Hacker und die Elektromobilität

Warum Cybersicherheit wichtig ist!

h_da

darmstadt university
of applied sciences

Christoph Krauß

Ringvorlesung Cybersicherheit
Hessisches Ministerium des Innern und für Sport

7. Dezember 2023

Über mich

- Prof. Dr. Christoph Krauß
  - Professor für Netzwerksicherheit
  - Sprecher der „Fachgruppe IT-Sicherheit"
- Forschung
  - Leiter der Forschungsgruppe „Applied Cyber Security Darmstadt“
  - Mitglied des Promotionszentrums Angewandte Informatik (PZAI)
  - Forschungsinteressen
    - Sicherheit von Protokollen und formale Analyse
    - Trusted Computing, Netzwerksicherheit, angewandte Kryptographie
    - Sicherheit und Datenschutz für Automobil, Bahn, intelligente Energiesysteme und IoT
- Sonstige Aktivitäten
  - Mitgründer und Leiter Automotive Security Research INCYDE GmbH

acsd applied cyber security darmstadt

INCYDE

Applied Cyber Security Darmstadt

- Forschungsgruppe am Fachbereich Informatik
- Leitung
  - Prof. Dr. Christoph Krauß
  - Prof. Dr. Alexander Wiesmaier
- Online: https://acsd.h-da.de
- Forschungsthemen (Auswahl)
  - Sicherheit und Datenschutz im Automobil
  - Netzwerksicherheit
  - Formale Protokollanalyse
  - Angewandte Kryptographie

Source: Gregor Schuster for ACSD

Teile des ACSD Automotive Security Teams





Einleitung

Motivation

- E-Mobilität ist eine wichtige Technologie zur Reduzierung von Emissionen
- E-Mobilität befindet sich auf der Überholspur
  - 1.013.009 zugelassene batterieelektrische Fahrzeuge (EV) in Deutschland (1. Januar 2023)
  - Zusätzlich 864.712 Plug-in-Hybridautos (1. Januar 2023)
- IT ermöglicht intelligentes Laden
  - Plug & Charge (PnC)
  - Anpassung an Nutzeranforderungen
  - Demand Response und Lastmanagement
  - Vehicle-to-Grid (V2G)

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/

electrive.com
industry service for electric mobility

Menu

Automobile >

Jan 9, 2023 - 11:26 am

Over one million purely electric cars now on German roads

BEV | EUROPE | GERMANY | SUBSIDIES

The German Institute for Economic Research (DIW) has reported that the mark of one million pure electric cars in Germany has been crossed. According to the report, the mark was passed in the new record month of December 2022.

In the last month of 2022, Germany's old – higher – environmental bonus and innovation premium was still valid, and 104,325 new electric cars were newly registered. The DIW says that the reduction in the electric car subsidies as of the New Year accounts for the strong increase in December.

As of January this year, an electric car purchase came with a maximum of 4,500 euros from the state, whereas up until the end of last year, the subsidy was 6,000 euros plus the manufacturer's share, which is half of the state's support.

The one million mark reached accounts only for purely battery electric cars and not plug-in hybrids recorded in December. As it stands, PHEVs also set a record in December, as the environmental bonus for these motor types was abolished completely at the turn of the year.

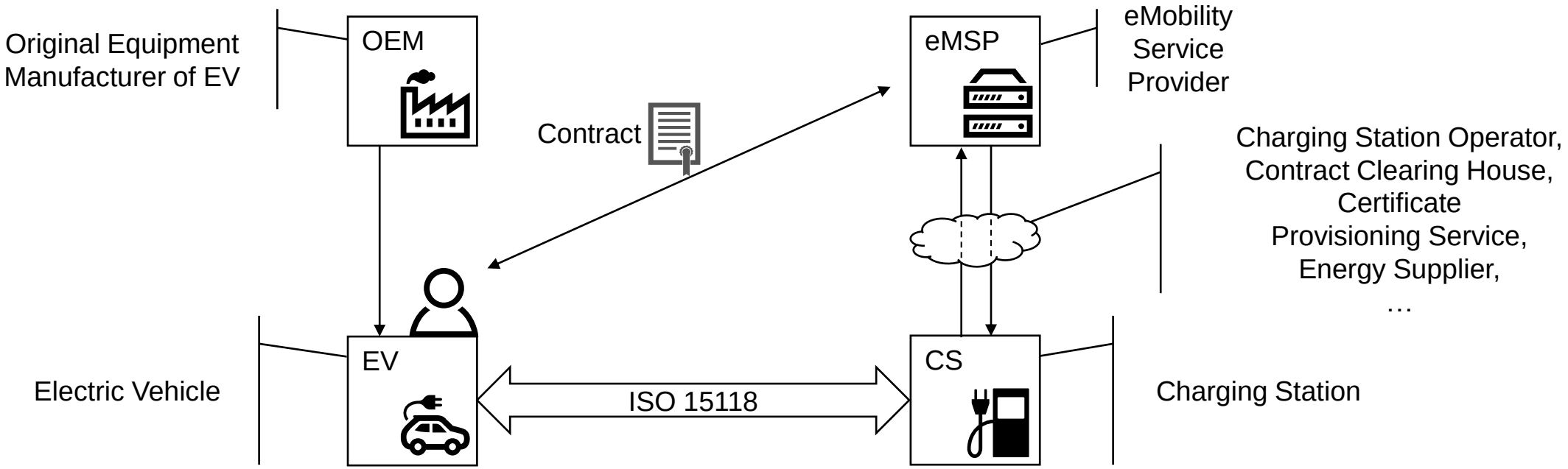
The German Federal Motor Transport Authority has not yet published figures on the number of cars with a cut-off date of 1 January 2023 but as of 1 October 2022, already recorded 840,645 electric cars. If the monthly BEV registrations in October, November and December are added to this figure, the result is 1,038,731 electric cars. If the million mark was indeed cracked, fewer than 38,731 electric cars must have been deregistered in the last quarter.

The increase is startling when compared to the previous two years. As of 1 January 2022, the number of electric cars in Germany was still 618,460, while as of 1 January 2021, there were only 309,083 electric cars on German roads.

Since the December record is primarily attributed to the change in Germany's so-called 'environmental bonus', the DIW report was sceptical as to whether the German government's target of 15 million electric cars can be achieved by 2030. As the institute calculates, about 145,000 electric cars would have to be newly registered every month from now on to make the target. Despite the record figures at the end of the year, there were still only 32,000 electric cars newly registered per month on average in 2022. At the same time, numerous manufacturers have announced that they will only offer electric cars in the course of the decade, which should mark exponential growth in new monthly registrations.

