Berlin, 07.12.2021

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.

Reinhardtstraße 32
10117 Berlin

www.bdew.de

Positionspapier

Positionen und offene Punkte zum Umgang mit dem Kommunikationsstandard ISO 15118 für die Funktion Plug and Charge

Inhalt

1 Einführung

Die automatische Authentifizierung beim Verbinden des Ladekabels mit dem Elektrofahrzeug stellt eine Komfortfunktion beim Laden und Bezahlen dar. Für Kundinnen und Kunden entfällt damit das Starten eines Ladevorgangs mittels App oder RFID-Karte. Für die Ladepunktsuche, die Anzeige der Ladehistorie, das Monitoring des Ladevorgangs, die Preistransparenz und das Beenden des Ladevorgangs wird hingegen aktuell ein zusätzliches Medium, zumeist eine App, benötigt. Künftig könnte dies auch über das Fahrzeug dargestellt werden.

Für eine Umsetzung von Plug and Charge bestehen aktuell unterschiedliche Mechanismen, die genutzt werden können. Eine Möglichkeit besteht mit der Implementierung des Kommunikationsstandards ISO 15118 auf Seiten des Fahrzeugs und der Ladesäule. Abhängig von ihrer Version kann die ISO 15118 eine Vielzahl von Funktionen ermöglichen, z.B. auch bidirektionales Laden. Die Funktion der automatischen Authentifizierung auf Basis der ISO 15118 wird Plug and Charge genannt. Aktuell kann nur die Version ISO 15118-2 bereits implementiert werden. Die Version -20 ist in der Finalisierung und soll bald auf dem Markt verfügbar sein. Die Version -20 enthält eine Reihe weiterer Funktionen und bringt auch Neuerungen für die Funktion Plug and Charge mit sich (u.a. das Hinterlegen mehrerer Vertragszertifikate von Ladestromanbietern). Die Arbeitsgruppe 5 der Nationalen Plattform Zukunft der Mobilität hat 2020 bereits eine Roadmap erstellt, die einen Überblick zu allen Funktionen der ISO 15118 gibt.

Neben Plug and Charge erlaubt auch die Funktion AutoCharge den Kundinnen und Kunden sich automatisch zu authentifizieren. AutoCharge wird auch bereits von Ladepunktbetreibern in Deutschland und den Niederlanden eingesetzt, und bietet einen vergleichbaren Komfort beim Ladevorgang wie Plug and Charge. Im Wettbewerb wird sich über die Zeit zeigen, welche Technologie sich für die automatische Authentifizierung mehrheitlich durchsetzen wird.

In Folgendem liegt der Fokus jedoch auf dem Einsatz der ISO 15118 für die Funktion Plug and Charge sowie der Public Key Infrastruktur (PKI), die für die Umsetzung von Plug and Charge sowie der weiteren möglichen Funktionen notwendig ist. Neben grundlegenden Positionen der Branche zur Sicherstellung eines fairen Wettbewerbs, werden auch offene Punkte benannt, die vor einer flächendeckenden Einführung des Standards zu klären sind, um eine technisch reibungslose, faire und rechtssichere Nutzung zu gewährleisten.

2 Positionen und offene Punkte zu einzelnen Schritten beim Laden mit Plug and Charge

Elementar für eine einfache Nutzung von Plug and Charge und eine möglichst hohe Transparenz der dahinterliegenden Prozesse gegenüber den Kundinnen und Kunden ist, dass die einzelnen Prozessschritte und Verantwortlichkeiten zwischen den Marktteilnehmern geklärt werden. Auf die zentralen Schritte, einhergehenden Forderungen und offenen Punkte wird in Folgendem eingegangen.

1

Das Hinterlegen der Vertragszertifikate der Ladestromanbieter im Fahrzeug

Damit Kundinnen und Kunden die Funktion Plug and Charge nutzen können, muss zunächst ein Vertragszertifikat von einem oder mehreren Ladestromanbietern im Fahrzeug hinterlegt werden. Dabei muss im Sinne eines fairen Wettbewerbs gelten:

