Threats to electric mobility and how to establish trust

Prof. Dr. Christoph Krauß
INCYDE GmbH
Darmstadt University of Applied Sciences HDA

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

04.11.2021
Virtual OpenS3 Workshop

INCYDE GmbH

Experience and Knowledge

- Risk analysis, measure definition, planning, realisation
- Security appraisals
- IEC 62443, TS 50701, ISO 27001, ISO/SAE 21434, ISO 15118, AUTOSAR
- Rail – Automotive – Industry – Energy
- International cooperation and projects
- Security research projects

Employee profiles

- Practitioners / Experts
- Security Specialists
- Audit Experienced
- Consultants
- Researcher

Founders

- Dipl. Ing. (FH) Max Schubert, Managing director
- Prof. Dr. Stefan Katzenbeisser, Head of Railway Security Research, Appraiser
- Prof. Dr. Christoph Krauß, Head of Automotive Security Research
- NEXTRAIL GmbH, Railway experts

Our Services

- Security strategy and standardization
- Threat and risk analysis
- Test planning and accomplishment
- Appraisal of security concepts, measures, and implementations against prTS 50701, IEC 62443 and ISO 27001
- Security and awareness training
- Migration solutions and strategies
- Security management definition and implementation
- Security solution concepts
- Academic network
- Standardisation
- Research projects

Locations

- Berlin
- Frankfurt / Main
- Munich
- Leipzig

Applied Cyber Security Darmstadt

INCYDE

- Research group at Darmstadt University of Applied Sciences HDA
- Headed by
  - Prof. Dr. Christoph Krauß
  - Prof. Dr. Alexander Wiesmaier
- Research Topics
  - Automotive Security
  - Network Security
  - Formal Protocol Analysis
  - Cryptography with focus on post-quantum cryptography

acsd applied cyber security darmstadt

h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES

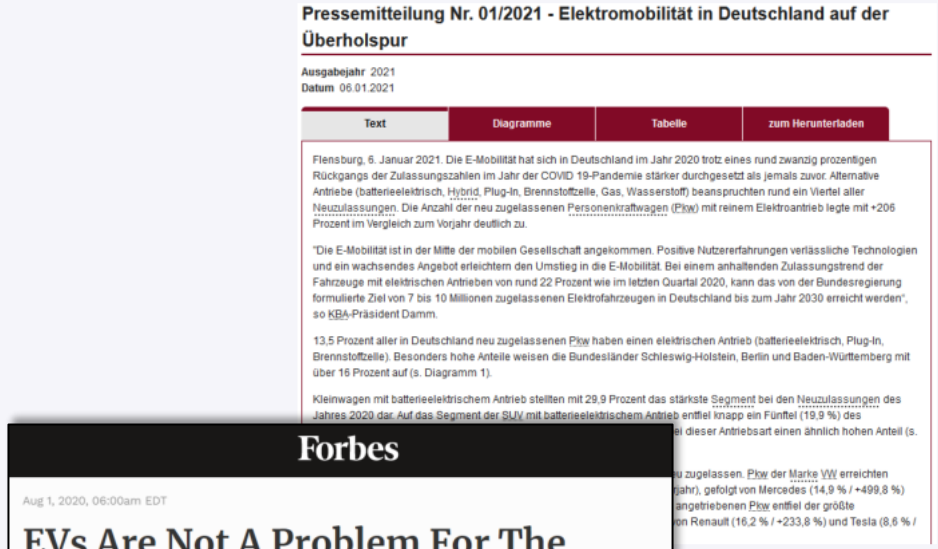
ACSD Automotive Security Team

Introduction

Motivation

- E-Mobility is an important technology for reducing emissions
- E-Mobility in the fast lane
  - In 2020, the number of newly registered electric vehicles (EV) in Germany increased by +206 percent
  - Target of 7 to 10 million registered EVs in Germany can be achieved by 2030
- Future EVs will drive autonomously and charge themselves
- Requires smart charging
  - Satisfy user requirements
  - Demand response and load management
  - Vehicle-to-Grid (V2G)

➔ Information and communication technology (ICT) required



Pressemitteilung Nr. 01/2021 - Elektromobilität in Deutschland auf der Überholspur

Ausgabejahr 2021
Datum 06.01.2021

Text | Diagramme | Tabelle | zum Herunterladen

Flensburg, 6. Januar 2021. Die E-Mobilität hat sich in Deutschland im Jahr 2020 trotz eines rund zwanzig prozentigen Rückgangs der Zulassungszahlen im Jahr der COVID 19-Pandemie stärker durchgesetzt als jemals zuvor. Alternative Antriebe (batterieelektrisch, Hybrid, Plug-In, Brennstoffzelle, Gas, Wasserstoff) beanspruchten rund ein Viertel aller Neuzulassungen. Die Anzahl der neu zugelassenen Personenkraftwagen (Pkw) mit reinem Elektroantrieb legte mit +206 Prozent im Vergleich zum Vorjahr deutlich zu.

"Die E-Mobilität ist in der Mitte der mobilen Gesellschaft angekommen. Positive Nutzererfahrungen verlässliche Technologien und ein wachsendes Angebot erleichtern den Umstieg in die E-Mobilität. Bei einem anhaltenden Zulassungstrend der Fahrzeuge mit elektrischen Antrieben von rund 22 Prozent wie im letzten Quartal 2020, kann das von der Bundesregierung formulierte Ziel von 7 bis 10 Millionen zugelassenen Elektrofahrzeugen in Deutschland bis zum Jahr 2030 erreicht werden", so KBA-Präsident Damm.

13,5 Prozent aller in Deutschland neu zugelassenen Pkw haben einen elektrischen Antrieb (batterieelektrisch, Plug-In, Brennstoffzelle). Besonders hohe Anteile weisen die Bundesländer Schleswig-Holstein, Berlin und Baden-Württemberg mit über 16 Prozent auf (s. Diagramm 1).

Kleinwagen mit batterieelektrischem Antrieb stellten mit 29,9 Prozent das stärkste Segment bei den Neuzulassungen des Jahres 2020 dar. Auf das Segment der SUV mit batterieelektrischem Antrieb entfiel knapp ein Fünftel (19,9 %) des

Source: https://www.kba.de/DE/Presse/Pressemitteilungen/2021/Allgemein/pm01_2021_E_Antrieb.html

Forbes

Aug 1, 2020, 06:00am EDT

EVs Are Not A Problem For The Electric Grid, They Are The Solution

James Morris Contributor
Transportation
I write about the rapidly growing world of electric vehicles

One of the stock arguments you will hear against the wide adoption of electric vehicles is about how the power supply grid is going to cope with all these high-voltage devices drawing current to recharge. A home EV charging station will require somewhere between 2kW and 7kW when it is replenishing a car battery. If all EVs are plugged in at once, surely the grid will collapse and power stations will be overextended? Dogs and cats will live together, and mass hysteria will break out? But not only is this a complete misunderstanding of EV charging habits, it could be getting things completely the wrong way round. Here's why.

Source: https://www.forbes.com/sites/jamesmorris/2020/08/01/evs-are-not-a-problem-for-the-electric-grid-they-are-the-solution/

Problem

- New security and privacy threats arise
  - Safety-adverse effects
  - Financial damage
  - Privacy loss

Source: https://insideevs.com/news/423581/severe-electric-car-fire-explosion-charging/

- Current protocols and standards require improvements
  - Insufficient (or sometimes no) security
  - No cryptographic agility
  - No verification of the trustworthiness of a system
  - No privacy protection
  - …

Forbes

As More EVs Hit The Road, Blackouts Become Likely

Members of the Energy Practice at Oliver Wyman

Source: https://www.forbes.com/sites/oliverwyman/2019/05/15/as-more-evs-hit-the-road-blackouts-become-likely/?sh=628ea8f9dc30

