Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

DELTA

Handlungsempfehlungen des Förderprojekts DELTA

DKE VDE DIN · FKFS · Fraunhofer SIT · innogy · ITSEC · webolution

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

DELTA

Datensicherheit und -integrität in
der Elektromobilität beim Laden
und eichrechtkonformen Abrechnen

Impressum

Autoren:
Frank Brosi, Forschungsinstitut für Kraftfahrwesen und Fahrzeugmotoren Stuttgart FKFS
Andreas Harner, DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
Prof. Dr. Christoph Krauß, Fraunhofer-Institut für Sichere Informationstechnologie SIT
Christian Seipel, DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
Markus Springer, Fraunhofer-Institut für Sichere Informationstechnologie SIT
Michael Staubermann, Webolution GmbH
André Suhr, Itsecworld
Stephan Voit, innogy SE
Maria Zhdanova, Fraunhofer-Institut für Sichere Informationstechnologie SIT

Herausgeber und Ansprechpartner:
DKE Deutsche Kommission Elektrotechnik
Elektronik Informationstechnik in DIN und VDE
Christian Seipel,
Stresemannallee 15
60596 Frankfurt am Main
Telefon 069 6308-454
Christian.seipel@vde.com
https://www.dke.com

Diese Publikation ist im Rahmen des Förderprogramms „Elektro Power II“ im Verbundprojekt „Datensicherheit- und integrität in der Elektromobilität beim Laden und eichrechtskonformen Abrechnen“ (kurz: DELTA) erstellt worden. Sie ist kostenfrei erhältlich.

Erscheinungsdatum: Dezember 2018

Einleitung

Sowohl während der Fahrt als auch beim Ladevorgang tauschen Elektrofahrzeuge Daten aus. Dabei kommt der Datensicherheit und dem Datenschutz eine äußerst zentrale Rolle zu. Nur bei der Gewährleistung dieser Aspekte kann eine korrekte Abrechnung, ein sicheres Laden für Nutzer und Anbieter und der metrologische Verbraucherschutz sichergestellt werden. Ein valides Datensicherheits- und Datenschutzkonzept zur Einbindung der Elektrofahrzeuge in das intelligente Energienetz (Smart Grid) bildet die Grundlage zum Laden sowie für die Etablierung und Nutzung von Mehrwertdiensten. So wird Elektromobilität komfortabel und sicher und letztendlich vom Bürger akzeptiert. Dies stellt die gesellschaftliche Grundlage für eine Marktdurchdringung der Elektromobilität dar. Hier setzte das vom Bundesministerium für Wirtschaft und Energie initiierte Förderprojekt DELTA an.

Die vorliegenden Handlungsempfehlungen basieren auf den Ergebnissen dieses Projekts. Dazu zählen u.a. eine Sammlung von relevanten Anwendungsfällen (Use Cases) im Kontext Laden und Abrechnen, Referenzarchitekturen für domänenspezifische Funktions-und Komponentenschichten, Entwürfe von Schutzprofilen für Komponenten der Ladeinfrastruktur und grundlegende funktionale Sicherheitsanforderungen. Die Handlungsempfehlungen betrachten die kontinuierliche Weiterentwicklung dieser Arbeiten und beziehen sich auf den erreichten Entwicklungsstand der Elektromobilität und insbesondere der Ladeinfrastruktur von Ende 2018. Die Empfehlungen adressieren Handlungsfelder für Politik, Normung/Standardisierung, Ladeeinrichtungshersteller und Automobilhersteller, sowie für zukünftige Förderprojekte. Damit können die Voraussetzungen geschaffen werden die Elektromobilität IT-sicher in den Markt zu bringen um Nachhaltigkeit und Investitionssicherheit für alle beteiligten Industrien zu gewährleisten.

Kurzfassung

Handlungsempfehlungen an die Politik

- Abfrage von bezogenen und gelieferten Strom- und Spannungswerten über eine Prüfschnittstelle ermöglichen (I.1)
- Ermöglichen einer Überprüfung des Gesundheitszustandes der Batterie für Fahrzeughalter und unabhängige Dritte (I.2)
- Novellieren des Rechtsrahmens zur Schaffung einer einheitlichen Systematik, Transparenz, Verbrauchernähe und Praxistauglichkeit (I.3)
- Ermöglichen von regelmäßigen Überprüfungen innerhalb des Lebenszyklus der Ladeinfrastruktur mittels Sicherheitsaudits und Penetrationstests (I.4)
- Vorgaben an die Verarbeitung personenbezogener Daten und Zertifizierung der Roaming-Dienstleister (I.5)
- Bereitstellung einer PKI für die Kommunikation der Nutzerautorisierung (I.6)
- Anpassung der Technischen Richtlinien und Schutzprofile des SMGW nach MsbG [1] für die Verwendung in öffentlichen Ladepunkten (I.7)

Handlungsempfehlungen an die Normung/Standardisierung

- Entwicklung von Normen für das netzdienliche Einspeisen von Energie aus Elektrofahrzeugen (II.1)
- Entwicklung von Normen zur Sicherstellung von Mindeststandards zur IT-Sicherheit auf dem Stand der Technik (II.2.1)
- Erstellen von Produktnormen für die Elektromobilität unter Berücksichtigung von Datenschutz, Eichrechtskonformität, Safety und Security by Design und Kryptoagilität (II.2.2)
- Berücksichtigung der Langzeitsicherheit, inkl. Migrationsstrategien für kryptographische Verfahren sowie der Post-Quantenkryptografie in der Normung (II.3)
- Entwicklung automatisierter datenschutzkonformer Nutzerautorisierung (II.4)
- Verstärkt die neuen Stakeholder im Umfeld der Elektromobilität für Normung und Standardisierung gewinnen, um nachhaltige und investitionssichere Lösungen zu schaffen (II.5)
- Förderung etablierter und offener Ansätze und Verfahren der IT-Sicherheit, so dass keine proprietären Verfahren in Normen und Standards die Entwicklung verzögern oder sich gar Monopole bei Herstellern ergeben (II.6)