Source: https://www.electrive.com/2023/01/09/over-one-million-purely-electric-cars-now-on-german-roads/
Based on numbers of the German KBA.

(Vereinfachte) Intelligente Ladeinfrastruktur*



* Angelehnt an ISO 15118 [ISO14] und ISO 15118-20 [ISO22]

Neue Bedrohungen für Cybersicherheit und Datenschutz

- Betriebsstörungen
  - Laden verhindern
  - Störungen des Stromnetzes
- Funktionale Sicherheit
  - Auslösen eines Brands
  - Schutzmaßnahmen deaktivieren
- Finanzielle Schäden
  - Kostenloses Laden / Laden auf fremdes Konto
  - Beschädigung der Batterie oder Verringerung der Lebensdauer / Kapazität
- Verlust der Privatsphäre
  - Generierung von Bewegungsprofilen
  - Analyse von Zeit und Ort der verwendeten Ladestationen

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


Forbes

As More EVs Hit The Road, Blackouts Become Likely

Oliver Wyman Contributor

Oliver Wyman Contributor Group

Aerospace & Defense

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

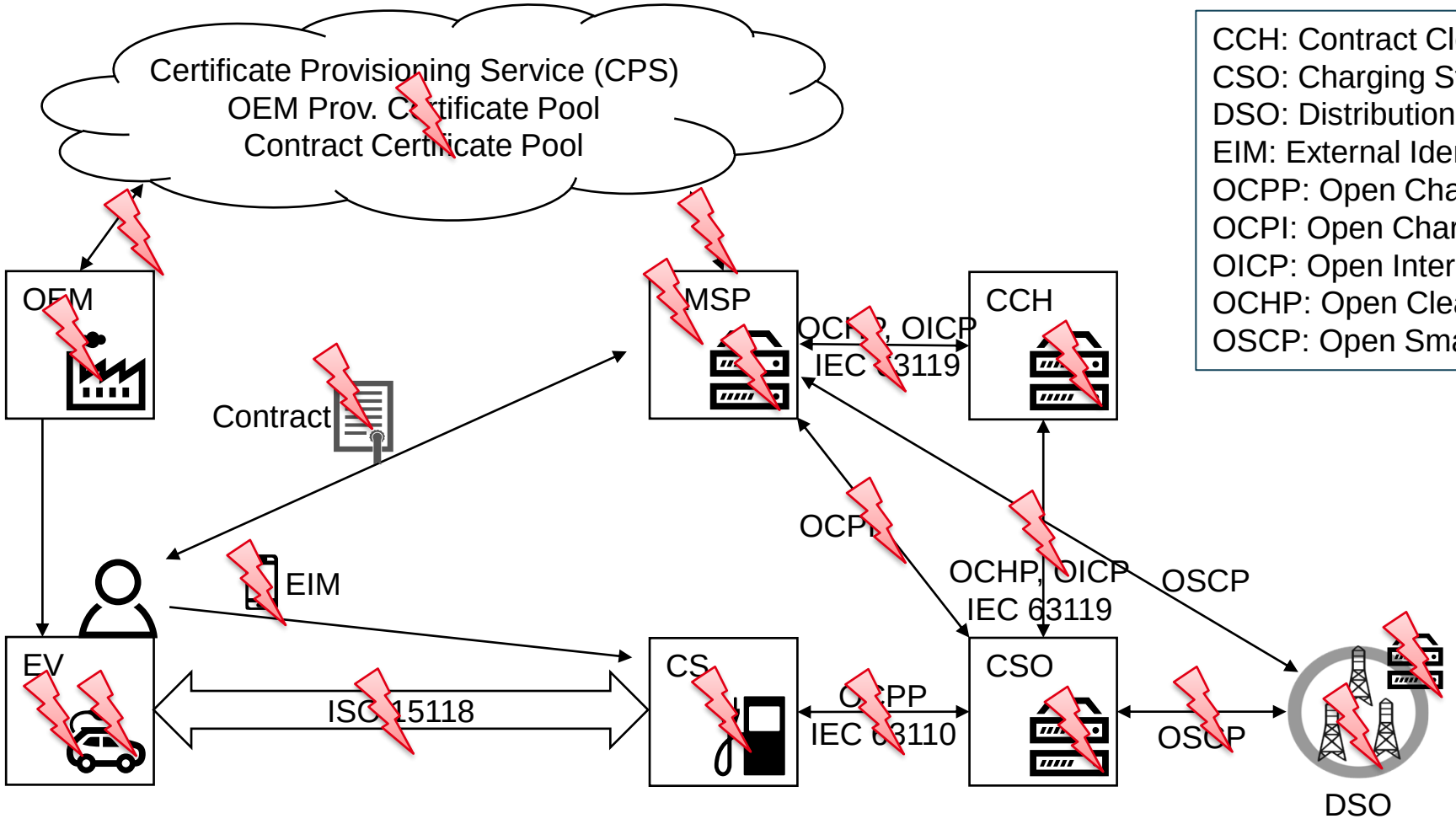
2017-12-27 00:43:00, 46halbe

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

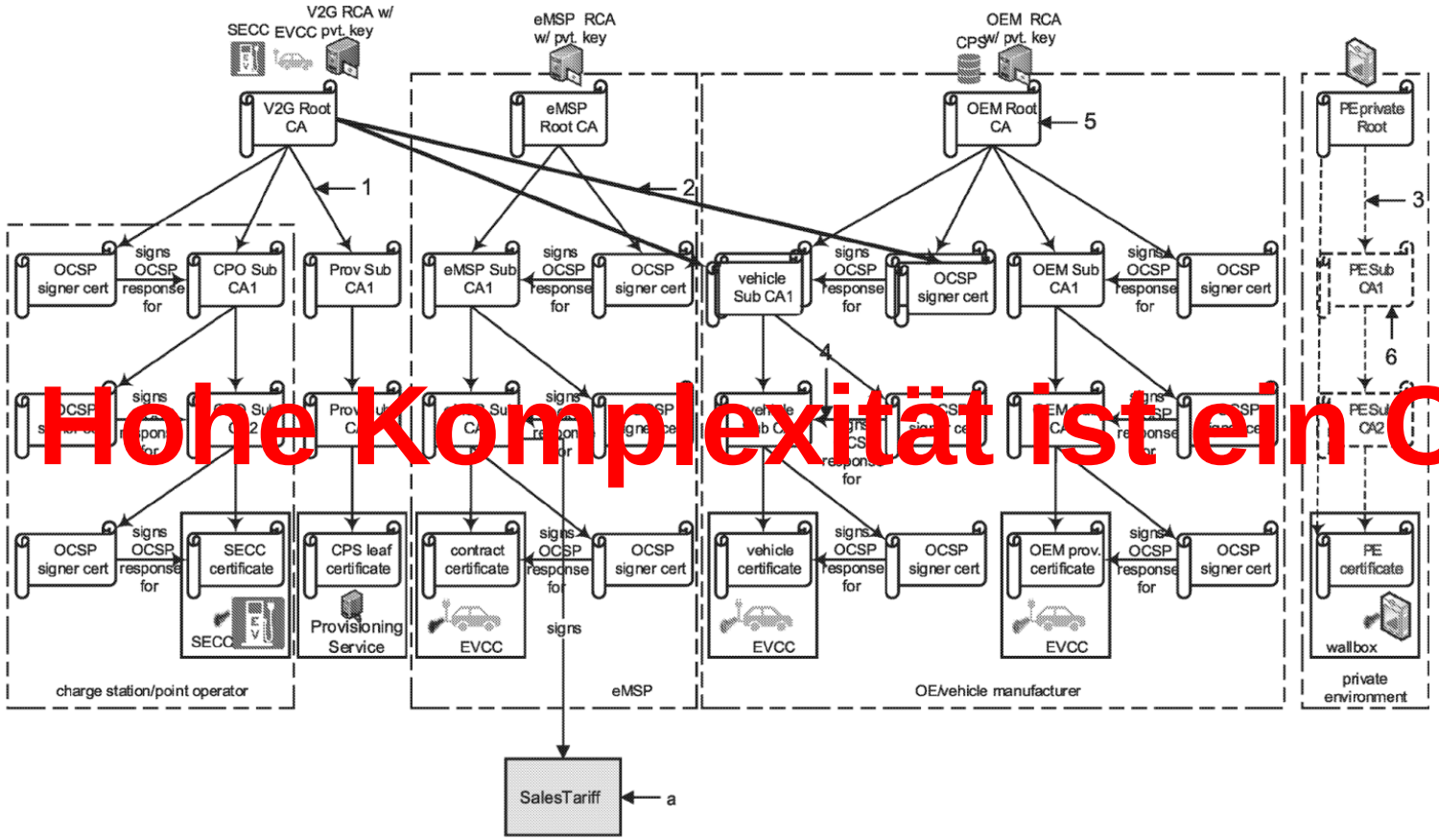
Herausforderungen

Herausforderung #1 – Komplexität
Intelligente Ladeinfrastruktur (mehr Details)



CCH: Contract Clearing House
CSO: Charging Station 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