Chaos Computer Club hacks e-motor charging stations

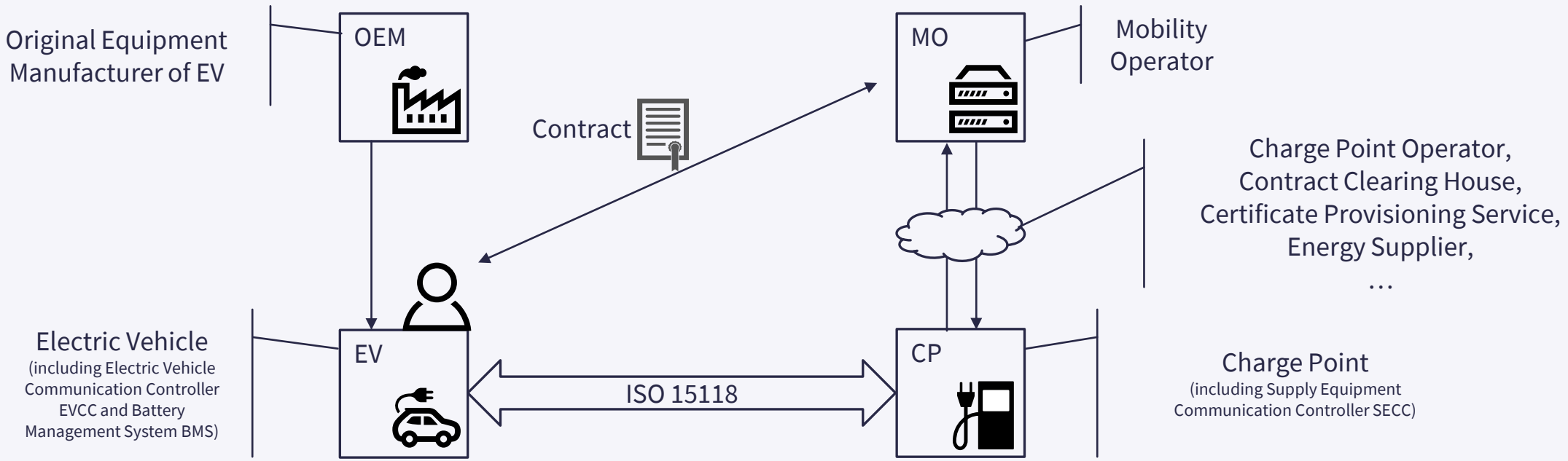
2017-12-27 00:43:00, 46halbe

Currently, the infrastructure for charging electronic vehicles is rolled out in Germany – once again without paying much attention to IT security. The convenient charging cards are currently so insecure that it is not advisable to use them. It is trivially possible to charge your car while having someone else unknowingly being forced to pay. Nearly all charging cards are affected by this vulnerability. Charging network providers that issue these cards have refused to fix the security problems, despite being given several months pre-warning. The details of the vulnerabilities will be presented in detail today at the 34th Chaos Communication Congress at 12:45 in Leipzig.

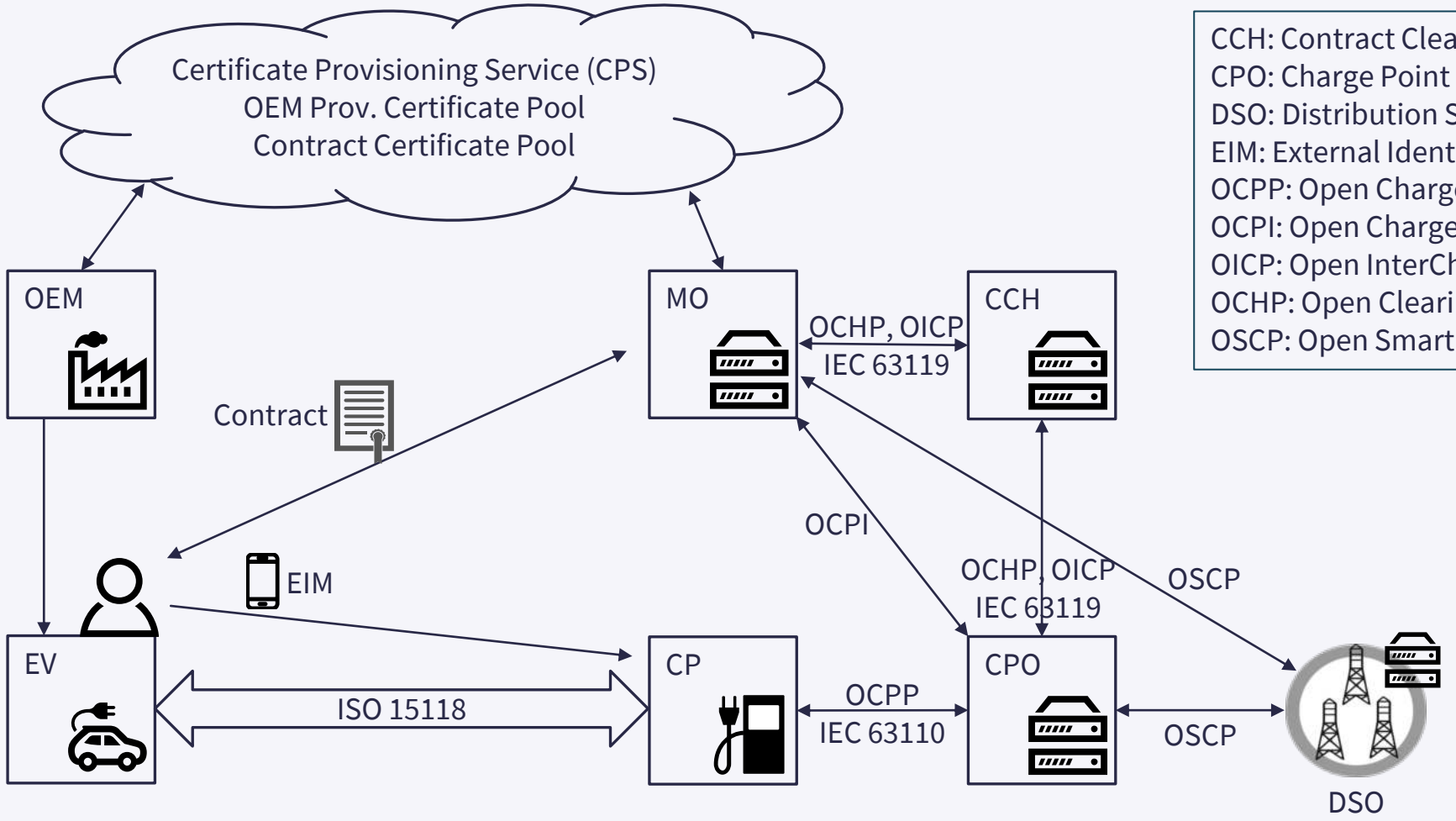
Source: http://ccc.de/en/updates/2017/e-motor

Current State of the Art

E-Mobility Charging Architecture (simplified)



E-Mobility Charging Architecture (more details)



CCH: Contract Clearing House
CPO: Charge Point Operator
DSO: Distribution System Operator
EIM: External Identification Means
OCPP: Open Charge Point Protocol
OCPI: Open Charge Point Interface
OICP: Open InterCharge Protocol
OCHP: Open Clearing House Protocol
OSCP: Open Smart Charging Protocol

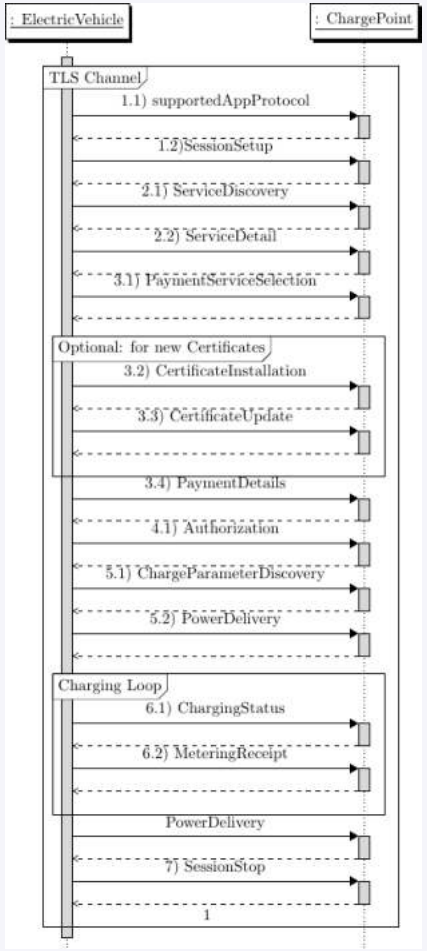
E-Mobility Communication Protocols (Selection of most relevant)