Handlungsempfehlungen an Ladesäulenhersteller/-betreiber und Automobilhersteller

- Verwendung von zertifizierten Sicherheitsmodulen zur Absicherung der Kommunikation über externe Schnittstellen des Fahrzeugs (III.1)
- Implementieren von Privacy Enhancing Technologies (PETs) zum datenschutzwahrenden Laden und Abrechnen (III.2)
- Hardware- und softwareseitige Separierung von safety- oder security-kritischen Anwendungen zur Aufwandsreduzierung von Zertifizierungen oder Rezertifizierungen (III.3)

Handlungsempfehlungen an zukünftige Förderprojekte

- Berücksichtigung des Rechtsrahmens in Fördermaßnahmen (IV.1)
- Berücksichtigung der Normung/Standardisierung in Fördermaßnahmen (IV.2)
- Förderung von Maßnahmen für einen einheitlichen Fachwortschatz (IV.3)
- Förderung der Forschung im Bereich anonymer Bezahlverfahren (IV.4)
- Förderung von vertrauensvollen Plattformen für eine geordnete, vertrauenswürdige und unternehmensübergreifende Zusammenarbeit im Rahmen des Schwachstellenmanagements (IV.4)

Inhaltsverzeichnis

I. Handlungsempfehlungen an die Politik

I.1 Prüfschnittstelle für Strom- und Spanungssollwerte beim Laden

Die Entwicklung und Nutzung des In-Kabel-Messsystems (InKaMs) der PTB im Rahmen des Projektes DELTA zeigte, dass für die Interpretation der Messwerte die gelieferten Strom- und Spannungswerte (Soll- und Istwerte), sowie die vereinbarten Tarifinformationen notwendig sind. Die Interpretation dieser Messungen unterstützt die Diagnose von Fehlern im Feld und die Konformitätsbewertung der Ladeeinrichtungen. Die zusätzlichen notwendigen Informationen für die Interpretation sollen über eine geeignete Prüfschnittstelle von berechtigten Personen und Institutionen auslesbar sein.

Der Politik empfehlen wir auf eine Vorschrift zur Abfrage von bezogenen und gelieferten Strom- und Spannungswerten und vereinbarten Tarifinformationen, über eine zu definierende Prüfschnittstelle zwecks Diagnose- und Konformitätsbewertung, zu drängen. Auf Seite der Ladeinfrastruktur fehlt derzeit hierzu eine interoperable, genormte und vorgeschriebene Prüfschnittstelle. Auf Fahrzeug Seite schlagen wir vor, die Vorschriften zur Onboard-Diagnose-Schnittstelle (OBD) entsprechend zu erweitern.

I.2 Transparenz über den Batteriezustand für den Letztverbraucher

Für eine Batteriebewertung, zum Beispiel für den Verkauf eines Fahrzeuges, ist die Abfrage des State of Health (SoH) der Batterie interessant. Diese Information sollte visuell über die Bedienelemente des Fahrzeugs und/oder über eine definierte Schnittstelle, wie z.B. OBD, bereitgestellt werden.

Für eine Bewertung der Batterie durch unabhängige Dritte, wie einer Aufsichtsbehörde oder einer Prüfgesellschaft, sind die Spannungs- und Stromwerte der Batterie des Fahrzeuges, insbesondere beim Laden und beim Stillstand des Fahrzeuges, hilfreich. Ein solches Verfahren ist zum Beispiel in der Dissertation „Beitrag zur Bewertung des Gesundheitszustands von Traktionsbatterien in Elektrofahrzeugen“ von Phan-Lam Huynh [2] beschrieben. Mit einem geeigneten Zugriff auf die Zellspannungen werden detailliertere Bewertungen der Batterien erzielt.

Die Politik sollte darauf drängen, dass dem Fahrzeughalter eine Möglichkeit zur Überprüfung des SoH bereitgestellt wird. Darüber hinaus sollte es berechtigter unabhängigen Dritten (z. B. Sachverständige) ermöglicht werden, den Gesundheitszustand der Batterie zu bewerten. Dies ist in Hinblick auf den Gebrauchtwagenmarkt und Gebrauchtakkumarkt sinnvoll. Neben einem ersten Schritt der Bereitstellung der Strom- und Spannungswerte ist dazu die weitere Unterstützung der Forschung zu empfehlen.

I.3 Rechtliche Regulierung für Elektromobilität

Die rechtliche Regulierung im Bereich der Elektromobilität ist über zahlreiche Vorschriften (MsbG, EU-DSGVO [3], MessEG [4], PAngV [5], LSV [6]) mit jeweils unterschiedlicher Granularität verteilt, was eine erschwerte Systematisierbarkeit zur Folge hat. Auf dieser Erkenntnis basierend wird folgende Handlungsempfehlung gegeben:

Ein kompliziertes rechtliches Regelungsgefüge und damit verbundene juristische Unsicherheiten dürfen nicht zu Innovationshemmnissen führen! Deshalb besteht zeitnaher Bedarf, das Regelungsgefüge zur E-Mobility zu novellieren. Im Mittelpunkt stehen sollten dabei eine einheitliche Systematik, Transparenz sowie Verbrauchernähe und nicht zuletzt eine weitaus stärkere Praxistauglichkeit der gesetzlichen Vorgaben als bisher. Das Gesetz zur Digitalisierung der Energiewende stellt lediglich einen ersten Ausgangspunkt dar, weshalb in Zukunft sogar zu überlegen wäre, spezialgesetzliche (Datenschutz-)Regelungen zu den Anwendungsfeldern, Verarbeitungen und berechtigten Akteuren beim Laden & Abrechnungen in der E-Mobility zu kodifizieren, sodass alle Anwendungsfelder, Prozesse und Akteure in einem ausreichenden Maße berücksichtigt und Schnittstellen genutzt werden. Gleichzeitig müssen neue gesetzliche Vorgaben aber auch in einem hinreichenden Maße technologieoffen ausgestaltet sein. Über unbestimmte Rechtsbegriffe und Generalklauseln ist dabei ein umfassender Bezug zur technischen Normung und Standardisierung sicherzustellen.