- Das Hinterlegen der Vertragszertifikate ist über das Fahrzeug (OEM Telematik Backend) stets einfach, schnell und kostenfrei für die Kundinnen und Kunden möglich. Dafür müssen Kundinnen und Kunden den eindeutigen Identifikator für ihr Fahrzeug (PCID) einfach erhalten können, um ein Hinterlegen zu veranlassen. Zudem existiert die Möglichkeit die Vertragszertifikate über die Ladesäule im Fahrzeug zu hinterlegen. Für das Abholen der Vertragszertifikate aus einem Plug and Charge Contract Certificate Pool (CCP – siehe Glossar) durch den Automobilhersteller bedarf es einer standardisierten Schnittstelle (API), die einen einheitlichen und sicheren Prozess ermöglicht.
- Es darf keine Einschränkungen für Kundinnen und Kunden geben, nur Verträge von vorab festgelegten Ladestromanbietern in ihrem Fahrzeug hinterlegen zu können. Auf Wunsch der Kundinnen und Kunden kann ein oder mehrere Verträge direkt bei Kauf des Fahrzeugs hinterlegt werden.
- Mit der Einführung der Version ISO 15118-20 können Kundinnen und Kunden mehr als ein Vertragszertifikat im Fahrzeug hinterlegen. Dies gibt den Kundinnen und Kunden eine größere Wahlfreiheit. Als minimale Untergrenze sollen Kundinnen und Kunden mindestens fünf Vertragszertifikate für das europäische Roaming in ihrem Fahrzeug hinterlegen können, unabhängig von den in Europa etablierten Root Certificate Authorities (siehe Kapitel 3 und Glossar).
- Für die Hinterlegung eines Vertragszertifikates im Fahrzeug müssen Kundinnen und Kunden aktuell über ein Zwei-Faktor-Verfahren nochmals gegenüber dem Ladestromanbieter bestätigen, dass ein Vertrag mit dem entsprechenden Fahrzeug abgeschlossen werden soll. Dieses Verfahren soll beibehalten werden.

2

Das Anzeigen und die Auswahl der Vertragszertifikate oder alternativer Autorisierungsmittel

Vor dem Starten eines Ladevorgangs, ist im Sinne der Kundentransparenz und des fairen Wettbewerbs zu klären, wie den Kundinnen und Kunden ihre Auswahlmöglichkeiten angezeigt werden. Dabei muss gelten:

- Der Automobilhersteller ist verpflichtet, die im Fahrzeug hinterlegten Vertragszertifikate entweder im Fahrzeug oder in der dem Fahrzeug zugehörigen OEM-App

anzuzeigen. Hierbei ist der Klarname des Anbieters bzw. Vertrages anzuzeigen und keine technische Darstellung einer Zertifikatsnummer.

- Die Anzeige der Vertragszertifikate muss in einer übersichtlichen Darstellung aller hinterlegten Vertragszertifikate erfolgen (inkl. der Festlegung von Favoriten durch die Kundinnen und Kunden).
- Die Preistransparenz muss auch bei Plug and Charge gewährt werden. Da es aktuell kein standardisiertes Vorgehen zur Einbindung der Automobilhersteller in die Roamingprozesse gibt, um die Tarifinformationen der Ladestromanbieter im Fahrzeug anzuzeigen, muss die Preisanzeige bis dahin in der App des Automobilherstellers, der Ladestromanbieter oder der Ladepunktbetreiber erfolgen.
- Kundinnen und Kunden sollen regelmäßig durch ihren Automobilhersteller informiert werden, dass ihnen für die Nutzung von Plug and Charge unterschiedliche Tarife im Rahmen ihrer Ladeverträge zur Verfügung stehen sowie neben Plug and Charge auch andere Authentifizierungsmittel genutzt werden können. Damit soll sichergestellt werden, dass Kundinnen und Kunden sich bewusst für einen Tarif entscheiden. Denkbar wäre z.B., dass Kundinnen und Kunden in regelmäßigen Abständen im Fahrzeug informiert werden, mit welchem Tarif sie aktuell laden und eine Bestätigung eingefordert wird. Sollten Kundinnen und Kunden nicht an Ihre Tarifwahl und Alternativen erinnert werden wollen, sollten sie diese Erinnerungsfunktion deaktivieren können.