Herausforderung #1 – Komplexität
Beispiel: ISO 15118-20 PKI und Zertifikate



Beispiel: ISO 15118-20 Public Key Infrastructure (PKI) mit cross signing [ISO22]

ISO 15118-20 certificate profiles			V2G root V2G
TbsCertificate	Version		2 ("2" indicates X.509v3)
	SerialNumber		(Positive integer)
	Signature	AlgorithmIdentifier	x
		algorithm	x id-Ed448
		parameters	-
	Issuer	Country	(x)
		Organization	x
		Organization unit	(x)
		Common name	x
		Domain component	(x)
	Validity	Validity	x (25 years)
		notBefore	x
		time	x (GeneralizedTime expressed in Greenwich Mean Time (Zulu) with format YYYYMMDDHHMMSSZ) [Actual time is CA discretionary]
		notAfter	x
		time	x (GeneralizedTime expressed in Greenwich Mean Time (Zulu) with format YYYYMMDDHHMMSSZ) [Actual time is CA discretionary]
	Subject	Country	(x)
		Organization	x
		Organization unit	(x)
		Common name	x
		Domain component	(x)
	SubjectPublicKey Info	AlgorithmIdentifier	x
		algorithm	x id-Ed448
		parameters	-
		SubjectPublicKey	x (BIT STRING)
	IssuerUniqueID		-
	SubjectUniqueID		-
	Extensions	AuthorityKeyIdentifier	-
		SubjectKeyIdentifier	x / nc id-ce-subjectKeyIdentifierx
		keyIdentifier	x (see [V2G20-1852])
		KeyUsage	x / c id-ce-keyUsage
		digitalSignature	0/1
		nonRepudiation (contentCommitment)	0/1
		keyEncipherment	0/1

Beispiel: V2G Root CA Certificate [ISO22]