I.4 Regelmäßige Überprüfungen

Um den State of the Art der IT-Sicherheit von vernetzten Fahrzeugen, Systemen und Komponenten der Ladeinfrastruktur über den gesamten Lebenszyklus zu gewährleisten, sollten rechtliche Vorgaben Mindeststandards festlegen.

Während Schutzprofile nach Common Criteria in der Lage sind Sicherheitsanforderungen an Produkte zu definieren, so sollten diese wiederum keine direkte Anforderung an deren Umsetzung stellen. Diese werden grundsätzlich durch technische Richtlinien vorgegeben. Dabei herrschen weiterhin viele Freiheitsgrade bezüglich der finalen Implementierung durch den Hersteller, die zu Fehlern führen könnten. Auch Schwachstellen durch Implementierungsfehler stellen hierbei ein Risiko dar. Um diese Probleme zu umgehen, ist es sinnvoll, zusätzlich vor der Marktzulassung eines neuen Produktes Security Audits und Pentests durchzuführen. Diese helfen, etwaige Bugs und Sicherheitsprobleme schon vor dem Ausbringen der teuren Hardware/Ladesäulen zu finden.

Vor allem vor dem Hintergrund der langen Lebensdauer der Ladesäulen, ist es sinnvoll, auch nach deren Ausbringung in regelmäßigen Abständen eine solche Überprüfung durchzuführen. Da Ladesäulen eine Schnittstelle zu kritischen Infrastrukturen, genauer gesagt dem Energienetz, darstellen und künftig als Kritische Infrastruktur angesehen werden können, sind diese ein interessantes Angriffsziel für allerlei unterschiedliche Angreifer, deren Motivation von reinem Betrug bei der Abrechnung bis hin zum Angriff des Energienetzes reichen kann. Zudem zeigt die jüngste Vergangenheit (z.B. Spectre & Meltdown), dass gerade im informationstechnischen Bereich immer wieder Sicherheitsprobleme gefunden werden, welche schon lange vorhanden sind, aber bisher nicht öffentlich bekannt waren. Daher sollten Ladesäulen im Rahmen ihres Lebenszyklus immer wieder in regelmäßigen Abständen überprüft werden, um mögliche Angriffsflächen, die evtl. auch nicht von Schutzprofilen abgedeckt werden können, zu verhindern. Eine rechtliche Bindung sollte dabei über das Messstellenbetriebsgesetz stattfinden, welches den Betrieb von Ladesäulen regelt.

Es wird empfohlen, einen Rechtsrahmen zu definieren, der die Mindestdauer festlegt, in der die OEMs, Hersteller der Ladeinfrastruktur verpflichtet sind sicherheitsrelevante Updates zur Verfügung zu stellen..

I.5 Roaming

Die Aufgaben des Roamings- und E-Mobility-Providers sollten im Rechtsrahmen definiert werden.

Der Rechtsrahmen sollte einen einheitlichen Katalog von erforderlichen Verarbeitungszwecken für das Roaming definieren, so dass keine informierten Einwilligungen für das Roaming für den Ladevorgang erhoben werden müssen. Aufgrund der derzeitigen Vielfalt der beim Roaming eingesetzten Protokolle kann eine Konvertierung der Datenformate durch Roaminganbieter notwendig sein. Sollte dabei eine Entschlüsselung und Neuverschlüsselung der Daten erforderlich werden, muss klar sein, dass es sich dabei um eine Auftragsdatenverarbeitung handelt. Auf lange Sicht muss dennoch eine europäische Interoperabilität der Ladepunkt- bzw. Roamingprotokolle hergestellt werden, die eine solche Konvertierung vermeidet, um den umfänglichen Datenschutz zu gewährleisten.

Da Roamingdienstleister eine zentrale Stelle einer großen Menge von verarbeiteten Daten sind, sollte der Rechtsrahmen klarstellen, dass Roaming-Dienstleister eine ISMS-Zertifizierung zu IT-Sicherheit und Datenschutz nachweisen müssen.

Durch Verwendung einer interoperablen (einheitlichen) „Marktkommunikation“ für die Nutzerautorisierung, Abrechnung und SmartCharging-Teilnahme ist eine Ende-Zu-Ende Verschlüsselung zwischen den Ladeinfrastruktur-Teilnehmern möglich. Damit ist für Authentizität, Nicht-Abstreitbarkeit und Vertraulichkeit eine technische Lösung statt einer organisatorischen Lösung möglich, die die Anfälligkeit für organisatorische Schwachstellen beim Roaming-Dienstleister minimiert.

I.6 Public Key Infrastructure (PKI)

Für die Nutzerauthentifizierung und -autorisierung wird eine europäische und/oder nationale PKI benötigt. Mögliche Teilnehmer sind die E-Mobilisten, Fahrstromanbieter/Ladedienstanbieter, Ladepunkte, OEMs, Ladepunktbetreiber, Roaming-Dienste.

