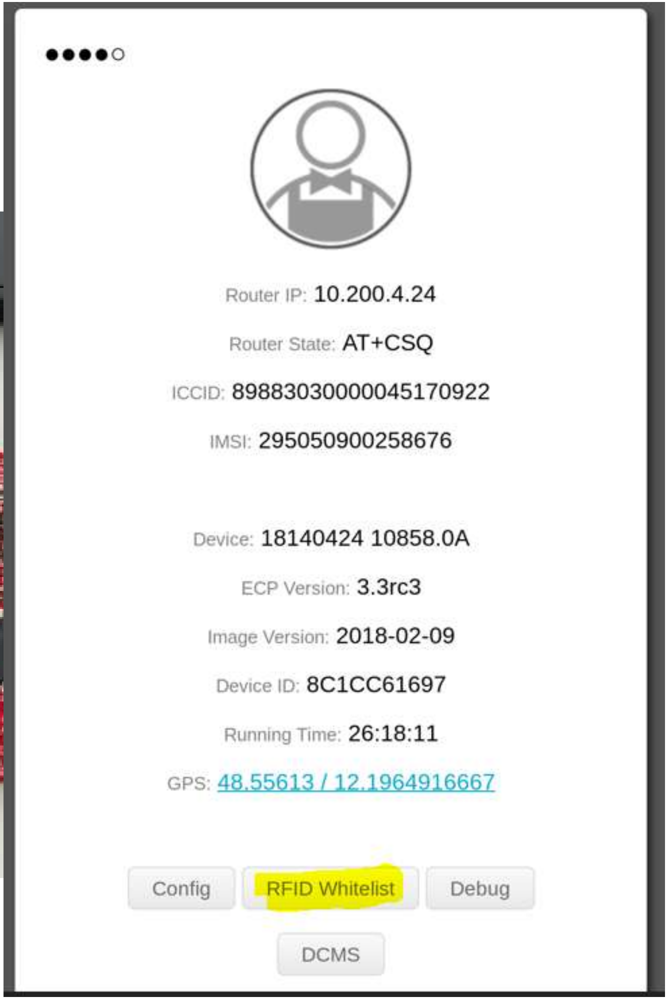
MIFARE Classic compatible
ISO/IEC 14443-3 (Type A) compatible
ISO/IEC 14443-2 (Type A) compatible

Android technology information

Tag description:
- TAG: Tech [android.nfc.tech.NfcA, android.nfc.tech.MifareClassic, android.nfc.tech.NdefFormatable]
- Maximum transceive length: 253 bytes
- Default maximum transceive time-out: 618 ms

Detailed protocol information

ID: [redacted]
ATQA: 0x0400
SAK: 0x08
ATS: 0x82000000000000000000000000000000
- Max. accepted frame size: 16 bytes (FSCI: 0)