INCYDE

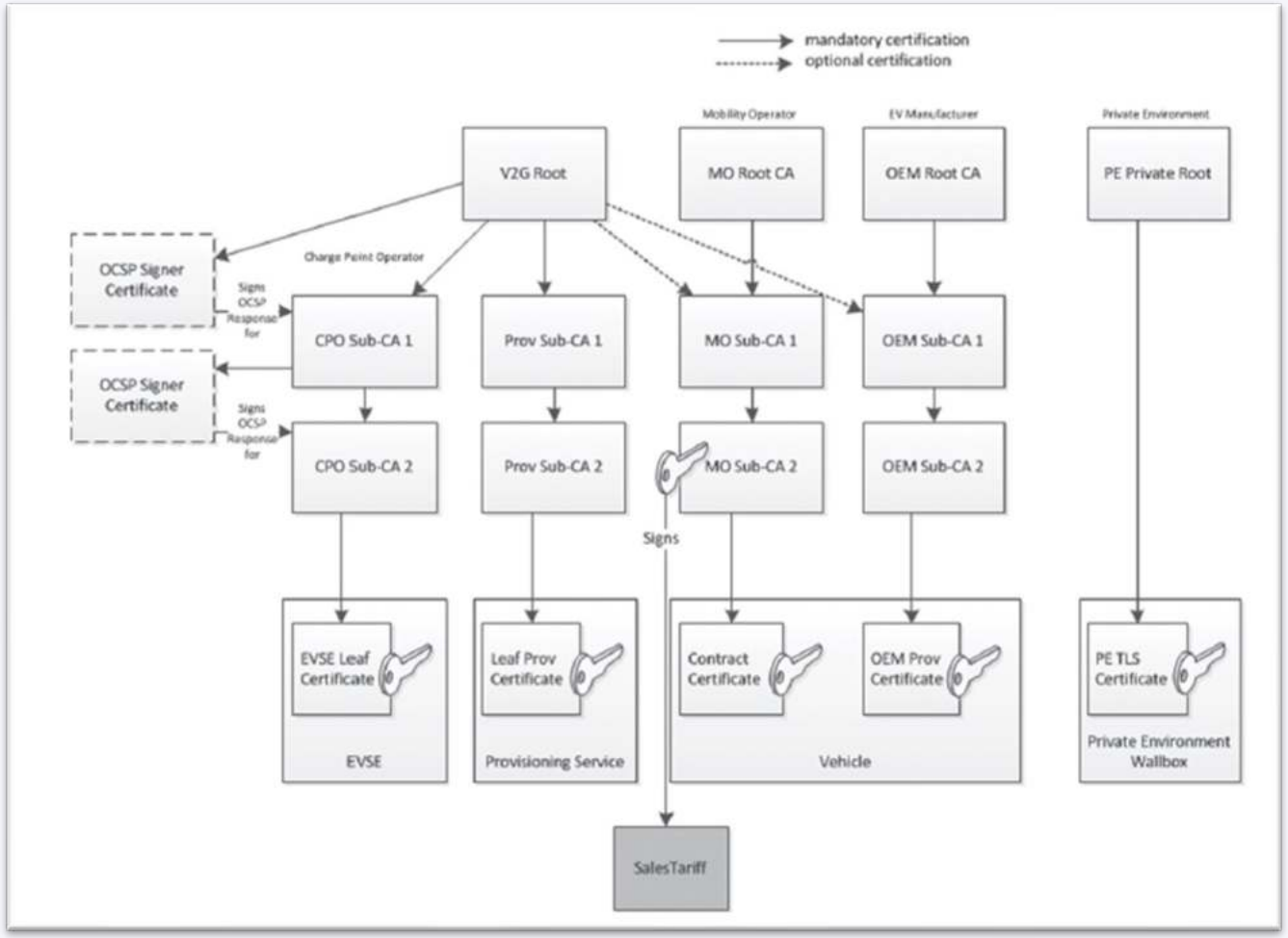
Protocol	Transport	Security	Privacy	Communication Partners
ISO 15118	V2GTP, EXI	TLS	none	EV - CP
NEMA EVSE 1.2	ISO 14443	ISO 7816-4	none	RFID card - CP
OCPP 1.6-S	HTTP, XML, SOAP	none	none	CP - CPO
OCPP 1.6-J	HTTP, JSON over Websockets	TLS	none	CP - CPO
OCPP 2.0.1	HTTP, JSON over Websockets	TLS	none	CP - CPO
OCPI 2.2	HTTP, JSON, REST	TLS	none	MO - CPO
OCHP 1.4	SOAP	WS-Security	none	MO - CCH, CPO - CCH
OICP 2.2	HTTP, SOAP, REST	none	none	MO - CCH, CPO - CCH
OSCP 2.0	JSON / REST	TLS	none	CPO - DSO

ISO 15118 Overview

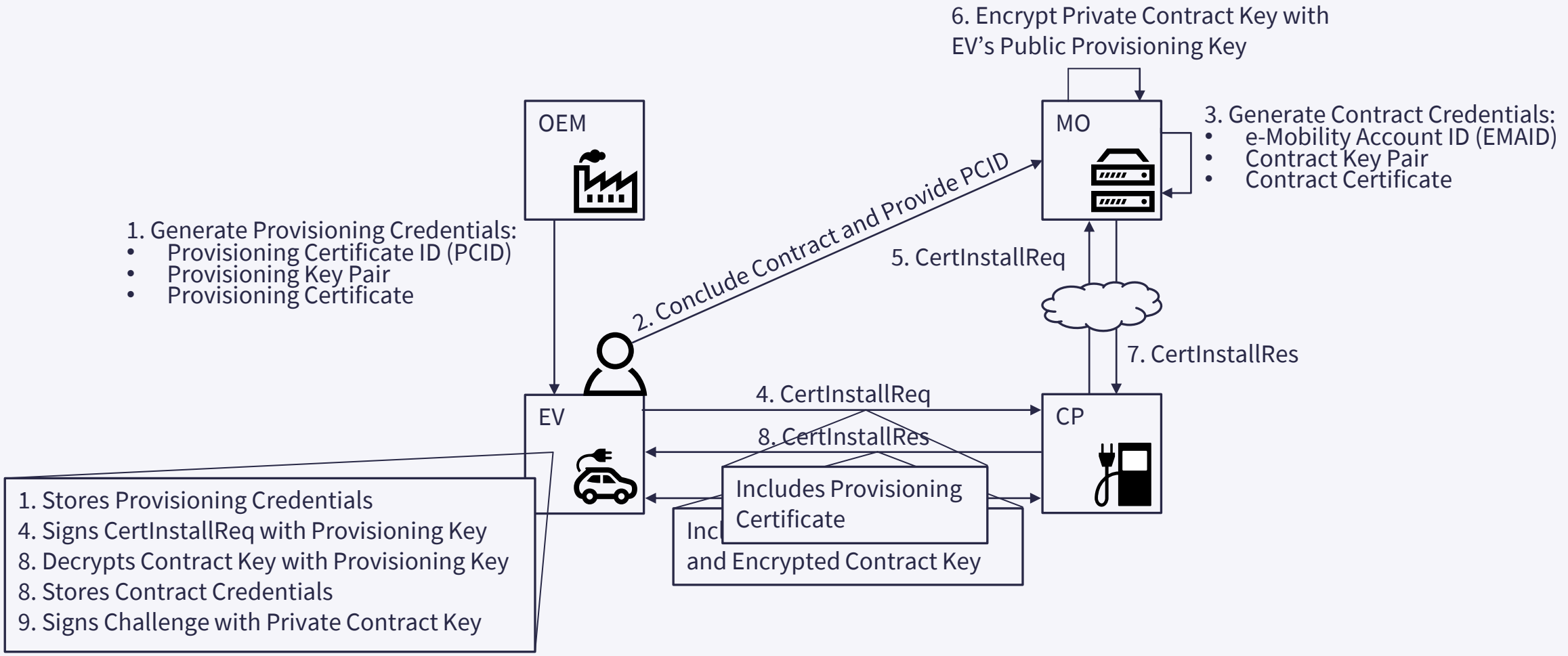
- ISO 15118 standard published in 2014 [ISO14]
  - Vehicle to grid communication interface
    - Dynamic exchange of charging information between EV and CP
      - Enables (“grid-friendly”) negotiation of charging parameter, schedule etc.
    - Supports EIM, e.g., RFID cards
    - Enables Plug-and-Charge (PnC)
  - Security is based on digital certificates
    - TLS 1.2 channel between EV and CP (CP authentication)
    - EV authentication on application layer using EV credentials
- ISO/FDIS 15118-20 (2nd Edition of ISO 15118)
  - FDIS registered for formal approval in October 2021
  - Improved security