Die Services der PKI dienen als Grundlage:

- der Absicherung (Authentifizierung, Integritätssicherung und Verschlüsselung) der Kommunikation zwischen den Teilnehmern
- der Authentifizierung der Fahrzeugnutzer (bei Plug & Charge und Karten- oder App-basiertem Bezahlen)
- der Nicht-Abstreitbarkeit von Mess- und Abrechnungsdaten

I.7 Verknüpfung mit den BSI/BMWi-Projekten zur Digitalisierung der Energiewende

Für die BSI/BMWi-Projekte zur Digitalisierung der Energiewende und insbesondere für den Einsatz der SMGW-Kommunikationsplattform im Bereich Smart Mobility können die Projektergebnisse aus DELTA eine fundierte und umfangreiche Quelle darstellen. Zu den Projektergebnisse für eine weitere Ausgestaltung der BSI/BMWi-Projekte gehören u.a.:

- Anwendungsfälle beim Laden und Abrechnen zur Identifikation der domänenspezifischen Funktionalitäten
- Glossar zur Identifikation der domänenspezifischen Rollen und Objekte
- Referenzarchitekturen für domänenspezifische Funktionale- und Komponentensichten, um eine Abgrenzung hinsichtlich der MsbG/GDEW [7] Anforderungen zu treffen
- Entwürfe von Schutzprofilen für Komponenten der Ladeinfrastruktur (Ladecontroller im Fahrzeug, Ladecontroller und Messung im Ladepunkt und im Backendsystem) für die grundlegenden funktionalen Sicherheitsanforderungen, schützenswerten Daten und der Definition des zu lösenden Sicherheitsproblems
- Identifizierung vorhandener Standards zur Bestimmung des Standardisierungs-Scopes
- Identifizierung des recherchierten domänenspezifischen Rechtsrahmens

I.8 Empfehlungen für BSI und Regelermittlungsausschuss der PTB für das MessEG zum Einsatz in der Elektromobilität

Aus den ermittelten Anwendungsfällen (u.a. für die Fahrstrommessung und –abrechnung) lautet die Empfehlung, folgende Merkmale in den technischen Richtlinien des BSI und den Dokumenten des Regelermittlungsausschuss der PTB zu berücksichtigen:

- Abrechnung nach Zeitdauer einer Dienstleistung
- Keine Bindung an ein 15 Minuten Registrierperiodenraster
- Messperiode an Start/Ende des Ladevorganges gekoppelt
- Unterstützung nicht-stationärer und nicht-vertraglich gebundener Energienutzer
- Anforderungen zur Kommunikationssicherheit einer modernen Messeinrichtung für Elektromobilität festlegen
- Anforderungen an die Zertifizierung von Komponenten für die Messung- und Abrechnung von Elektromobilitätsdiensten festlegen, um Transparenz und Vergleichbarkeit der durchgeführten Konformitätstests zu erhalten

- Festlegen von Übergangsfristen für vorhandene Ladepunkte
- Aufzeigen von Migrationspfaden über die Förderrichtlinien zur öffentlichen und privaten Ladeinfrastruktur
- Anpassung der Betriebsumgebung der Schutzprofile nach MsbG auf den Betrieb in einer öffentlichen Ladesäule
- Der CSO (Betreiber des Ladepunktes, aus LSV) kann als (wettbewerblicher) MSB das SMGW[1] für den Netzanschluss des Ladepunktes administrieren. Die Nutzbarkeit des SMGW für die Lade- und Versorgungsenergiemessung ist im Schutzprofil und den Technischen Richtlinien zu ermöglichen. Die Nutzung des SMGW für die Fahrstrommessung ist im Rechtsrahmen mindestens zu ermöglichen und klarzustellen.
- Nutzung eines für öffentliche Ladeeinrichtungen angepassten SMGW als sichere Kommunikationseinheit bei der Anbindung von Ladepunkten (als Verbrauchs- oder Erzeugungsanlage) an das Energienetz
    - Trennung der Kommunikationsflüsse der WAN-, Fahrzeug- und Messgeräte-Schnittstelle durch die sichere Kommunikationseinheit
    - Alleinige Erfassung und Verarbeitung von Messwerten im SMGW für öffentliche Ladeeinrichtungen
- Bereichsspezifische Datenschutzregeln zur Verarbeitung von Mobilitätsdaten für Abrechnungszwecke (gesetzliche Zwecke, Nennung der Rollen, Aufbewahrungsfristen)

[1] Unter der Vorrausetzung das die technischen Richtlinien und Schutzprofile des SMGW für die Verwendung in der Ladeinfrastruktur der Elektromobilität angepasst werden.

II. Handlungsempfehlungen an die Normung/Standardisierung

II.1 Rückspeisung

Bezüglich des Einspeisens von Wechselstrom sind viele länderspezifische Vorschriften vorhanden. Für das "Rückspeisen" von Energie aus Elektrofahrzeugen sollte eine Vereinheitlichung der Vorschriften erfolgen. Ziel dieser Vereinheitlichung muss es sein, die lokalen Bestimmungen über wenige Parameter zu definieren. Diese Parameter sollen die Grenzwerte für Spannung, Frequenz, genehmigter Phasenverschiebung (Kosinus φ) und Oberwellen (Total Harmonic Distortion, THD) bestimmen. Die Vereinheitlichung erleichtert durch die Begrenzung der Parameter die Überwachung auf Einhaltung der Vorschriften über Ländergrenzen hinweg.

Eine Anpassung an lokale Gegebenheiten des Netzes wird durch die Vereinheitlichung dadurch erleichtert, dass notwendige Parameter bekannt und standardisiert sind. Darauf aufbauend kann die Kommunikation zwischen Ladepunkt und Fahrzeug entsprechend standardisiert werden. Dies ist eine Vorrausetzung für ein netzdienliches Einspeisen aus Elektrofahrzeugen. Die Möglichkeiten der so erweiterten Kommunikation, können z.B. dazu genutzt werden, eine Stabilisierung des Netzes, (Kosinus φ Korrektur) mittels der Power Factor Correction (PFC) Einheiten der Fahrzeuge zu realisieren.

Das netzdienliche Einspeisen aus Elektrofahrzeugen muss darüber hinaus in den Normen und Standards berücksichtigt werden. Die Standardisierung hat dabei unter anderem auf die Konformität bezüglich des Mess- und Eichrechts, der EMV-Vorschriften eines Einspeisemanagement und auf das lokale Energiemanagement zu achten. Das netzdienliche Einspeisen lag nicht im Fokus des Projekts DELTA, es werden weitere Untersuchungen empfohlen.