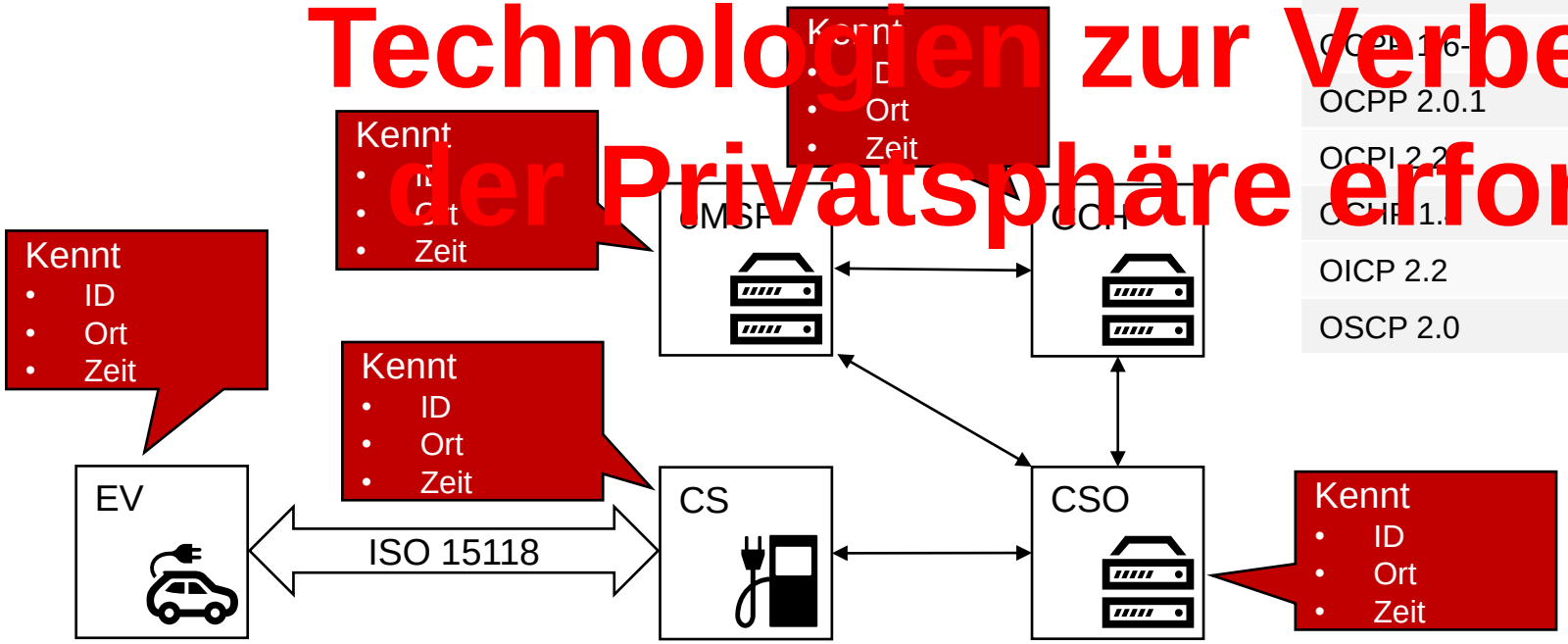
Hohe Komplexität ist ein Cyberrisiko

Herausforderung #2 – Schutz der Privatsphäre

- Keine Maßnahmen zum Schutz der Privatsphäre in aktuellen Protokollen
- Bedrohungen der Privatsphäre
  - Generierung von Bewegungsprofilen
  - Ableitung des Nutzerverhaltens

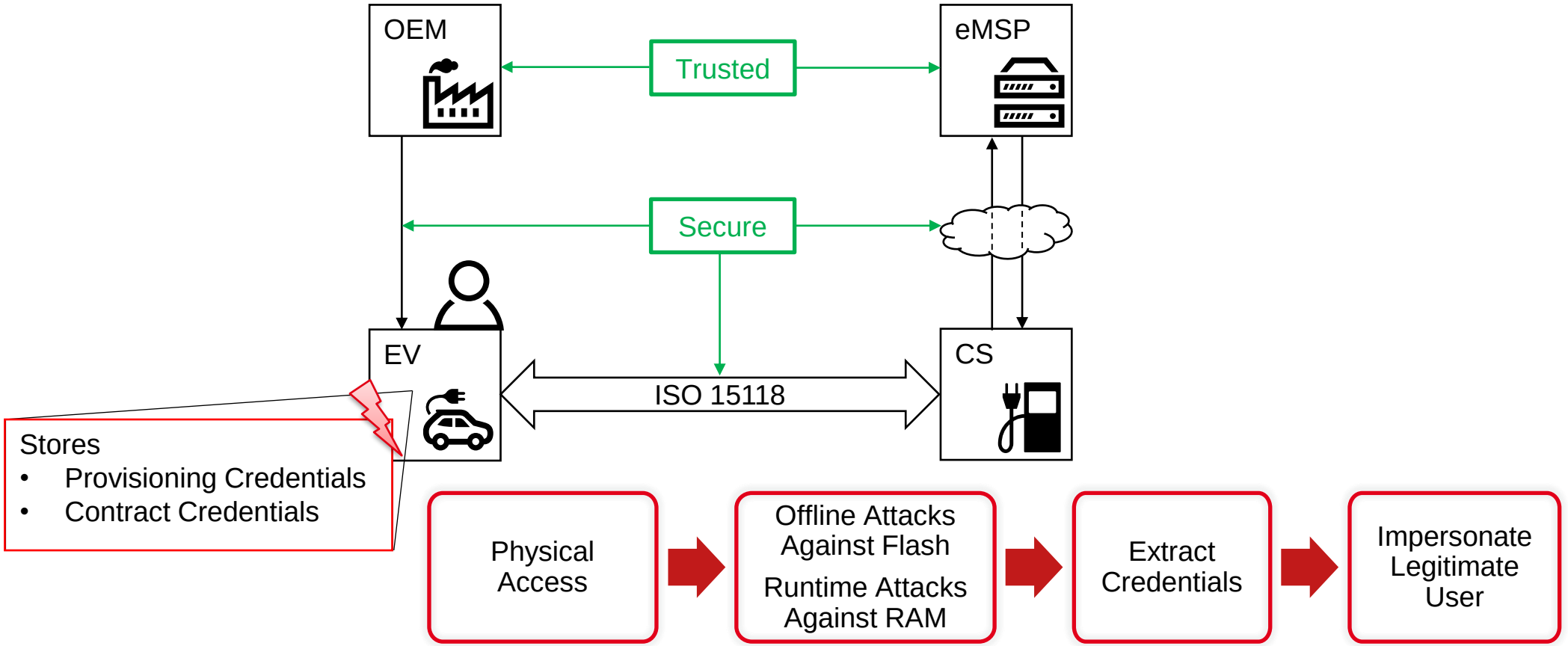
Protocol	Security	Privacy	Communication Partners
ISO 15118	TLS	none	EV – CS
NEMA EVSE 1.2	ISO 7816-4	none	RFID card – CS
OCPP 1.6-S	none	none	CS – CSO
OCPP 1.6-	TLS	none	CS – CSO
OCPP 2.0.1	TLS	none	CS – CSO
OCPI 2.2	TLS	none	MO – CSO
OCHP 1.3	X.509-Security	none	MO – CCH, CSO – CCH
OICP 2.2	none	none	MO - CCH, CSO – CCH
OSCP 2.0	TLS	none	CSO – DSO