ISO 15118
Certificate Handling

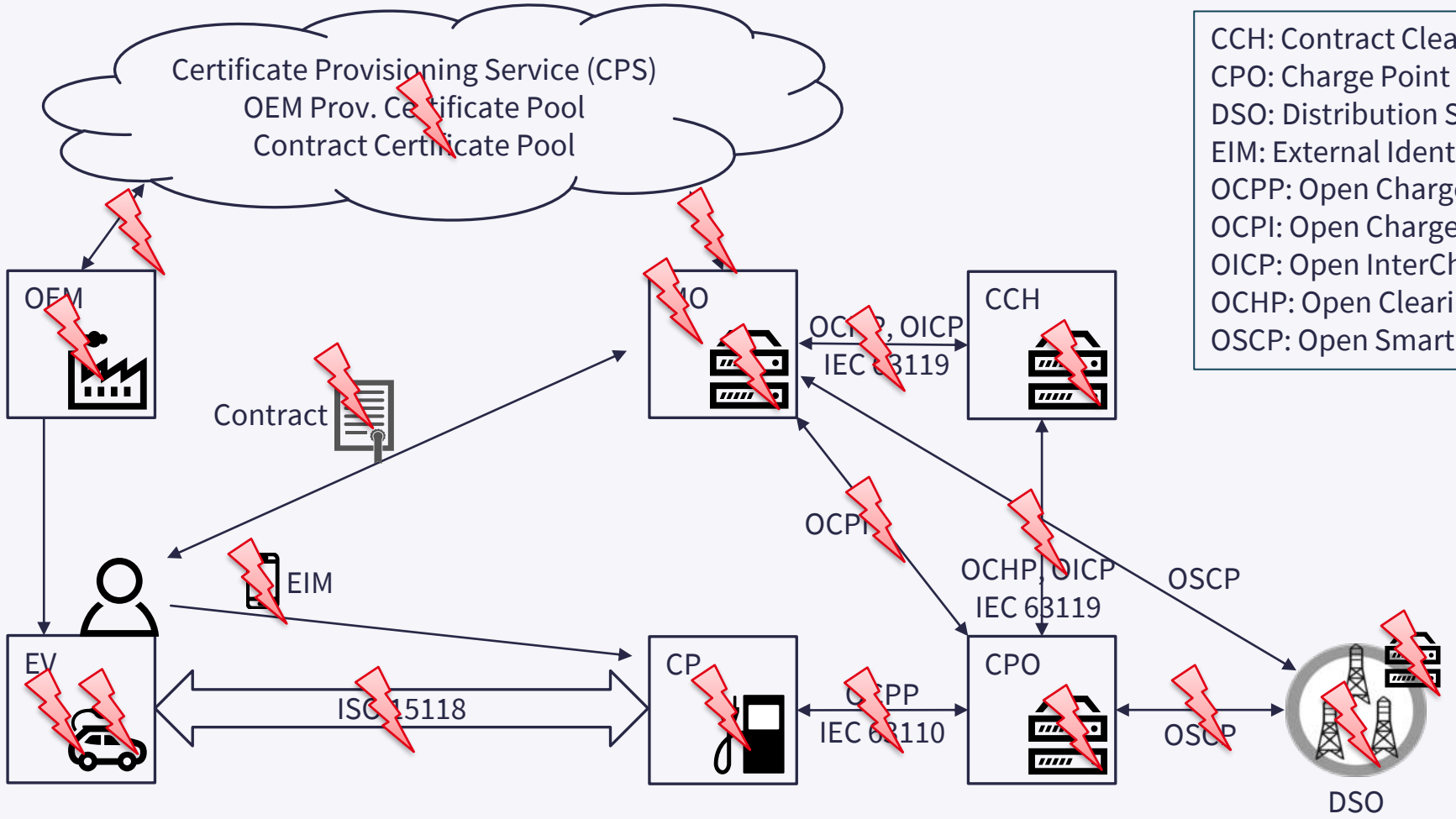


ISO 15118 Processes



E-Mobility Security and Privacy Threats

Attack Points



CCH: Contract Clearing House
CPO: Charge Point Operator
DSO: Distribution System Operator
EIM: External Identification Means
OCPP: Open Charge Point Protocol
OCPI: Open Charge Point Interface
OICP: Open InterCharge Protocol
OCHP: Open Clearing House Protocol
OSCP: Open Smart Charging Protocol

Attack Point: EIM

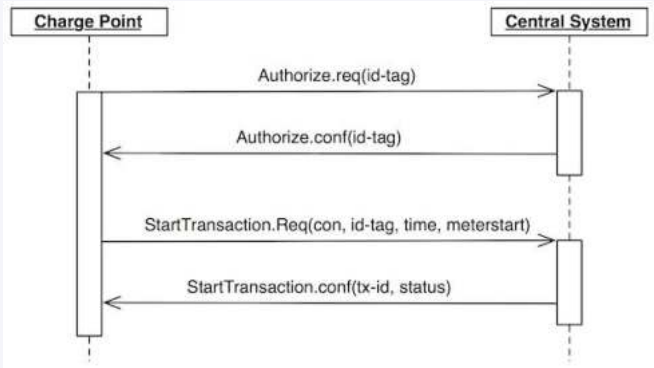
- Attacks on Charging Cards [Dal17]
  - Insecure charging cards
    - Use of (public) card ID (ID Tag) for billing
    - Use of broken Mifare Classic chip
  - Charging cards can be easily copied
  - IDs can be guessed
- Threat
  - Charge to another's account
  - …


```
$ xxd newmotion.mfd
00000000: XXXX XXXX XXXX XX88 4400 c820 0000 0000
00000010: 0000 0000 0000 0000 0000 0000 0000 0000
00000020: 0000 0000 0000 0000 0000 0000 0000 0000
00000030: ffff ffff ffff ff07 8069 ffff ffff ffff
00000040: 0000 0000 0000 0000 0000 0000 0000 0000
00000050: 0000 0000 0000 0000 0000 0000 0000 0000
00000060: 0000 0000 0000 0000 0000 0000 0000 0000
00000070: ffff ffff ffff ff07 8069 ffff ffff ffff
[...]
000003c0: 0000 0000 0000 0000 0000 0000 0000 0000
000003d0: 0000 0000 0000 0000 0000 0000 0000 0000
000003e0: 0000 0000 0000 0000 0000 0000 0000 0000
000003f0: ffff ffff ffff ff07 8069 ffff ffff ffff
```

Contents of NewMotion Charging Card [Dal17]

Attack Point: Backend Communication

- Attacks on (insecure) backend communication
  - Backend communication (was) often not secured, e.g.,
    - Communication between CP and CPO via insecure OCPP 1.5 / 1.6-S
    - Unencrypted transmission of ID Tag [Dal17]
  - …
- Threats
  - Charge to another's account (or for free)
  - Prevent charging
  - Analyze user (privacy)
  - …

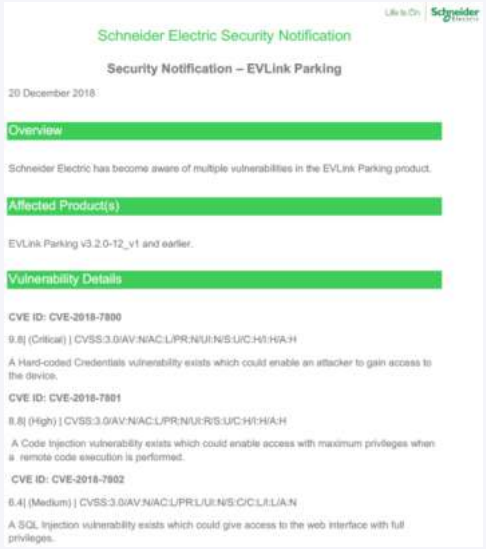



```
<s:complexType name="AuthorizeRequest">
    <s:sequence>
        <s:element name="idTag" type="tns:IdToken" minOccurs="1" maxOccur
s="1"/>
    </s:sequence>
</s:complexType>

<s:simpleType name="IdToken">
    <s:restriction base="s:string">
        <s:maxLength value="20"/>
    </s:restriction>
</s:simpleType>
```

Attack Point: Charge Point

- Attacks exploiting CP vulnerabilities
  - Exploit insecure USB update mechanism [Dal17]
  - Exploit insecure authentication, e.g., use vehicle MAC address [Dal17]
  - Exploit hard-coded credentials and other vulnerabilities [Sch18]
  - …
- Threats
  - Influence power grid
  - Charge to another's account (or for free)
  - Prevent charging
  - Analyze CP user (privacy)
  - …



Schneider Electric Security Notification

Security Notification – EVLink Parking

20 December 2018

Overview

Schneider Electric has become aware of multiple vulnerabilities in the EVLink Parking product.

Affected Product(s)

EVLink Parking v3.2.0-12_v1 and earlier.

Vulnerability Details

CVE ID: CVE-2018-7800

9.8| (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A Hard-coded Credentials vulnerability exists which could enable an attacker to gain access to the device.

CVE ID: CVE-2018-7801

8.8| (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A Code Injection vulnerability exists which could enable access with maximum privileges when a remote code execution is performed.

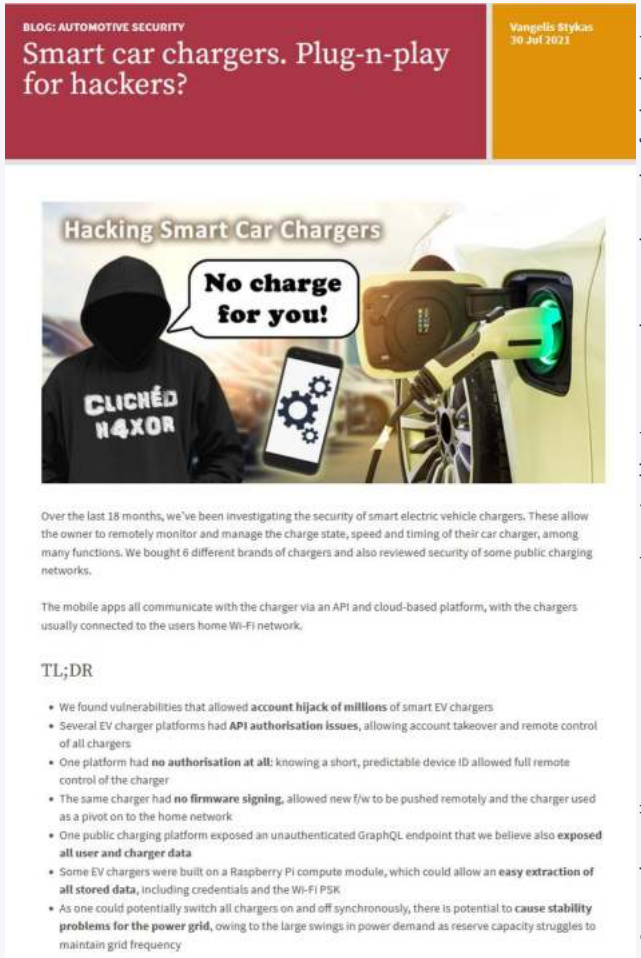
CVE ID: CVE-2018-7802

6.4| (Medium) | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

A SQL Injection vulnerability exists which could give access to the web interface with full privileges.