II.2 Produktnormen

Mit der Analyse der IEC 62443 bezüglich Übertragbarkeit in die Elektromobilität wurden in DELTA grundlegenden Sicherheitskonzepte untersucht. Für eine konkrete Hilfestellung für Hersteller, Integratoren und Betreiber im Umfeld der Elektromobilität fehlt es aber noch an Guidelines bzw. Umsetzungshinweisen. Die Empfehlung lautet, (vor) normative Dokumente zu entwickeln, die neben den technischen Sicherheitsanforderungen auch organisatorische Anforderungen enthalten und zusätzlich spezifische Anforderungen an Datenschutz (Privacy), Eichrechtskonformität sowie Safety & Security by Design berücksichtigen. Hierbei gilt es insbesondere die Policies bzgl. Patchmanagement zu untersuchen und ebenso Anforderungen an Komponenten mit Blick auf einen sicheren Produktlebenszyklus zu definieren. Von großer Wichtigkeit ist die Kompatibilität zu weiteren bestehenden Normen neben der IEC 62443 [8]: Die IEC 62351 [9] beschreibt technische Sicherheitslösungen für die Kommunikation in der Energieversorgung. Daraus können Sicherheitsanforderungen und Lösungsansätze für eine sichere Kommunikation im Ökosystem Elektromobilität abgeleitet werden. Die ISO/IEC 27019 [10] als branchenspezifischer Sicherheitsstandard der Energieversorgung beschreibt ein ISMS auf Grundlage der ISO/IEC 27000 [11] Reihe. Weiterhin müssen Maßnahmen zum Vorgehen bei Angriffen bzw. Vorfällen untersucht und beschrieben werden. Es muss zudem möglich sein, aufgrund der großen Lebensdauer von Ladesäulen und Fahrzeugen Softwareupdates und Hardwareupdates vorzunehmen, die u.a. ein Updaten der eingesetzten Kryptographie ermöglicht. Dies bezieht sich nicht nur auf Post-Quantenkryptographie sondern auch auf die generelle Kryptoagilität; Austausch von Schlüsseln, Wechsel auf längere Schlüssel, Wechsel von Protokollen und Verfahren, und sichere Over-the-Air Updates (siehe Kapitel II.3).

II.3 IT-Sicherheit über den Lebenszyklus/Langzeitsicherheit

Da die Nutzungszeit der Ladeinfrastruktur einen langen Zeitraum umfasst, muss dies bei der Realisierung der IT-Sicherheitsmaßnahmen berücksichtigt werden. Dies umfasst neben der Möglichkeit (remote) Updates einzuspielen auch Maßnahmen zum Austausch gebrochener kryptographischer Schlüssel oder gar Verfahren.

Ebenfalls relevant ist, dass die Nutzungszeit länger als der prognostizierte Zeitpunkt der praktischen Verfügbarkeit von Quanten-Computern zur Infragestellung der Vertrauenswürdigkeit vertraulicher Kommunikation ist. Deshalb müssen innerhalb von höchsten 5 Jahren in der Standardisierung und innerhalb von höchstens 10 Jahren in der Implementierung Voraussetzungen für die Migration zu Post-Quantenkryptographie (PQ) und -Protokollen geschaffen werden.

Das Ziel sollte dabei die Vorbereitung der Migration heutiger kryptografischer Verfahren, Sicherheitsprotokollen und Vertrauensmodellen (PKI) sein. Es muss ein Bewusstsein (Awareness) für die möglichen gebrochener Verfahren sowie die Ankunft von Quantenrechnern, welche Post-Quantenkryptographie notwendig machen, geschaffen werden. Empfohlen wird für die Übergangszeit die Verwendung von Hybridverfahren, bei denen sowohl ECC- bzw. RSA-basierte Signaturverfahren und Verschlüsselungsverfahren als auch Post-Quantenverfahren ausgewählt werden können [12].

Um den Stand der Technik bezüglich IT-Sicherheit über den gesamten Lebenszyklus von Fahrzeugen und Ladesäulen zu gewährleisten, ist es wichtig, Langzeitsicherheit und Kryptoagilität zu betrachten. Dabei wird diese Agilität in der Normung durch die Anwendung von Vornormen und Anwendungsregeln, unterstützt.[2]

Komponenten der Ladeinfrastruktur sind über lange Zeit im Einsatz. Da sich die Bedrohungslage ständig ändert und ehemals als sicher eingestufte Verfahren mittels neuer Angriffsmethoden gebrochen werden könnten, müssen diese Komponenten so entwickelt werden, dass sie an die zukünftigen Anforderungen angepasst werden können. Die Herausforderung IT-Systeme mit langer Lebensdauer sicher zu betreiben ist besonders hoch, weil der Mindeststandard zur IT-Sicherheit über den gesamten Lebenszyklus gewährleistet sein muss. Gleichzeitig muss dieser Mindeststandard stetig auf den aktuellen Stand der Technik angepasst werden.

Deshalb müssen geeignete Verfahren für agile Anpassung und Migration von Protokollen und Kryptographie in die Komponenten der Ladeinfrastruktur von Anfang an integriert werden. Dies gilt sowohl für die System- als auch für die Kommunikationssicherheit.

Auch die Langzeitkryptographie muss stets mitbetrachtet werden: Alle Daten, die heute verschlüsselt werden, könnten entweder bei deren Übertragung abgefangen oder von Speichermedien kopiert und gespeichert werden. Später, wenn die dafür notwendigen Werkzeuge verfügbar sind, können diese dann vom Angreifer entschlüsselt werden. Dies hat zur Folge, dass eventuell weitere Anforderungen bzgl. des Datenschutzes (z.B. Anonymisierung/Pseudonymisierung) berücksichtigt werden müssen.