Offene Punkte

- Zur Anzeige der Ladetarife im Fahrzeug bedarf es eines Standardisierungsprozesses, der die Einbindung der Automobilhersteller in die Roamingprozesse ermöglicht. Die dafür notwendigen Schnittstellen müssen mit allen Marktteilnehmern genau abgestimmt werden, um eine reibungslose Anzeige zu ermöglichen. Dies ist insbesondere mit der perspektivischen Einführung dynamischer Preise von großer Bedeutung.
- Im Sinne des Datenschutzes sowie eines fairen Wettbewerbs muss sichergestellt sein, dass Kundeninformationen zur Nutzung bzw. Nutzungshäufigkeit eines EMP-Produktes für die Funktion Plug and Charge durch die Automobilhersteller nicht ausgelesen und nicht weitergegeben werden können. Hierfür bedarf es einer standardisierten Lösung (z.B. getrennte Rollen von Automobilhersteller und EMP oder Schaffung eines „generischen“ EMP im Rahmen der PKI, der als neutraler Mittler fungiert).

Das Starten und Stoppen des Ladevorgangs über Plug and Charge

Um Kundinnen und Kunden Informationen zum Stand des Authentifizierungsvorgangs und dem Ladevorgang zu übermitteln, sowie eine einfache Möglichkeit den Ladevorgang zu stoppen, werden Anbieter in den meisten Fällen auf bestehende Mittel (z.B. Display im Fahrzeug oder App) zurückgreifen müssen. Dabei muss im Sinne der Kundentransparenz gelten:

- Nach dem Verbinden des Ladekabels mit dem Fahrzeug sollten Kundinnen und Kunden eine Information erhalten, wenn der Authentifizierungsvorgang entweder erfolgreich abgeschlossen oder abgebrochen wurde. Die Anzeige darüber sollte auch im Fahrzeug erfolgen.
- Sollte der Authentifizierungsvorgang aufgrund einer fehlenden Roamingverbindung zwischen EMP und CPO fehlschlagen, bedarf es einer Fehlermeldung, die im Fahrzeug, der App des Automobilherstellers und, sofern technisch möglich, in der App des genutzten EMP, angezeigt wird.
- Die Anzeige des aktuellen Ladevorgangs, des Zahlungsvorgangs und der Ladehistorie findet nach wie vor über die heute gängigen Mittel statt (App, Fahrzeug, Ladesäule).
- Zum Stoppen des Ladevorgangs werden Kundinnen und Kunden weiterhin eine Bestätigung im Fahrzeug oder der EMP-App nutzen. Besitzen die Kundinnen und Kunden eine RFID-Karte mit der gleichen EMAID (Identifikator des Ladestromanbieters für seine Kundinnen und Kunden), wie sie im genutzten Vertragszertifikat hinterlegt ist, kann auch mit der RFID-Karte der Ladevorgang beendet werden.

Offene Punkte

- Es bedarf eines Standardisierungsprozesses für die Anzeige von Fehlermeldungen, wenn die Kommunikation zwischen Fahrzeug und Ladesäule fehlschlägt. Die Ursache für die fehlgeschlagene Kommunikation sollte den Kundinnen und Kunden übermittelt werden. Dabei ist die Anzeige von Fehlermeldungen nicht allein bei der Nutzung von Plug and Charge sinnvoll, sondern auch bei anderen Authentifizierungsmitteln (z.B. App oder RFID-Karte).

Das nachträgliche Hinterlegen und Löschen von Vertragszertifikaten

Damit Kundinnen und Kunden jederzeit auch Vertragszertifikate austauschen oder neue hinzufügen können, ist es wichtig, einen einfachen und intuitiven Prozess zu etablieren. Dabei muss auch im Sinne eines fairen Wettbewerbs gelten:

- Bei dem nachträglichen Hinterlegen von Zertifikaten gilt, wie auch bei der Hinterlegung eines ersten Zertifikates, dass der Vorgang über das Fahrzeug (OEM Telematik Backend) stets einfach, schnell und kostenfrei für die Kundinnen und Kunden sein muss. Kundinnen und Kunden sollen den Wechsel selbstständig ohne Werkstattbesuch über den Automobilhersteller, CPO oder EMP vornehmen können. Dafür müssen Kundinnen und Kunden den eindeutigen Identifikator für ihr Fahrzeug (PCID) einfach erhalten können, um einen Wechsel zu veranlassen. Wie in Schritt 1 erwähnt, braucht es auch in Schritt 4 für das Abholen der Vertragszertifikate aus einem Plug and Charge Contract Certificate Pool durch den Automobilhersteller eine standardisierte Schnittstelle (API), die einen einheitlichen und sicheren Prozess ermöglicht.
- Das Löschen von Vertragszertifikaten muss einfach und schnell im Fahrzeug oder in der App des Automobilherstellers durch die Kundinnen und Kunden möglich sein. Dies muss der Automobilhersteller gegenüber seinen Kundinnen und Kunden sicherstellen.
- Um die Verbindung des Vertragszertifikates mit dem Fahrzeug endgültig aufzuheben, z.B. wenn das Fahrzeug weiterverkauft wird, muss dies durch den EMP vorgenommen werden. Dieser muss die Verbindung zwischen der EMAID und der PCID aufheben und das Vertragszertifikat vollständig löschen und widerrufen.