Security Notification – EVLink Parking

Attack on Keba P30 via insecure USB update [Dal17]



BLOG: AUTOMOTIVE SECURITY

Smart car chargers. Plug-n-play for hackers?

Vangelis Stykas
30 Jul 2021

Hacking Smart Car Chargers

No charge for you!

CLICHÉD H4XOR

Over the last 18 months, we've been investigating the security of smart electric vehicle chargers. These allow the owner to remotely monitor and manage the charge state, speed and timing of their car charger, among many functions. We bought 6 different brands of chargers and also reviewed security of some public charging networks.

The mobile apps all communicate with the charger via an API and cloud-based platform, with the chargers usually connected to the users home Wi-Fi network.

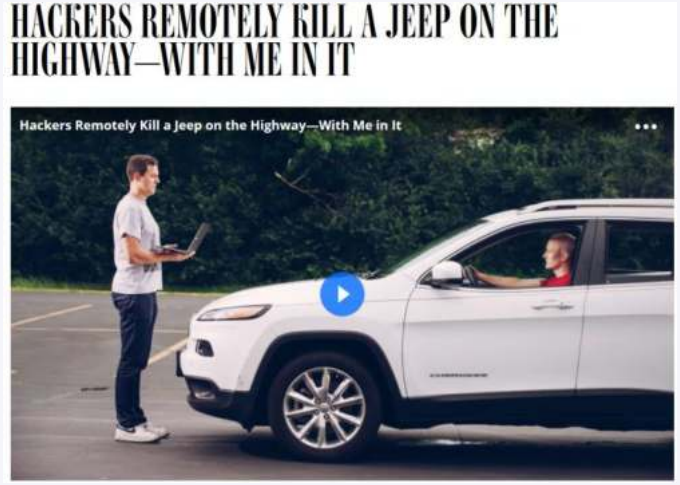
TL;DR

- We found vulnerabilities that allowed **account hijack of millions** of smart EV chargers
- Several EV charger platforms had **API authorisation issues**, allowing account takeover and remote control of all chargers
- One platform had **no authorisation at all**: knowing a short, predictable device ID allowed full remote control of the charger
- The same charger had **no firmware signing**, allowed new f/w to be pushed remotely and the charger used as a pivot on to the home network
- One public charging platform exposed an unauthenticated GraphQL endpoint that we believe also **exposed all user and charger data**
- Some EV chargers were built on a Raspberry Pi compute module, which could allow an **easy extraction of all stored data**, including credentials and the Wi-Fi PSK
- As one could potentially switch all chargers on and off synchronously, there is potential to **cause stability problems for the power grid**, owing to the large swings in power demand as reserve capacity struggles to maintain grid frequency

Source: https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/

Attack Point: EV

- Attacks
  - Vulnerability in the infotainment system of a Tesla Model 3 in 2019
  - Vulnerability in the infotainment system of Volkswagen and Audi in 2018
  - Remote hack of a Tesla Model S in 2016
  - Insecure smartphone app for Nissan Leaf in 2016
  - Remote hack of a Jeep Cherokee in 2015
  - …
- Threats
  - Charge to another's account
  - Share a contract
  - Drain battery
  - Influence power grid
  - …



Source: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Nissan Leaf App / VIN-based Authentication

Attack Point – EV-CP Communication

- Attacks
  - Shortcomings of ISO 15118 (cf. for example [BVWS18])
    - TLS not mandatory
    - No requirements for secure key generation and storage
    - No end-to-end security
    - No real cryptographic agility, fixed cipher suites
      - TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
      - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - Skimming / Man-in-the-Middle attacks
  - Wireless attacks on Wi-Fi communication in case of inductive charging
- Threats
  - Charge to another's account
  - Share a contract
  - Prevent charging
  - Analyze user (privacy)
  - …

MitM Attack Preventing Charging

Source: https://www.swri.org/press-release/electric-vehicle-charging-cybersecurity-vulnerabilities

Resulting Threats

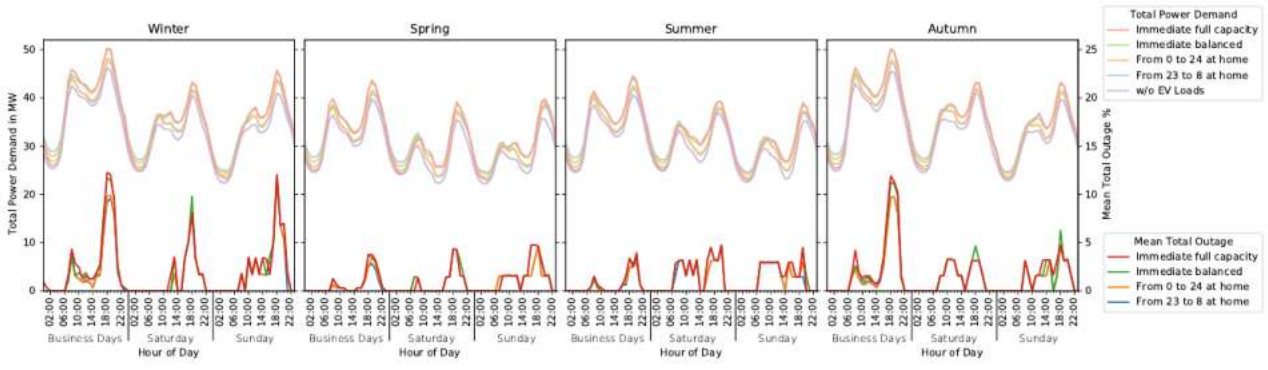
- Safety-adverse effects
  - Triggering fire event
  - Influence power grid
  - Disabling safety measures
  - …
- Financial damage
  - Charge to another's account
  - Charging for free
  - Prevent charging
  - Damage EV battery or reduce lifetime / capacity
  - Damage CP
  - Manipulate billing
  - …
- Privacy loss
  - Generation of movement profiles
  - Analysis of time and location of the used CPs
  - …

Source: https://insideevs.com/news/423581/severe-electric-car-fire-explosion-charging/

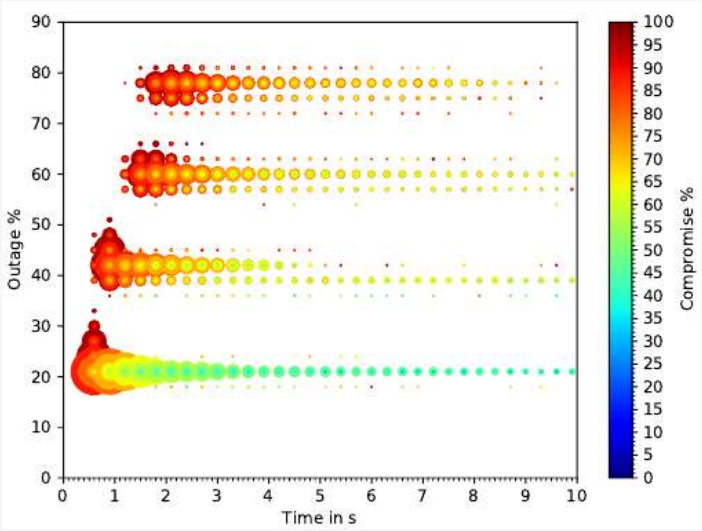
Source: Entega

Example: Influence Power Grid

- Impact of e-mobility-based attacks on power grid resilience [KK21]
  - Framework for simulating and analyzing how e-mobility-based attacks can cause power outages
    - At what times of a day are attacks most easily carried out?
    - How many compromised CPs and EVs are needed for successful attacks?
    - How much time is available to respond to attacks before a power outage occurs?