Technologien zur Verbesserung der Privatsphäre erforderlich



Herausforderung #3 – Schutz von Zugangsdaten

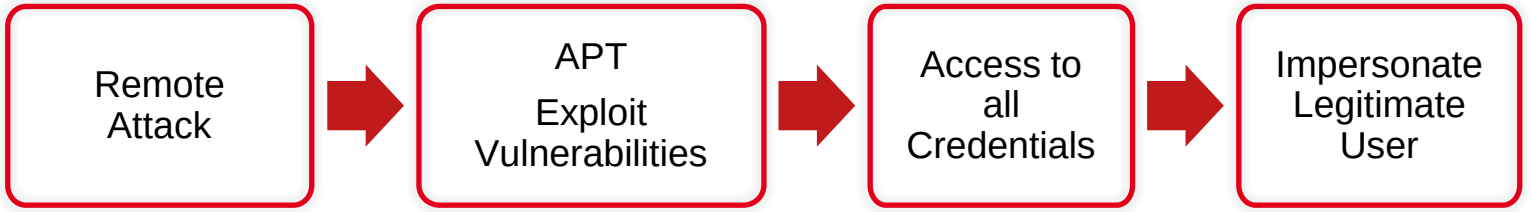
Angriff auf das Fahrzeug



Herausforderung #3 – Schutz von Zugangsdaten

Angriff auf Backend Systeme

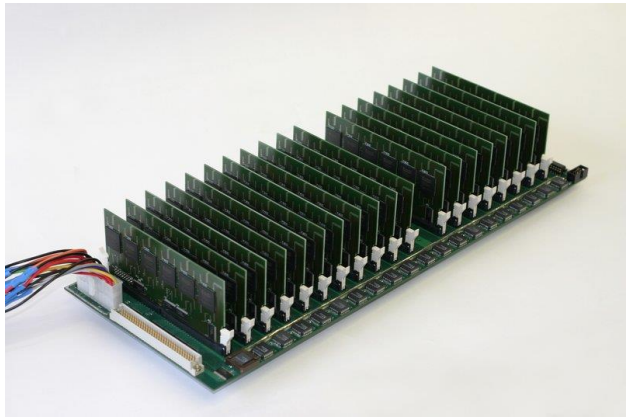
Sichere Generierung und Speicherung von Zugangsdaten erforderlich



Challenge #4 – Kryptographie

- Aktuelle Standards definieren feste kryptographische Algorithmen
- Kein Austausch von Algorithmen unterstützt
- Kryptografische Algorithmen können unsicher werden
  - Beispiel: Data Encryption Standard (DES) von 1977 wurde 20 Jahre später gebrochen
  - Quantencomputer bedrohen die Sicherheit der derzeit verwendeten Algorithmen

Kryptografische Agilität erforderlich



COPACOBANA: Günstige Plattform für schnelles Brechen von DES (2006)

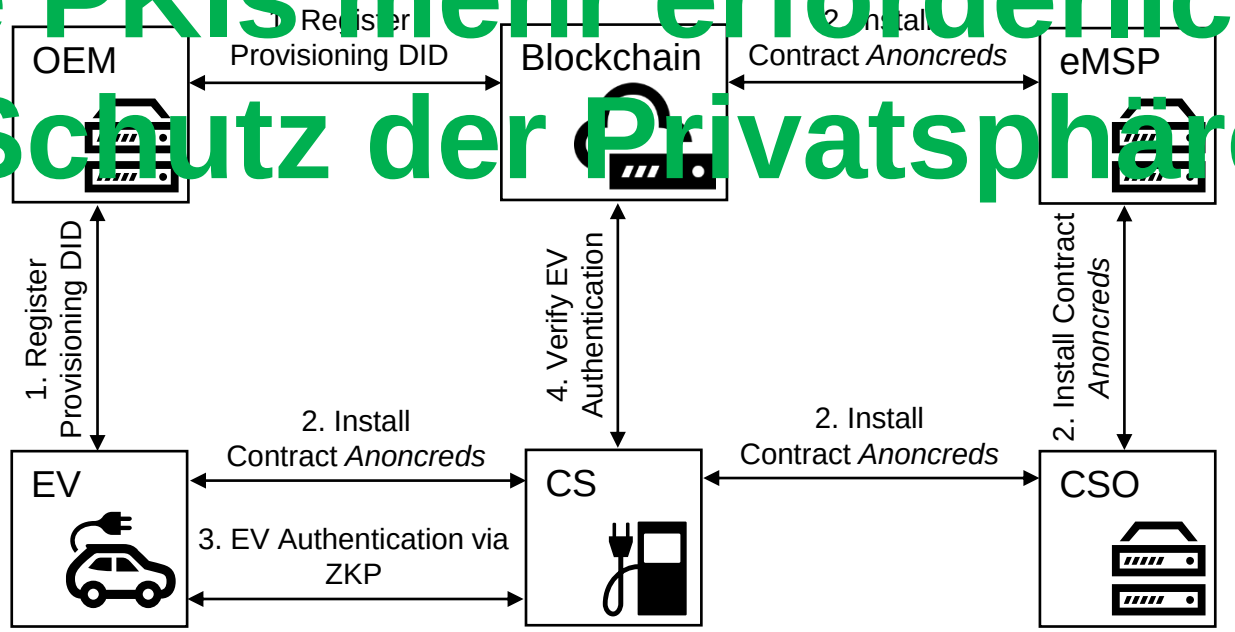
IBM Quantencomputer

Lösungen

Lösung 1: Self-Sovereign Identity (SSI) basiertes Laden
Komplexitätsreduzierung und Schutz personenbezogener Daten

- SSI-PnC [KKK24]
  - Ersetzen der PKI-basierten Authentifizierung durch SSI-basierte Authentifizierung
    - Decentralized Identifier (DID) ermöglicht Verifizierung ohne zentrale Stelle
    - Zero-Knowledge-Proof (ZKB)-basierte verifizierbare Nachweise „Anoncreds“
  - Datenschutzfreundliche Fahrzeugauthentifizierung (über Anoncreds)

Keine PKIs mehr erforderlich und Schutz der Privatsphäre



[KKK24] A. Kailus, D. Kern, C. Krauß. *Self-Sovereign Identity for Electric Vehicle Charging*. In 22nd International Conference on Applied Cryptography and Network Security (ACNS), 2024, to appear

Lösung 2: Protokollerweiterungen zum Datenschutz
Schutz personenbezogener Daten

- Datenschutzerweiterungen für ISO 15118
  - PnC mit Direct Anonymous Attestation (DAA) [ZSZK18]
  - Erweiterung für die gesamte Ladeinfrastruktur und weitere Dienstleistungen [KLK22]
- Entitäten können nur auf absolut notwendige Daten zugreifen

Schutz der Privatsphäre

	CP	CPO	CCH	eMSP
Cr[illegible] Provi[illegible]				
[illegible]ioning Certificate	(X)	(X)	(X)	X
Contract Credentials	(X)	(X)	(X)	X
Charge Authorization				
eMAID	(X)	(X)	(X)	X
Location	X	X	(X)	(X)
Time	X	X	X	X
Charge Billing (CDRs)				
eMAID	(X)	(X)	(X)	X
Location	X	X	(X)	(X)
Transaction Information	X	X	(X)	X

X = actor knows this personal data; arguably required for operation
(X) = actor knows this personal data; arguably not required for operation

Beispiel: Personenbezogene Daten in der Ladeinfrastruktur für Elektrofahrzeuge [KLK22]

[KLK22] D. Kern, T. Lauser, and C. Krauß. *Integrating Privacy into the Electric Vehicle Charging Architecture.* PoPETs, vol. 2022, no. 3, 2022.