II.4 Nutzerauthentifizierung

Eine Nutzerauthentifizierung (automatisiert nach ISO 15118 [13] oder bei punktuellem Aufladen) an der Ladeinfrastruktur sollte folgende Kriterien erfüllen:

- einheitliche Standardisierung[3]
- sichere und datenschutzkonforme Verfahren (unterstützt durch Privacy Enhancing Technologies, siehe Kapitel 4.4)
- nutzerfreundliche Handhabung
- europäisch akzeptierte Verfahren zur nicht-abstreitbaren Autorisierung von punktuell nutzbaren Ladedienstleistungen bzw. Ladevorgängen

[2] Im Rahmen von DELTA ist mit der VDE-Anwendungsregel VDE-AR-E 2802-100-1 ein vornormatives Dokument entstanden, das den Ansatz der entwicklungsbegleitenden Normung und Standardisierung umgesetzt hat.
[3] Das DKE-Gremium AK 353.0.8 „Nutzerautorisierung für Ladeinfrastruktur“ behandelt das Thema der sicheren und interoperablen Nutzerautorisierung über karten- und webbasierte Verfahren.

II.5 Verstetigung/Öffentlichkeitsarbeit

Mit der wachsenden Vernetzung durch die Digitalisierung dringen IKT-Themen auch in Bereiche ein, die bisher nicht damit in Berührung gekommen sind. Dies trifft im besonderen Maße auf die Elektromobilität zu, die mit der Ladeinfrastruktur, den Elektrofahrzeugen und zukünftig mit dem autonomen Fahren die Automobil- und Energiewirtschaft vor große Herausforderungen stellt. Die Normung und Standardisierung kann dabei helfen, den Herausforderungen durch Sicherstellung von Nachhaltigkeit und Investitionssicherheit zu begegnen. Dazu müssen gerade die neuen Stakeholder im Umfeld der Elektromobilität wie z.B. Mobilitätsanbieter oder Roaming-Plattformen in die Normungsaktivitäten eingebunden werden. Die Empfehlung lautet daher, vermehrt über die Vorteile der Normung und Standardisierung und die aktuellen Normungsaktivitäten im Bereich der Elektromobilität zu informieren. Die bisherigen Aktivitäten sollten weiterhin durch die Veröffentlichung von Normungsroadmaps und Normungslandschaften und durch die Nationalen Plattform „Zukunft der Mobilität“ (NPM) unterstützt werden.

II.6 Förderung etablierter und offener Ansätze und Verfahren der IT-Sicherheit

Bei der Entwicklung von Standards und Normen sollte darauf geachtet werden, dass diese die Nutzung etablierter und offener Ansätze und Verfahren der IT-Sicherheit nicht einschränken bzw. sogar fördern. So sollte eine Einschränkung auf spezifische Verfahren, z.B. zur Schlüsselvereinbarung und zum Schlüsselaustausch, vermieden werden. So sollte bspw. eine Technische Richtlinie für ein Sicherheitsmodul keine entsprechenden Einschränkungen vorgeben, da sich sonst die Entwicklung geeigneter Sicherheitsmodule verzögert oder sich Lock-in oder Monopolsituationen ergeben könnten. Deshalb sollte die Nutzung etablierter und wenn möglich sogar offener Standards ermöglicht und gefördert werden.

III. Handlungsempfehlungen an Ladesäulenhersteller/-betreiber/ Automobilhersteller

Der Fahrzeughersteller (OEM) soll über die Nutzungsdauer hinweg Firmware-Updates für den sicheren Betrieb aller zugänglichen Kommunikationsschnittstellen des Fahrzeuges bereitstellen und dem Nutzer eine einfache Möglichkeit zur Deaktivierung und Aktivierung der nicht für den Betrieb notwendigen Schnittstellen anbieten.

Die Datenübertragung über die aktivierte Telematik- oder Diagnoseschnittstelle soll datensparsam und zweckgebunden erfolgen. Der Fahrzeughersteller soll dem Fahrzeugnutzer eine Intervenierbarkeit für die Übermittlung der Telemetrie- und Telematik-Daten anbieten und diese transparent gestalten.

III.1 Hardware-Sicherheitsmodul (HSM)

Um die Integrität von Ladesäulen und Fahrzeugen sowie die Absicherung der Kommunikation zwischen diesen Komponenten sicherzustellen, wird die Verwendung eines zertifizierten Sicherheitsmodules empfohlen.

Das dabei eingesetzte Hardware-Sicherheitsmodul sollte auf einem offenen Standard basieren, da offene Standards durch deren Verfügbarkeit den Wettbewerb unter den Herstellern fördert und einen Hersteller lock-in oder Monopolsituationen von vornherein ausschließen. Auf diese Weise können die Kosten für OEMs von Fahrzeugen und Ladesäulen gesenkt werden und die notwendigen Voraussetzungen für sichere Lösungen geschaffen werden. Sofern möglich sollte bereits ein geeigneter Open Source Software Stack verfügbar sein. Dies erhöht die Wahrscheinlichkeit, dass der Standard richtig implementiert wurde, da die Lösung durch einen wesentlich breiteren Kreis getestet und verifiziert werden kann. Weiterhin sollte dieses Modul die Basis zur Gewährleistung der Systemsicherheit sein (z.B. Secure oder Measured Boot) und diese überprüfbar machen (Attestation) sowie die Möglichkeit bieten kryptographische Schlüssel (für die Kommunikation) sicher zu erzeugen und abzulegen.