3 Anforderungen an die einzelnen Marktrollen und Infrastrukturkomponenten einer Public Key Infrastruktur (PKI) für die ISO 15118

Um Plug and Charge auf Basis der ISO 15118 zu nutzen, aber auch um weitere Funktionen der ISO 15118 künftig nutzen zu können, bedarf es einer Public Key Infrastruktur, die diskriminierungsfrei die benötigten Zertifikate ausstellt und signiert und somit sicherstellt, dass Akteure vertrauenswürdig sind und die Kommunikation untereinander sicher ist. Dafür müssen von den unterschiedlichen Marktrollen bestimmte Anforderungen erfüllt werden. Diese umfassen:

Vehicle-to-Grid Root Certification Authority (V2G Root CA)

- Es ist davon auszugehen, dass es mehrere V2G Roots für den Aufbau der PKI geben wird. Diese müssen interoperabel sein damit der Kundenkomfort weiterhin bewahrt wird z.B. über Trust Lists oder Cross Certification (siehe Glossar).

- Bei Trust Lists:
    - Wird eine Trust List genutzt, bedarf es eines Trust List Owners, der gewisse Sicherheitsanforderungen erfüllt. V2G Root CAs können nur in die Trust List aufgenommen werden, wenn diese ebenfalls diese Sicherheitsstandards erfüllen
    - Der Trust List Owner muss eine neutrale Instanz sein, die z.B. durch die EU-Kommission eingesetzt wird.

› Eine V2G Root CA muss als vertrauenswürde Institution für alle CPO und für alle Zertifikate des Certification Provisioning Service (CPS) fungieren und optional auch für die Zertifikate der EMP und der Automobilhersteller.

› V2G Root CAs vergeben Zertifikate an alle Marktteilnehmer unter den gleichen Sicherheitsanforderungen für die Zertifikate und die entsprechenden Attribute.

› Aufgrund der zentralen Bedeutung der Root CAs müssen Qualitätsaudits dieser von einer unabhängigen Partei durchgeführt werden. Die dafür zu Grunde liegenden ISO-Normen sind noch festzulegen.

Automobilhersteller (OEM)

› Alle Automobilhersteller müssen alle V2G Root CA Zertifikate im Fahrzeug (ab Werk oder over the Air) hinterlegen.

› Für die Version ISO 15118-20: Alle OEM-Roots müssen in den bestehenden Pools geführt werden, die für die anderen Marktteilnehmern zugänglich sind.

› Kundinnen und Kunden können auf expliziten Wunsch und unter Aufzeigen und Information alternativer EMP-Möglichkeiten ein oder mehrere Vertragszertifikat(e) bei Auslieferung bzw. Kauf des Fahrzeugs vorinstallieren lassen.

› Plug and Charge sollte bei Neuwägen kostenfrei für die Kundinnen und Kunden als Funktion nutzbar sein und muss diskriminierungsfrei für alle EMP-Verträge zur Verfügung stehen.

› Es muss die Möglichkeit geben, während der Nutzung des Fahrzeugs Zertifikate schnell, einfach und kostenfrei zu löschen oder neue zu installieren.

Elektromobilitätsdienstleister (EMP)

› Der EMP übergibt die Zertifikate in einem Bündel an einen Certification Provisioning Service (CPS).

› Alle EMP Contract Zertifikate müssen durch ein CPS Zertifikat signiert werden.

› Das CPS Zertifikat ist von einer V2G Root CA abgeleitet und daher vertrauenswürdig und sicher.

› Alle EMP müssen zu einem CPS Zugang haben können.

› Das CPS signiert die Zertifikate und stellt sie zur Verfügung im Contract Certificate Pool.

Ladepunktbetreiber (CPO)

› Alle regional relevanten EMP Roots und V2G Root CA Zertifikate sollten entweder in der Ladesäule hinterlegt bzw. installiert sein oder der Ladesäule durch ein Charging Station Management System zur Verfügung gestellt werden. Dies kann z.B. durch den Zugriff der CPO auf die sogenannten Root Certificate Pools erfolgen.