[ZSZ18] D. Zelle, M. Springer, M. Zhdanova, C. Krauß. *Anonymous Charging and Billing of Electric Vehicles.* ARES, 2018.

Lösung 3.1: TrustEV
Schutz von ISO 15118-Zugangsdaten

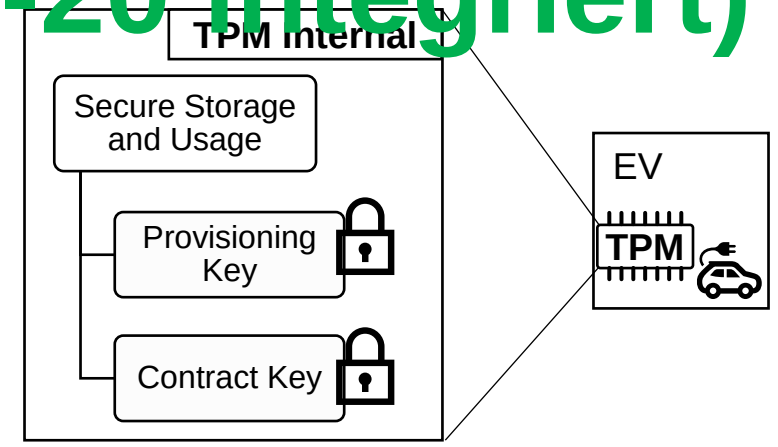
- TrustEV Sicherheitsarchitektur [FKK20a]
  - Sichere Bereitstellung, Speicherung und Nutzung von Zugangsdaten im Elektrofahrzeug
- Ansatz
  - Verwendung eines Hardware-Vertrauensankers: TPM 2.0
  - Neue X.509-Zertifikatserweiterung
  - Abwärtskompatible Protokollerweiterung
  - Minimaler Overhead

TrustEV schützt Zugangsdaten (und wurde in ISO 15118-20 integriert)

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

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

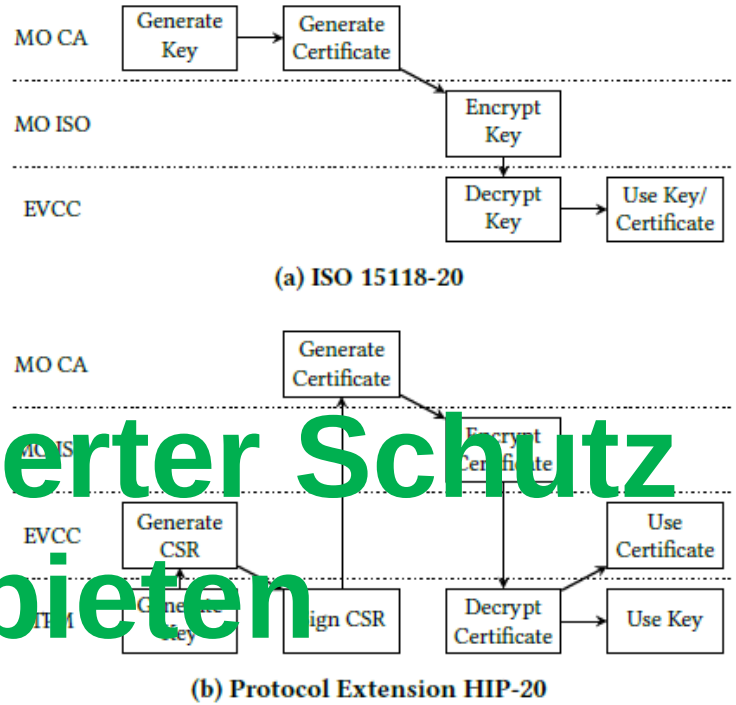


[FKK20a] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova. *TrustEV: Trustworthy Electric Vehicle Charging and Billing*. 35th ACM/SIGAPP Symposium on Applied Computing (SAC) - Computer Security (SEC), 2020

Lösung 3.2: HIP / HIP 2.0
Schutz von ISO 15118-Zugangsdaten

- HIP / HIP 2.0 [FKK20b, FKK20d]
  - Verbesserung von TrustEV
  - Schutz bei kompromittierten Backends
  - Sichere Schlüsselgenerierung im TPM des Fahrzeugs
    - Private Schlüssel verlassen niemals das TPM
    - Nur öffentliche Schlüssel werden im Backend gespeichert
  - Abwärtskompatibel
- HIP 2.0 bietet zusätzliche Funktionen, z.B.:
  - Unterstützung bei der Verwendung von Zertifikatspools
  - Einfache Integration in bestehende Zertifizierungsstellen (CAs) und Prozesse wie Certificate Signing Requests (CSRs)

HIP / HIP 2.0 würden erweiterter Schutz von Zugangsdaten bieten



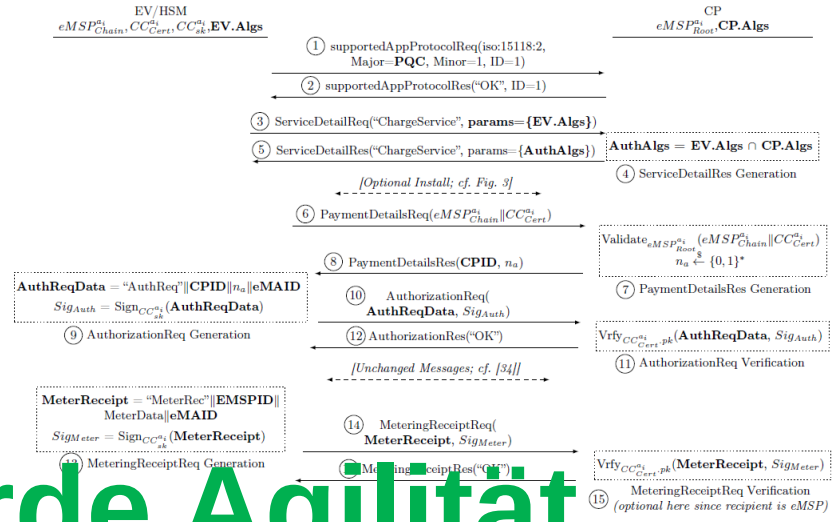
[FKK20b] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova. *HIP: HSM-based Identities for Plug-and-Charge*. 13th International Conference on Availability, Reliability and Security (ARES), 2020

[FKK20d] 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.