III.2 Implementierung von datenschutzwahrenden Lösungen

Neben der Entwicklung und Erforschung von Lösungen, die einen integren und manipulationsgesicherten Ladeprozess ermöglichen, ist auch das Einbeziehen des Datenschutzes eine wichtige Aufgabe. Zwar kann der Einsatz geeigneter Technologien verhindern, dass unautorisierte Dritte einfach Daten über den Nutzer an entsprechenden Endpunkten oder dazwischen abgreifen können, doch können auch Service-Anbieter innerhalb der Wertschöpfungskette selbst Ziel eines Angreifers werden. Dabei sind vor allem sogenannte bösartige Insider ein oftmals unterschätztes Risiko. Aus diesem Grund ist es nötig, entsprechende Methoden und Technologien zu entwickeln, die das Prinzip der Datensparsamkeit umsetzen und nur wirklich zwingend notwendige Daten erfassen, erzeugen und speichern. Eine entsprechend sicher entworfene Pseudonymisierung/Anonymisierung stellt dabei einen ersten Schritt dar. Auch die Speicherung und Übertragung der Daten sollte möglichst datenschutzkonform durchgeführt werden und keine Rückschlüsse mit Hilfe von Verhaltensanalysen sowie zeitlicher und räumlicher Korrelation auf einzelne Person zulassen. Entsprechende Lösungen sorgen in der Regel für ein erhöhtes Vertrauen der Kunden und sorgen dafür, dass ein Hersteller keinen und nur geringen Reputationsverlust erleidet, wenn es zu einem erfolgreichen Angriff kam.

III.3 Berücksichtigung der Wechselwirkung von Safety und Security

Oftmals führen Geräte eine Vielzahl verschiedener Services und Applikationen aus, die sich verschiedene Ressourcen des Systems teilen und untereinander kommunizieren. Je nach Anwendungsfall besitzen diese Applikationen teilweise stark unterschiedliche Schutzanforderungen. Beispielsweise gelten Safety-kritische Applikationen als besonders schutzbedürftig und dürfen nicht von anderen Applikationen beeinflusst werden. Aus diesem Grund ist es sinnvoll, Applikationen entsprechend ihrer Aufgaben und Anforderungen jeweils getrennt voneinander auszuführen. Die Trennung kann dabei auf physischer, d.h. auf Hardware-Ebene, also auch auf Software-Ebene (Compartmentalisierung, Virtualisierung) durchgeführt werden. Ein entsprechendes Design der Systeme erlaubt es damit auch, die unterschiedlichen Systemkomponenten nach unterschiedlichen EALs zu zertifizieren und zu prüfen. Damit können Hersteller z.B. zwischen Managementfunktionen des Ladecontrollers in der Ladesäule und der Messeinheit unterscheiden. Vor allem vor dem Hintergrund, dass auch Softwarekomponenten der Messeinheit einer Zertifizierung unterliegen, bevor diese eingesetzt werden dürfen, macht daher den Prozess zum Updaten der Systeme komplex und zeitintensiv. Um zeitnah auf mögliche Probleme und Sicherheitslücken reagieren zu können, ist deshalb eine Trennung des Systems hilfreich, um im Notfall auch ohne eine Rezertifizierung möglicherweise angreifbare Systemkomponenten auszutauschen.

IV. Handlungsempfehlungen an zukünftige Förderprojekte

IV.1 Fördermaßnahmen mit Rechtsrahmen verknüpfen

Zukünftige Förderprojekte sollen mit einem vorhandenen und sich entwickelnden Rechtsrahmen verknüpft werden, um die Verwertbarkeit der Projektergebnisse zu gewährleisten. Veröffentlichte Projektergebnisse sollten auch nach Auslaufen der Projektmittel langfristig auffindbar sein und kostenfrei bereitgestellt werden. Dafür könnte eine Plattform wie Researchgate genutzt werden. Dafür anfallende Kosten sollten durch Mittel des BMWi bereitgestellt werden.

IV.2 Fördermaßnahmen mit Normung/Standardisierung verknüpfen

Die Normung und Standardisierung insbesondere auf internationaler Ebene lebt von der Teilnahme der Experten und dem Einbringen deren Expertise. Umso wichtiger ist auf dem relativ neuen Gebiet der Elektromobilität Nachhaltigkeit und Investitionssicherheit für die deutsche Wirtschaft im Rahmen der Normung weiter zu sichern und auszubauen. Die Empfehlung lautet daher, Normungs- und Standardisierungsvorhaben in Fördermaßnahmen zu unterstützen. Dies betrifft vor allen Dingen die Verstetigung von Projektergebnissen in der Normung bei gleichzeitiger Berücksichtigung wirtschaftlicher Anschlussfähigkeit.

IV.3 Fördermaßnahmen für eine terminologische Begleitung

Die Elektromobilität verbindet die seit Jahrzehnten etablierte Automobilindustrie und die Energiewirtschaft. Für das Zusammenspiel wird u.a. auch ein einheitlicher Wortschatz benötigt. Mit einer zusätzlichen Betrachtung der Querschnittsthemen IT-Sicherheit, Eichrecht und Verbraucherschutz wird der Bedarf weiter verdeutlicht. Die Empfehlung lautet daher, Fördermaßnahmen der terminologischen Begleitung der Förderprojekte zur Schaffung eines einheitlichen Fachwortschatzes für den Bereich der Elektromobilität und angrenzende Bereiche wie IT-Sicherheit, Eichrecht und Verbraucherschutz umzusetzen.

IV.4 Förderung der Forschung im Bereich der IT-Sicherheit und Privacy Enhancing Technologies (für Mobilität, insbesondere für Elektromobilität)

Um die Akzeptanz der Nutzer für die Elektromobilität zu erhöhen, muss neben dem Ausbau der Infrastruktur auch die Privatsphäre der Nutzer gewahrt bleiben. Ein großer Vorteil des ausgebauten Tankstellennetzes gegenüber den elektrischen Ladesäulen liegt in der Möglichkeit der Barzahlung. Diese ermöglicht es Kunden, ohne direkte Nachverfolgbarkeit ihr Fahrzeug zu betanken. Da Ladesäulen zum Großteil nicht an Tankstellen aufgestellt werden, sondern unbewacht in der Umwelt an vielen Orten verteilt sind, steht bei diesen typischerweise die Möglichkeit der Barzahlung nicht zur Verfügung. Die Verwendung von Mobilen Applikationen, zum Teil in Verbindung mit weiteren Merkmalen wie QR Codes, auf Smartphones oder der Einsatz einer Kreditkarte zur Autorisierung des Ladevorganges, macht den Ladevorgang des Kunden immer auch direkt personenbeziehbar. Aus diesem Grund sollten in Form von Förderprojekten nach möglichen weiteren anonymen Bezahlverfahren geforscht werden. Diese sollten es einem Kunden ermöglichen, einen zuvor getätigten Ladevorgang ohne einen entsprechend einfachen herzustellenden Personenbezug zu bezahlen [14].