Base Grid Load Compared to Outage % in MV Oberrhein Scenario 2030 at 50% Compromise



Outage over Time at Different Compromise %

[KK21] D. Kern, C. Krauß. Analysis of E-Mobility-based Threats to Power Grid Resilience, In ACM Computer Science in Cars Symposium (CSCS), 2021. to appear

Example: Privacy Threats

- None of the current PnC protocols define privacy-preserving measures
  - Involved entities gain knowledge of a lot of personal data which is not required for their operation
  - No compliance with European GDPR rules
- Privacy threats
  - Generation of movement profiles
  - Analysis of time and location of the used CPs
- Privacy extension currently only proposed from researchers,
  - Example: Privacy-preserving billing process using Direct Anonymous Attestation (DAA) [ZSZK18]

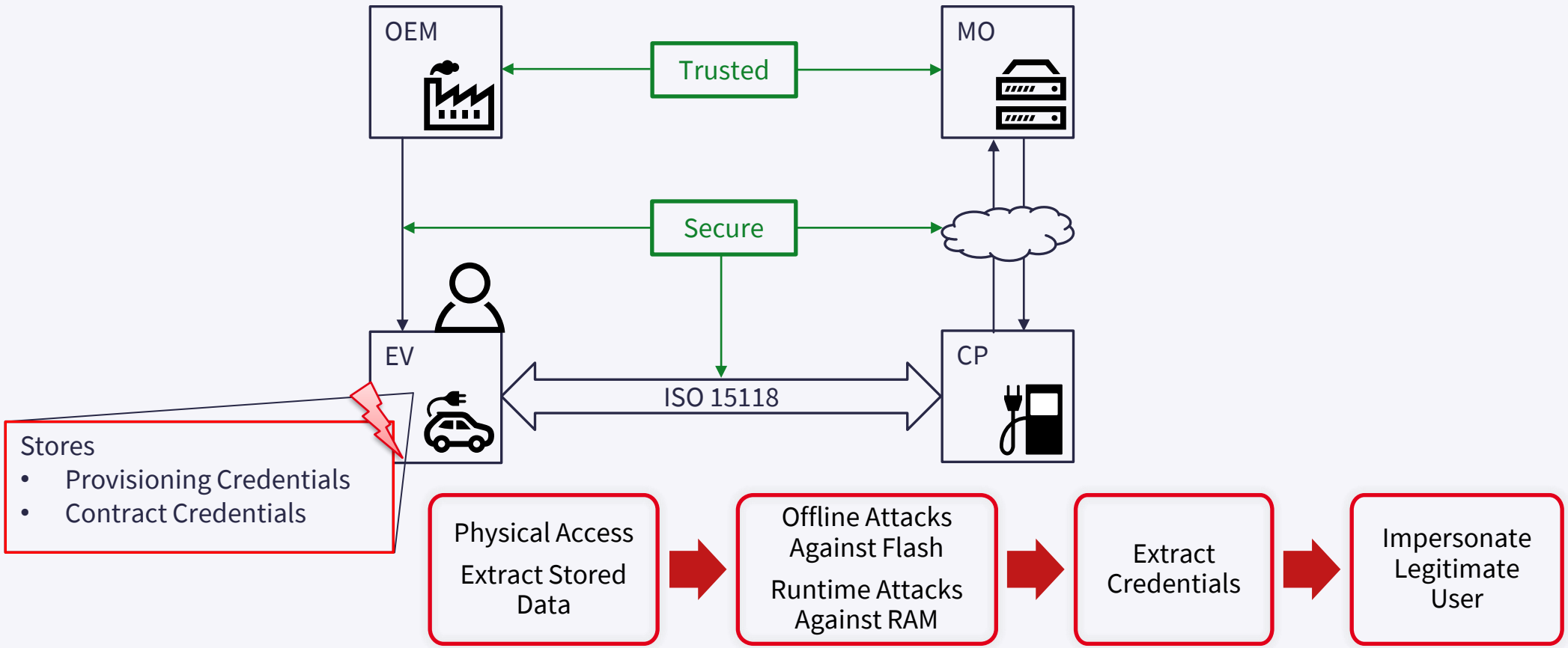
	EV	CP/CPO	CCH	MO
CDR		✓	✓	✓
Charging Parameters	✓	✓		
Contract Certificate	✓	✓		✓
EMAID	✓	✓	✓	✓
EVCCID	✓	✓		
EVSEID	✓	✓	✓	✓
Location	✓	✓	✓	✓
MeterID	✓	✓	✓	✓
Power Consumption	✓	✓	✓	✓
Time	✓	✓	✓	✓

Example: Personal Data in PnC [ZSZK18]

[ZSZK18] D. Zelle, M. Springer, M. Zhdanova, C. Krauß. Anonymous Charging and Billing of Electric Vehicles, ARES, 2018.

Securing ISO 15118 Credentials

Attack Point: EV
Unauthorized Extraction of Credentials



TrustEV – Overview

- TrustEV [FKKZ20a]
  - Security architecture for secure provisioning, storage, and usage of PnC credentials in an EV
- Approach
  - Use of a Hardware Trust Anchor: TPM 2.0
    - Trust establishment
    - No firmware manipulation
    - No illegitimate extraction of sensitive data
    - Secure cryptographic operations
    - Secure Key Storage and Key Usage Authorization
    - Secure Key Provisioning
  - New X.509 certificate extension
  - (Backwards compatible) protocol extension conformant to ISO 15118
  - Minimal Overhead

A safe for sensitive data in the car: Volkswagen relies on TPM from Infineon

Volkswagen is one of the first car makers to deploy the OPTIGA™ Trusted Platform Module (TPM) 2.0 from Infineon Technologies AG as a security solution for the connected car

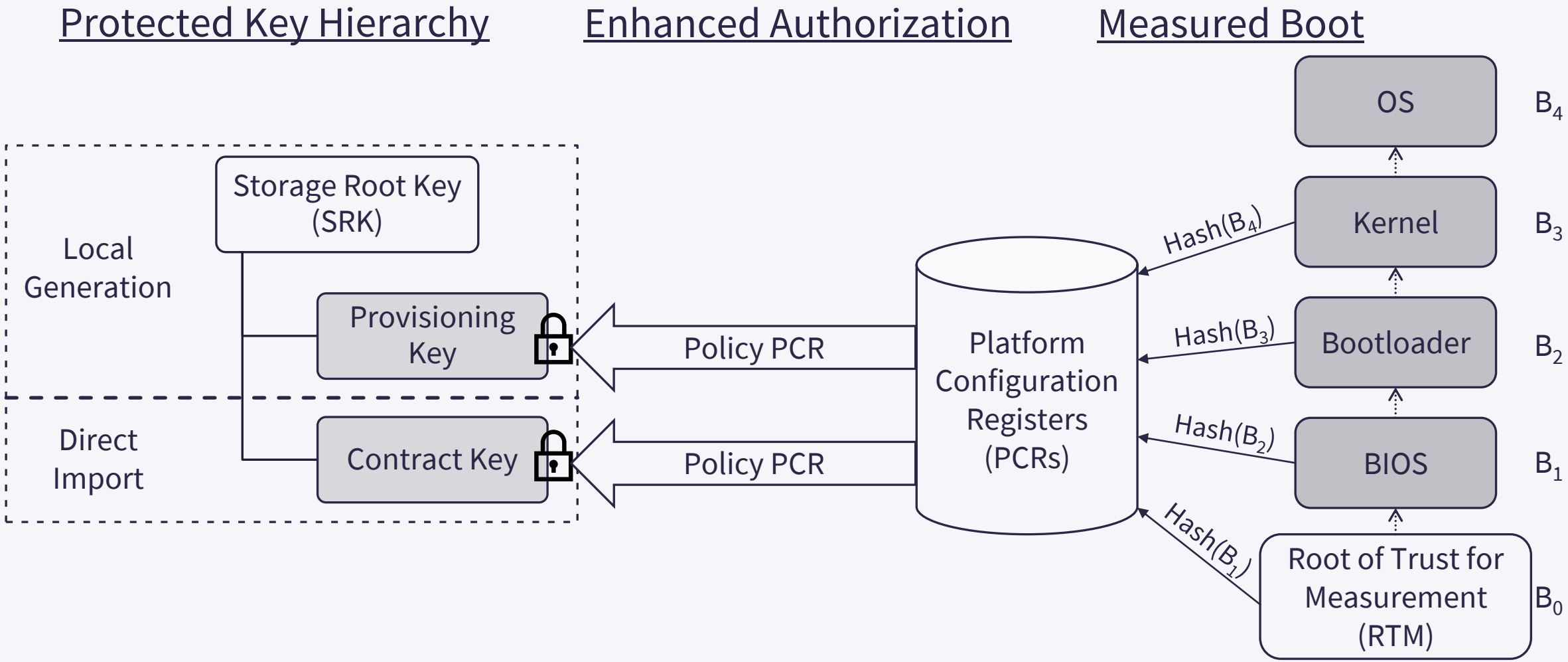
January 25th, 2019

Source: https://www.automotiveworld.com/news-releases/a-safe-for-sensitive-data-in-the-car-volkswagen-relies-on-tpm-from-infineon/