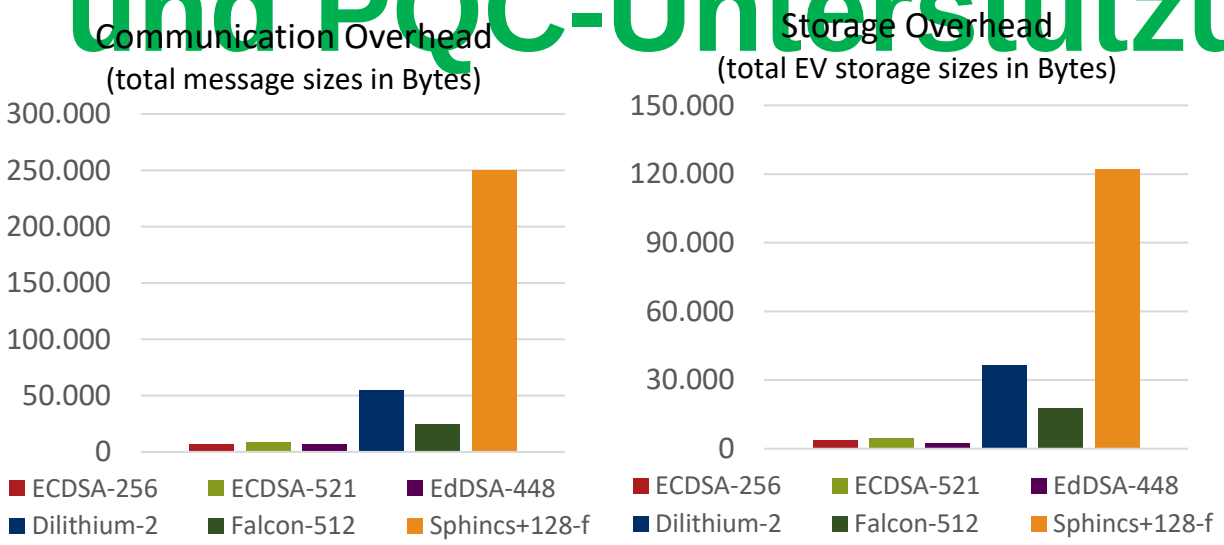
Lösung 4: QuantumCharge
Kryptografische Agilität und PQC-Integration

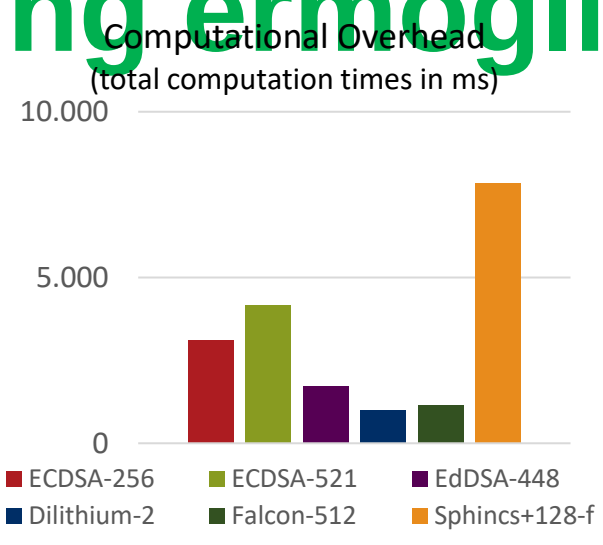
- QuantumCharge [KKL23]
  - ISO 15118-Erweiterung
    - Kryptografische Agilität durch Mechanismen zur Aushandlung von Algorithmen
    - Unterstützung für Post-Quanten-Kryptografie (PQC)
  - Prototypische Implementierung und formaler Sicherheitsnachweis

QuantumCharge würde Agilität und PQC-Unterstützung ermöglichen



Protocol flow when using contract credentials





[KKL23] D. Kern, C. Krauß, T. Lauser, N. Alnahawi, A. Wiesmaier, R. Niederhagen. *QuantumCharge: Post-Quantum Cryptography for Electric Vehicle Charging*, Applied Cryptography and Network Security (ACNS), 2023