IV.5 Schwachstellenmanagement im Kontext Laden und Abrechen

Im Zeichen zunehmender Digitalisierung ist es unabdingbar, Sicherheitslücken so schnell wie möglich nach ihrem Bekanntwerden zu schließen und Betroffene in die Lage zu versetzen, die Sicherheit eigener Anlagen und Systeme zu überprüfen bzw. erfolgreiche Angriffe zu erkennen und dann Angreifern den weiteren Zugriff zu verwehren. Jedoch versuchen auch heute noch zahlreiche Unternehmen, die Opfer eines solchen erfolgreichen Angriffs geworden sind, ihre Probleme alleine und isoliert in den Griff zu bekommen. Oft klappt dies nicht, weil Hintergrundinformationen oder das Wissen über ähnliche Angriffe (Vorgehensweise der Angreifer, Beeinflussungen auf Endgeräten, Ziele der Angreifer, Wirkung der Gegenmaßnahmen) fehlen, obwohl es bei Dritten bereits verfügbar ist. Die Auswirkungen für uns als Gesellschaft sind klar: Chancen werden nicht genutzt, die Kosten sind höher als nötig und wertvolle, sonst für Innovationen nutzbare, Ressourcen gehen verloren. Durch eine geordnete und vertrauenswürdige Zusammenarbeit betroffener Firmen im Umfeld (insbesondere aus dem KMU Bereich) der Ladeinfrastruktur auf einer vertrauensvollen Plattform kann der geschilderte Innovationsverlust (Fähigkeit zur Innovation geht verloren) verhindert oder zumindest eingedämmt werden. Insgesamt wird eine deutlich höhere Gesamt-IT-Sicherheit erreicht werden. Bedingt durch eine nationale Koordination der Arbeit von Produktsicherheitsteams und -verantwortlichen können gleichzeitig Standortvorteile geschaffen werden, da gleichwertige Prozesse auch zu besseren Produkten beitragen. Aus diesem Grund ist der Bedarf nach einem herstellerübergreifenden Austausch zur IT-Sicherheit auf einer neutralen, vertrauenswürdigen Basis von großer Wichtigkeit, um schon frühzeitig sicherheitsrelevante Informationen entlang der kompletten Wertschöpfungskette nutzbringend verarbeiten zu können. Hierfür wird empfohlen bisher kaum ausgeprägte Prozesse und funktionierende Meldeketten zielgerichtet und effektiv zu etablieren.

Literatur

[1] Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (MsbG), Ausfertigungsdatum: 29.08.2016, Geändert durch Art. 15 G v. 22.12.2016 I 3106.

[2] P.-L. Huynh, Beitrag zur Bewertung des Gesundheitszustands von Traktionsbatterien in Elektrofahrzeugen, Stuttgart: Springer Vieweg, 2016.

[3] EU-DSGVO: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates in der Fassung der, 2016.

[4] Gesetz über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung sowie über Fertigpackungen (Mess- und Eichgesetz - MessEG), Ausfertigungsdatum: 25.07.2013, Zuletzt geändert durch Art. 1 G v. 11.4.2016 I 718.

[5] Preisangabenverordnung (PAngV), Inkrafttreten der letzten Änderung: 1. Juli 2018; (Art. 7 G vom 17. Juli 2017).

[6] Verordnung über technische Mindestanforderungen an den sicheren und interoperablen Aufbau und Betrieb von öffentlich zugänglichen Ladepunkten für Elektromobile (Ladesäulenverordnung - LSV), Inkrafttreten der letzten Änderung: 14. Juni 2017; (Art. 2 VO vom 1. Juni 2017).

[7] Gesetz zur Digitalisierung der Energiewende, vom 29. August 2016, Bundesgesetzblatt Jahrgang 2016 | Nr. 43, ausgegeben zu Bonn am 1. September 2016.

[8] IEC 62443 Normenreihe, Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme.

[9] IEC 62351 Normenreihe, Power systems management and associated information exchange - Data and communications security.

[10] ISO/IEC 27019:2017-10, Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmaßnahmen für die Energieversorgung.

[11] ISO/IEC 27000 Normenreihe, Information technology - Security techniques - Information security management systems.

[12] R. Niederhagen und M. Waidner, „White Paper: Practical Post-Quantum Cryptography," Fraunhofer Institut für Sichere Informationstechnologie, Darmstadt, 2017.

[13] ISO 15118 Normenreihe, Road vehicles -- Vehicle to grid communication interface.

[14] D. Zelle, M. Springer, M. Zhdanova und C. Krauß, „Anonymous Charging and Billing of Electric Vehicles," in Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, ACM, 2018.

Abkürzungsverzeichnis

CPO	Charge Point Operator
EAL	Evaluation Assurance Level
ECC	Error correction code
HSM	Hardware-Sicherheitsmodul
IKT	Informations- und Kommunikationstechnik
InKaMs	In-Kabel-Messsystems
ISMS	Informationssicherheits-Managementsystem
KMU	Kleine und mittlere Unternehmen
LSV	Ladesäulenverordnung
MSB	Messstellenbetreiber
MsbG	Messstellenbetriebsgesetz
OBD	Onboard-Diagnose
OEM	Original Equipment Manufacturer
PKI	Public-Key-Infrastruktur
PQ	Post-Quatenkrypthographie
PTB	Physikalisch-Technische Bundesanstalt
RSA	Random sequential adsorption
SMGW	Smart Meter Gateway
SOH	State of health
WAN	Wide Area Network

DELTA

Datensicherheit und -integrität in
der Elektromobilität beim Laden
und eichrechtkonformen Abrechnen