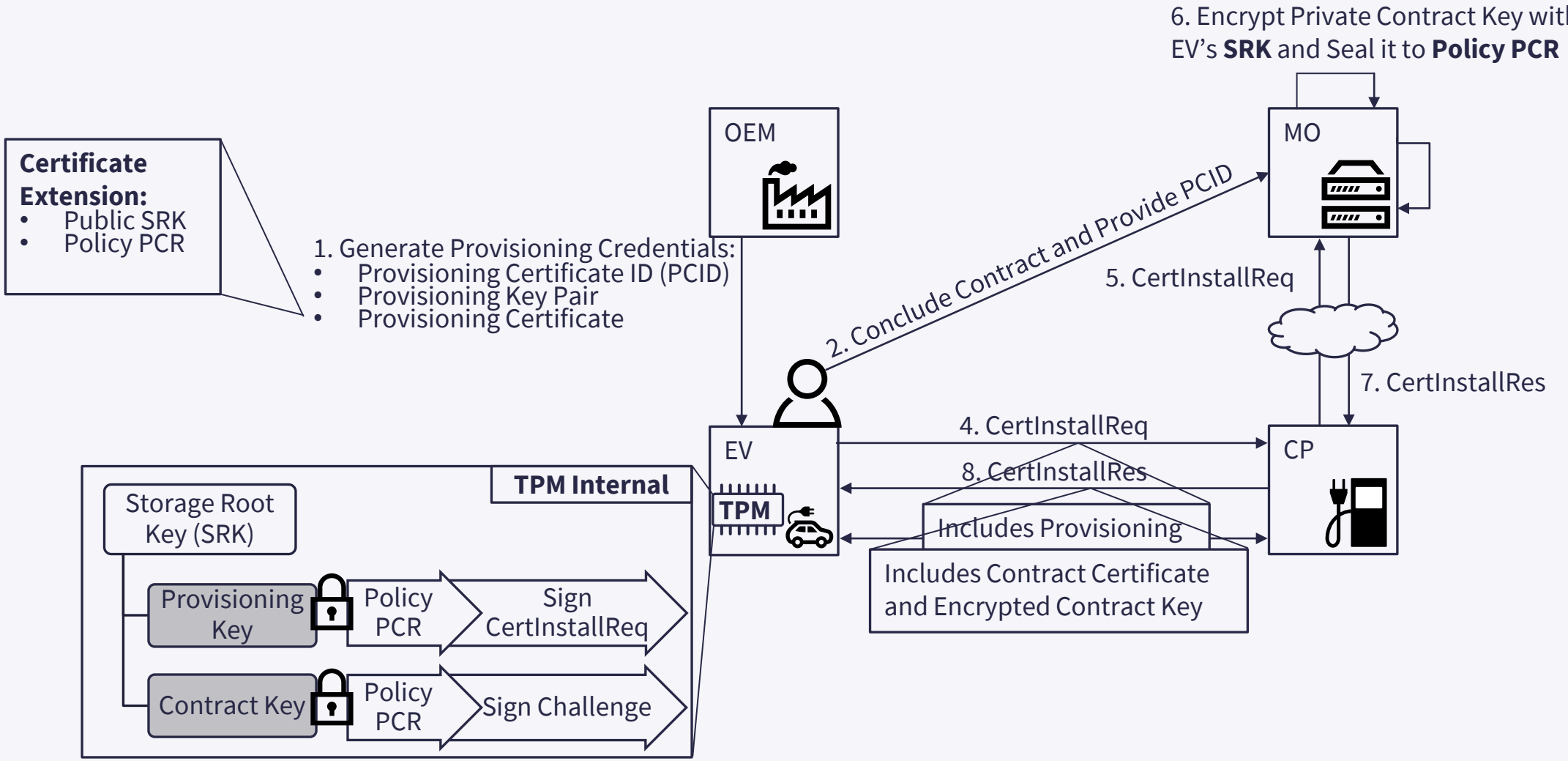
[FKKZ20a] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova. TrustEV: Trustworthy Electric Vehicle Charging and Billing. 35th ACM/SIGAPP Symposium on Applied Computing (SAC) - Computer Security (SEC), 2020