●●●●○

Router IP: 10.200.4.24

Router State: AT+CSQ

ICCID: 89883030000045170922

IMSI: 295050900258676

Device: 18140424 10858.0A

ECP Version: 3.3rc3

Image Version: 2018-02-09

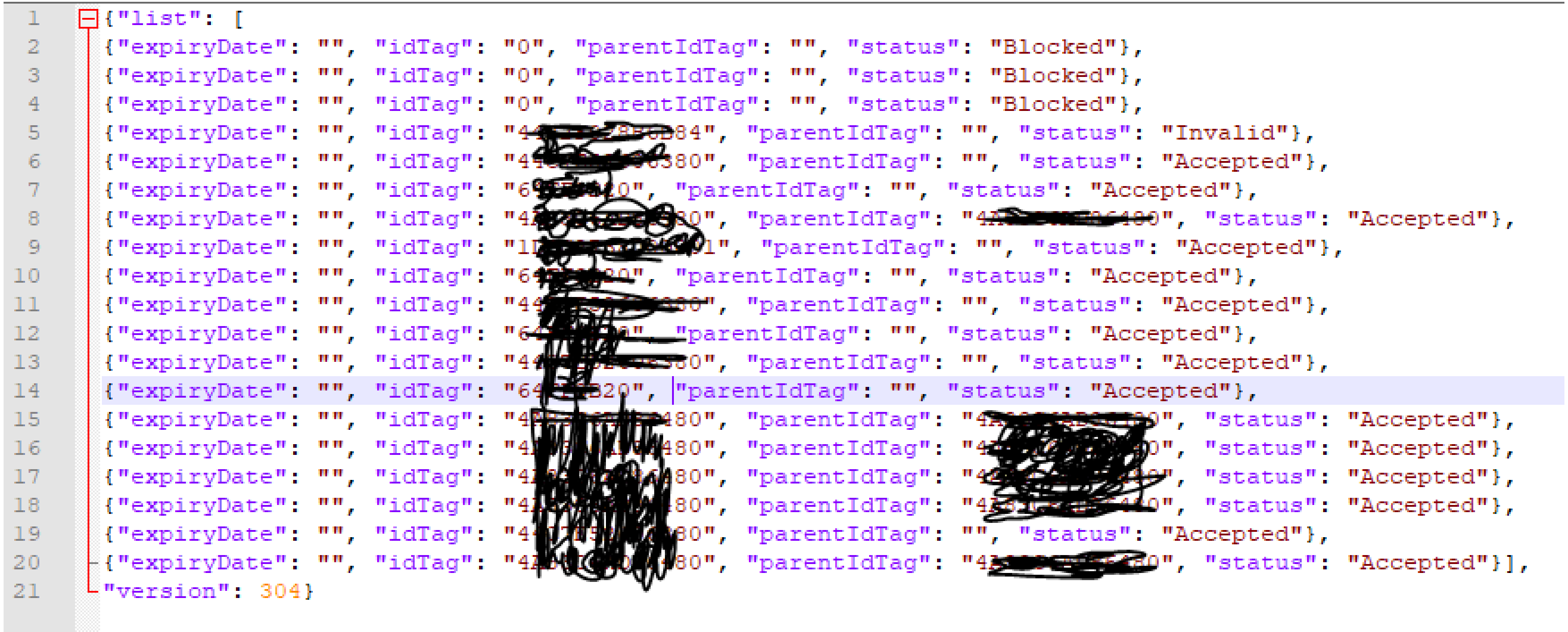
Device ID: 8C1CC61697

Running Time: 26:18:11

GPS: 48.55613 / 12.1964916667

Vulnerabilities **KLCERT-21-229**

EVTEC espresso&charge 4 in 1 EV charging Station



```
{"list": [
{"expiryDate": "", "idTag": "0", "parentIdTag": "", "status": "Blocked"},
{"expiryDate": "", "idTag": "0", "parentIdTag": "", "status": "Blocked"},
{"expiryDate": "", "idTag": "0", "parentIdTag": "", "status": "Blocked"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "", "status": "Invalid"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "", "status": "Accepted"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "", "status": "Accepted"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "[redacted]", "status": "Accepted"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "", "status": "Accepted"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "", "status": "Accepted"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "", "status": "Accepted"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "", "status": "Accepted"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "", "status": "Accepted"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "", "status": "Accepted"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "[redacted]", "status": "Accepted"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "[redacted]", "status": "Accepted"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "[redacted]", "status": "Accepted"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "[redacted]", "status": "Accepted"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "", "status": "Accepted"},
{"expiryDate": "", "idTag": "[redacted]", "parentIdTag": "[redacted]", "status": "Accepted"}],
"version": 304}
```

Vulnerabilities **KLCERT-21-230**

EVTEC espresso&charge 4 in 1 EV charging Station
Payment cards (RFID card) are clone able

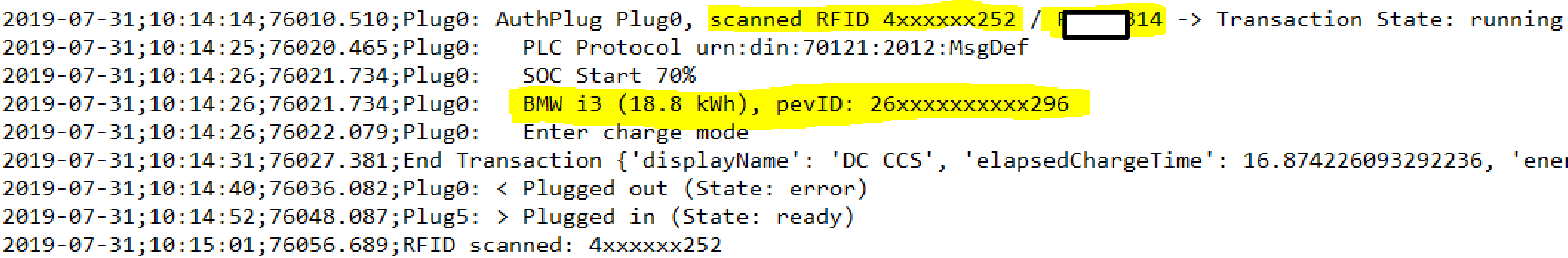
KLCERT-21-229 shows several ways to get an valid UID of an RFID payment card for the EV charging station.

Mifare Classic 1k RFID cards are used for the authentication and payment at the charging station.

Forensic Artefacts

Many usefully artefacts can be found during an analyze of charging point

- **UID of used payment card is logged**
- **pevID of the Car and Car Model**



```
2019-07-31;10:14:14;76010.510;Plug0: AuthPlug Plug0, scanned RFID 4xxxxxx252 / [redacted]314 -> Transaction State: running
2019-07-31;10:14:25;76020.465;Plug0:   PLC Protocol urn:din:70121:2012:MsgDef
2019-07-31;10:14:26;76021.734;Plug0:   SOC Start 70%
2019-07-31;10:14:26;76021.734;Plug0:   BMW i3 (18.8 kWh), pevID: 26xxxxxxxxxx296
2019-07-31;10:14:26;76022.079;Plug0:   Enter charge mode
2019-07-31;10:14:31;76027.381;End Transaction {'displayName': 'DC CCS', 'elapsedChargeTime': 16.874226093292236, 'ener
2019-07-31;10:14:40;76036.082;Plug0: < Plugged out (State: error)
2019-07-31;10:14:52;76048.087;Plug5: > Plugged in (State: ready)
2019-07-31;10:15:01;76056.689;RFID scanned: 4xxxxxx252
```

Thank you !

Stephan Gerling

Senior Security Researcher
Kaspersky ICS-CERT
Stephan.Gerling@Kaspersky.com

@obiwan666