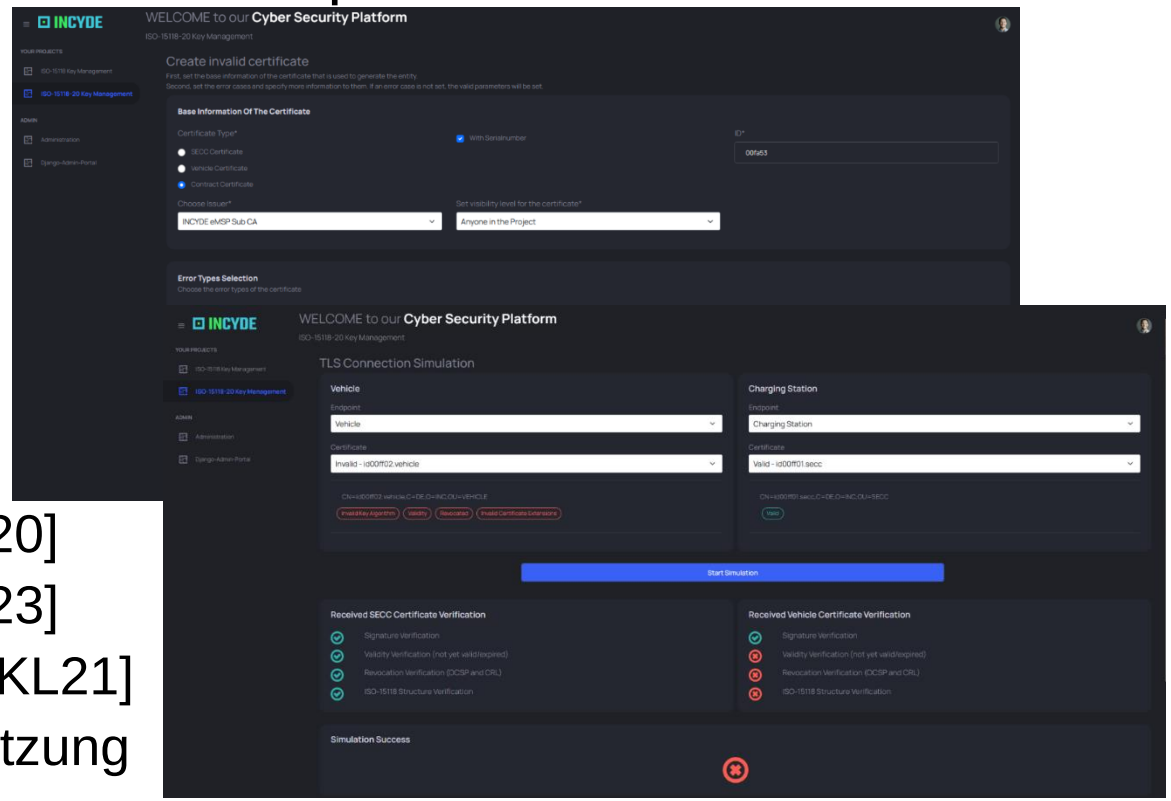
Fazit & Ausblick

Fazit

- „Intelligentes Laden“ ermöglicht Angriffe
  - Angriffe auf die Rechnungsstellung
  - Angriffe auf die Privatsphäre (Bewegungsprofile)
  - ...
- Sicherheits- und Datenschutzlösungen für
  - SSI-basiertes Laden [KKK24]
  - Schutz von Zugangsdaten [FKK20a, FKK20b, FKK20d]
  - Vertrauenswürdige Lade-Steuergeräte [FKK20c]
  - Kryptografische Agilität und PQC-Unterstützung [KKL23]
  - Datenschutzkonforme Abrechnung [KKK24, KLK22, ZSZ18]
  - Erkennung von Elektromobilitäts-basierten Angriffen auf Stromnetze [KK21, KKH23, KK23]
  - Absicherung von Ladestationen [KKZ19]
  - ...
- Forschungsergebnisse [FKK20a] wurden in ISO 15118-20 übernommen

Ausblick

- Ende-zu-Ende-Sicherheit für das Laden und Abrechnen
- Formale Analyse und Verbesserung weiterer Ladeprotokolle
- Praktische Sicherheitstests
  - Aktueller Systeme
  - Nutzung unser INCYDE Cyber Sicherheits-Platform



- Weitere Forschungsthemen
  - Analyse von Automotive-Protokollen [LZK20]
  - Analyse des Diagnoseprotokolls UDS [LK23]
  - Analyse und Erweiterung von SOME/IP [ZKL21]
  - Kryptografische Agilität und PQC-Unterstützung im Bordnetz [BKN20]

Literatur

Literatur

[BKN20] K. Bürstinghaus-Steinbach, C. Krauß, R. Niederhagen, M. Schneider. *Post-Quantum TLS on Embedded Systems: Integrating and Evaluating Kyber and SPHINCS + with mbed TLS*. In 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS), 2020

[FKK20a] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova. *TrustEV: Trustworthy Electric Vehicle Charging and Billing*. In 35th ACM/SIGAPP Symposium on Applied Computing (SAC) – Computer Security (SEC), 2020

[FKK20b] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova*. HIP: HSM-based Identities for Plug-and-Charge*. In 15th International Conference on Availability, Reliability and Security (ARES), 2020

[FKK20c] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova. *Securing Electric Vehicle Charging Systems through Component Binding*. In 39th International Conference on Computer Safety, Reliability and Security (SAFECOMP), 2020

[FKK20d] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova, R. Heddergott. *HIP-20: Integration of Vehicle-HSM-Generated Credentials into Plug-and-Charge Infrastructure.* In 4th ACM Computer Science in Cars Symposium (CSCS), 2020

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

[ISO22] ISO / IEC. *ISO 15118-20:2022 Road vehicles - Vehicle to grid communication interface - Part 20: 2nd generation network layer and application layer requirements*, 2022

[KK21] D. Kern, C. Krauß. *Analysis of E-Mobility-based Threats to Power Grid Resilience.* In 5th ACM Computer Science in Cars Symposium (CSCS), 2021

[KKH23] D. Kern, C. Krauß, M. Hollick. *Detection of Anomalies in Electric Vehicle Charging Sessions*. In 39th Applied Computer Security Applications Conference (ACSAC), 2023, to appear

[KK23] D. Kern, C. Krauß. *Detection of e-Mobility-based Attacks on the Power Grid*. In 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2023

[KKL23] D. Kern, C. Krauß, T. Lauser, N. Alnahawi, A. Wiesmaier, R. Niederhagen. *QuantumCharge: Post-Quantum Cryptography for Electric Vehicle Charging.* In 21st International Conference on Applied Cryptography and Network Security (ACNS), 2023

[KKK24] A. Kailus, D. Kern, C. Krauß. *Self-Sovereign Identity for Electric Vehicle Charging*. In 22nd International Conference on Applied Cryptography and Network Security (ACNS), 2024, 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

[KLK22] D. Kern, T. Lauser, and C. Krauß. *Integrating Privacy into the Electric Vehicle Charging Architecture.* In Proc. on Priv. Enhancing Technol. (PoPETs), vol.2022, no.3, 2022

[LK23] T. Lauser, C. Krauß. *Formal Security Analysis of Vehicle Diagnostic Protocols*. In 18th International Conference on Availability, Reliability and Security (ARES), 2023

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

[ZKL21] D. Zelle, D. Kern, T. Lauser, and C. Krauß. *Analyzing and Securing SOME/IP Automotive Services with Formal and Practical Methods*. In 16th International Conference on Availability, Reliability and Security (ARES), 2021

[ZSZ18] D. Zelle, M. Springer, M. Zhdanova and C. Krauß. *Anonymous Charging and Billing of Electric Vehicles.* In 13th Int. Conference on Availability, Reliability and Security (ARES), 2018

Kontakt

Prof. Dr. Christoph Krauß
Head of ACSD Research Group
Darmstadt University of Applied Sciences
Schöfferstr. 3, D-64295 Darmstadt
christoph.krauss@h-da.de
https://acsd.h-da.de

h_da
darmstadt university
of applied sciences

Prof. Dr. Christoph Krauß
Head of Automotive Security Research
INCYDE GmbH
Rheinstr. 16a, D-64283 Darmstadt
christoph.krauss@incyde.com
https://incyde.com

INCYDE