TrustEV – TPM 2.0 Basics

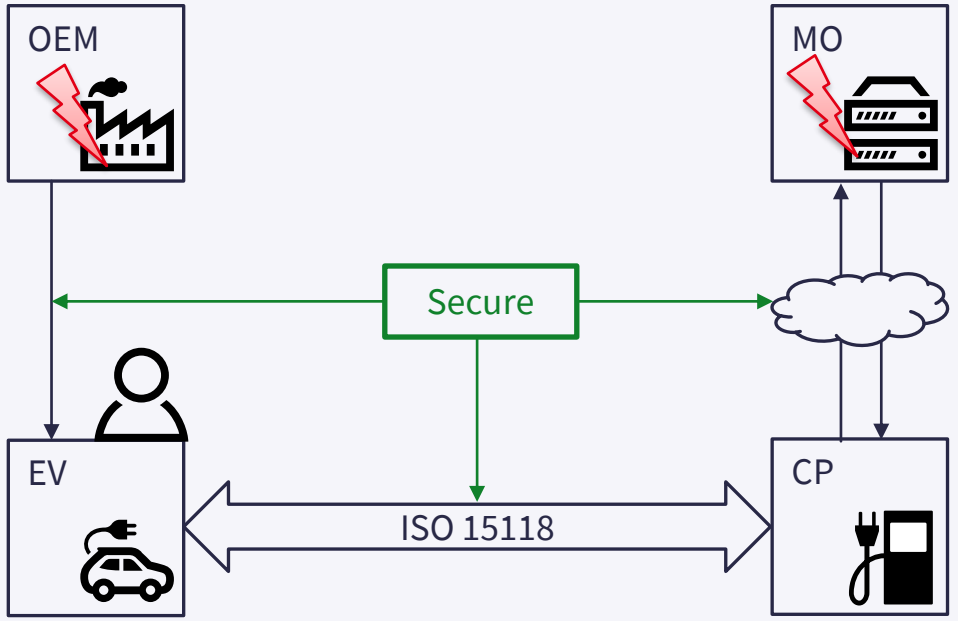
INCYDE



TrustEV – Processes

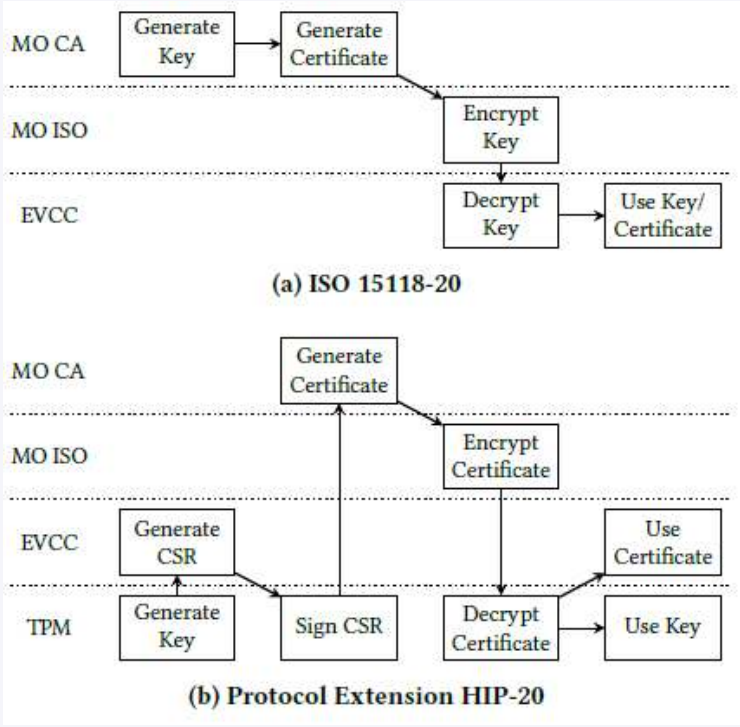


Attack Point: Backend Systems
Unauthorized Extraction of Credentials



HIP / HIP 2.0 – Overview

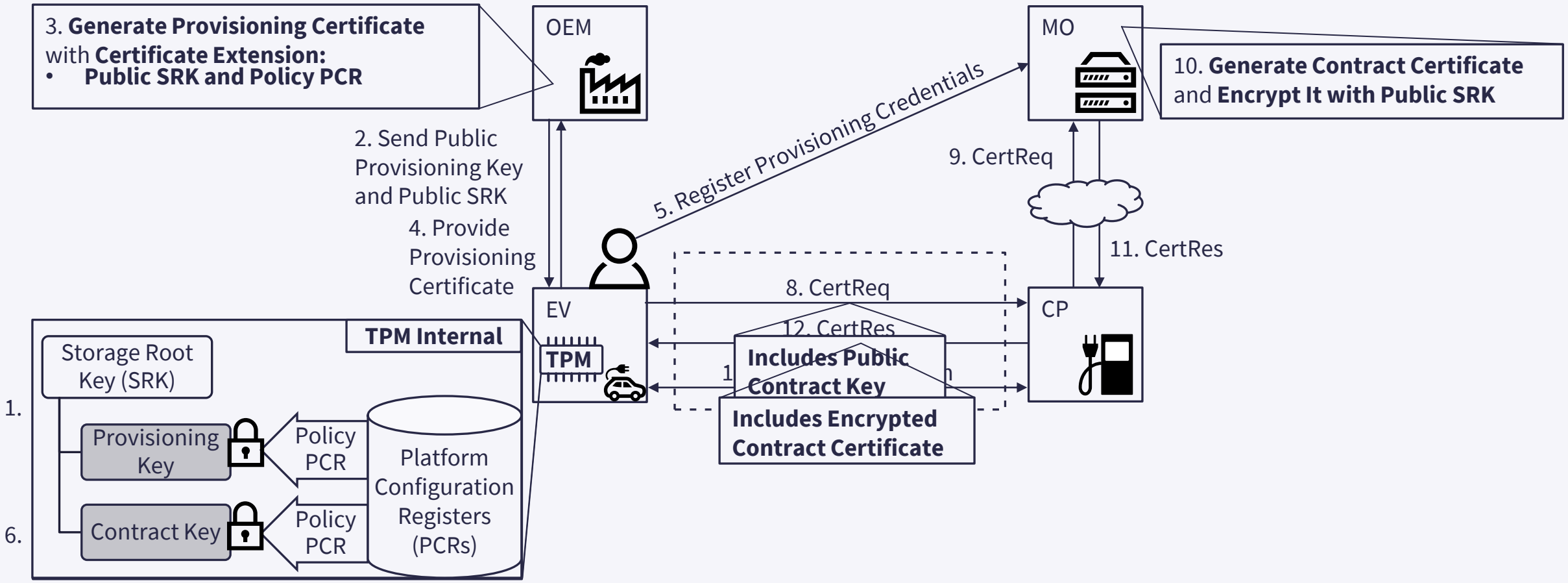
- HIP / HIP 2.0 [FKKZ20b, FKKZH20]
  - Improvement of TrustEV for secure generation, storage, provisioning, use, and revocation of PnC credentials
    - Protection against backend compromise
    - Secure keys generation in the TPM of the EV
      - Private keys never leave the TPM
      - Only public keys are stored in backends
    - Backwards compatible
  - HIP 2.0 provides additional features, e.g.,
    - Supporting the use of certificate pools
    - Easy integration into existing Certificate Authorities (CAs) and processes such as Certificate Signing Requests (CSRs)



[FKKZ20b] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova. HIP: HSM-based Identities for Plug-and-Charge. 13th International Conference on Availability, Reliability and Security (ARES), 2020

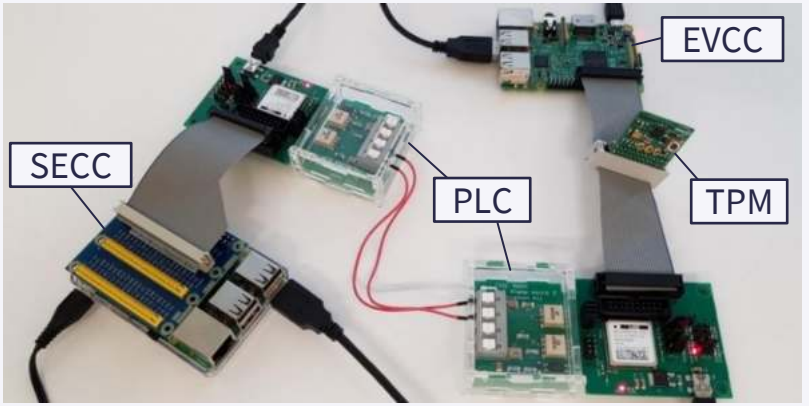
[FKKZH20] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova, R. Heddergott. HIP-20: Integration of Vehicle-HSM-Generated Credentials into Plug-and-Charge Infrastructure, In ACM Computer Science in Cars Symposium (CSCS), 2020.

HIP – Processes



Summary

- Trust EV and HIP / HIP 2.0 ISO 15118 Extension
- TPM 2.0-based security architecture
- Protection of ISO 15118 PnC credentials
  - Secure key storage with TrustEV in the EV
  - Secure key generation in the EV with HIP / HIP 2.0
  - Key usage authorized to trustworthy EVs only
- Seamless integration
  - Compatibility to ISO 15118
  - Minimal overhead
  - Backwards compatible
- Changes proposed to ISO standardization
  (parts have been included in 2nd Edition of ISO 15118)



Demonstration and Evaluation PoC

Conclusion & Future Work

Conclusion

- Electric mobility will be important part of our mobility
- Many attacks may be possible
  - Attacks on billing
  - Attacks on privacy (movement profiles)
  - Attacks on the power grid
  - …
- We developed hardware-assisted security and trust solutions for
  - Protecting ISO 15118 PnC credentials (in EV and backend) [FKKZH20, FKKZ20a, FKKZ20b]
  - Ensuring the trustworthiness of EVCC and BMS [FKKZ20c]
  - Privacy-preserving billing using DAA [ZSZK18]
  - Securing CPs [KKZ19]
  - …
- Parts of our research were adopted in the 2nd Edition of ISO 15118

Future Work

- Security and privacy requires additional research
  - Reliable threat models and impact analyzes (e.g., on power grids)
  - Improved security protocols, e.g., alternative authentication based on Self-Sovereign Identities
  - Integration of cryptographic agility and use of post quantum cryptography (PQC)
    - cf. for example our work on post quantum TLS on embedded systems [BKNS20]
  - (Formal) analysis of e-mobility communication protocols
    - cf. for example our work on formal analysis of SecOC [LZK20] and SOME/IP [ZKLK21]
- Adaption and integration of the research results into upcoming standards

Literature

[BKNS20] K. Bürstinghaus-Steinbach, C. Krauß, R. Niederhagen, M. Schneider. Post-Quantum TLS on Embedded Systems: Integrating and Evaluating Kyber and SPHINCS + with mbed TLS. 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS), 2020

[BVWS18] K. Bao, H. Valev, M. Wagner, H.Schmeck. A threat analysis of the vehicle-to-grid charging protocol ISO 15118. Comput Sci Res Dev 33, 3–12, 2018

[Dal17] M. Dalheimer. Ladeinfrastruktur für Elektroautos: Ausbau statt Sicherheit - Warum das Laden eines Elektroautos unsicher ist, 34C3, 2017

[El17] ElaadNL. EV Related Protocol Study, Version 1.1, 2017

[FKKZH20] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova, R. Heddergott. HIP-20: Integration of Vehicle-HSM-Generated Credentials into Plug-and-Charge Infrastructure, In ACM Computer Science in Cars Symposium (CSCS), 2020.

[FKKZ20a] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova. TrustEV: Trustworthy Electric Vehicle Charging and Billing. 35th ACM/SIGAPP Symposium on Applied Computing (SAC) - Computer Security (SEC), 2020

[FKKZ20b] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova. HIP: HSM-based Identities for Plug-and-Charge. 13th International Conference on Availability, Reliability and Security (ARES), 2020

[FKKZ20c] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova. Securing Electric Vehicle Charging Systems through Component Binding. In Proceedings of the 39th International Conference on Computer Safety, Reliability and Security (SAFECOMP), 2020

[ISO14] ISO / IEC. ISO 15118-2 Road vehicles - Vehicle-to-Grid Communication Interface - Part 2: Network and application protocol requirements, 2014

[KK21] D. Kern, C. Krauß. Analysis of E-Mobility-based Threats to Power Grid Resilience, In ACM Computer Science in Cars Symposium (CSCS), 2021. to appear

[KKZ19] D. Kern, C. Krauß, M. Zhdanova. System Security Mechanisms for Electric Vehicles and Charge Points Supporting ISO 15118 - Proposal for a Technical Guideline. Fraunhofer SIT. Technical Report. SIT-TR-2019-04, 2019

[LZK20] T. Lauser, D. Zelle, C. Krauß. Security Analysis of Automotive Protocols, 4th ACM Computer Science in Cars Symposium (CSCS), 2020

[NPE17] German National Platform for Electric Mobility (NPE). The German Standardisation Roadmap Electric Mobility 2020, April 2017

[Sch18] Schneider Electric. Security Notification – EVLink Parking , https://www.se.com/ww/en/download/document/SEVD-2018-354-01/

[ZKLK21] D. Zelle, D. Kern, T. Lauser, and C. Krauß. Analyzing and Securing SOME/IP Automotive Services with Formal and Practical Methods. In 14th International Conference on Availability, Reliability and Security (ARES), ACM, 2021.

[ZSZK18] D. Zelle, M. Springer, M. Zhdanova and C. Krauß. Anonymous Charging and Billing of Electric Vehicles, 13th International Conference on Availability, Reliability and Security (ARES), 2018

Prof. Dr. Christoph Krauß
Head of Automotive Security Research
INCYDE GmbH
Schaumainkai 91, D-60596 Frankfurt / Main
christoph.krauss@incyde.com
https://incyde.com

Prof. Dr. Christoph Krauß
Co-Head of ACSD Research Group
Darmstadt University of Applied Sciences
Haardtring 100, D-64295 Darmstadt
christoph.krauss@h-da.de
https://acsd.h-da.de