OEM Provisioning Certificate Pool (PCP) und Governance der Certificate Pools

› OEM Provisioning Certificate Pool (PCP):

- Jeder Automobilhersteller muss sich für einen PCP entscheiden, um sein OEM Provisioning Certificate zu hinterlegen.
- Falls es mehr als ein PCP gibt, müssen alle EMP Zugang haben zu dem Directory Service für OEM Provisioning Certificate Pools.

› Governance:

- Es ist eine Governance erforderlich, die allen CPO den Zugang zu allen Contract Certificate Pools gewährleistet und die allen EMP einen Zugang zu allen OEM Provisioning Certificate Pools gewährleistet. Wenn mehrere Pools bestehen, muss allen Parteien der Zugang zu einem Directory Service gewährleistet sein.
- Es muss ein Prozess etabliert werden, der das Widerrufen eines bestehenden EMP Vertrags vereinfacht.

4 Glossar

Begriffe	Bedeutung
Certification Provisioning Service (CPS)	Service, der die Vertragsdaten inkl. einem Vertragszertifikat von einem EMP erhalten hat und signiert und dem CPO und/oder dem OEM zur Verfügung stellt.
Charge Point Operator (CPO)	Ladepunktbetreiber
Contract Certificate	Durch EMP ausgestelltes Zertifikat für den Nutzer, das zu Authentifizierung und Autorisierung bzw. zum Start des Ladevorgangs benötigt wird und durch den CPS signiert werden.
Contract Certificate Pool (CCP)	Pool, der alle EMP Contract Certificates speichert und den anderen Marktteilnehmern zur Verfügung stellt.
Cross Certification	Bei der Cross Certification zertifizieren sich zwei V2G Root CAs gegenseitig und akzeptieren damit auch die Authentifizierungsdaten von Nutzern der anderen Root CA.
E-Mobility Account Identifier (EMAID)	Eindeutiger Identifikator des Ladestromanbieters für seine Kundinnen und Kunden, der zur Authentifizierung und Abrechnung benötigt wird.
E-Mobility Provider (EMP)	Ladestromanbieter
Original Equipment Manufacturer (OEM)	Automobilhersteller
OEM Provisioning Certificate	Durch OEM Root CA ausgestelltes, je Fahrzeug individuelles und digitalen Zertifikat zur Ausweisung eines Fahrzeugs.
OEM Provisioning Certificate Pool (PCP)	Pool, der alle OEM Provisioning Certificates speichert und den anderen Marktteilnehmern zur Verfügung stellt.
OEM Root Certification Authority (OEM Root CA)	Die OEM Root CA stellt das fahrzeugindividuelle OEM Provisioning Certificate aus.
Provisioning Certificate Identifier (PCID)	Eindeutiger Identifikator für das individuelle Fahrzeug, die z.B. zur Verknüpfung mit dem Vertragszertifikat eines Ladestromanbieters benötigt wird.
Public Key Infrastruktur (PKI)	Hierarchische Struktur von vertrauenswürdigen Organisationen (CAs und sub-CAs) zum Handling von Zertifikaten zur sicheren Kommunikation zwischen Fahrzeug und Ladepunkt.

Root Certificate Pools	Pools, die alle EMP Roots und V2G Root CA Zertifikate speichert und den anderen Marktteilnehmer zur Verfügung stellt.
Subordinate certificate authority (Sub-CA)	CAs die hierarchisch unter einer Root CA stehen und deren Zertifikate durch die Root CA signiert werden. Es darf minimal eine und maximal 2 Sub-CAs je Marktrolle bzw. PKI-Strang (also: CPO, EMP und OEM) geben.
Trust List	Die Trust List enthält alle vertrauenswürdigen und authentifizierten V2G Roots und garantiert die Interoperabilität zwischen den unterschiedlichen V2G Root CAs.
Trust List Owner	Der Trust List Owner verwaltet als neutrale Instanz die Trust List.
Vehicle-to-Grid Root Certification Authority (V2G Root CA)	Höchst gestellte CA innerhalb der PKI Hierarchie und muss für alle Marktteilnehmer vertrauenswürdig und neutral sein. Es kann mehrere Root CAs geben in einem Markt. Sie müssen dann auch einander vertrauen. Dazu gibt es zwei Möglichkeiten: über “trust lists” oder “cross certificates”. Die V2G Root signiert die Zertifikate aller sub-CAs der beteiligten Marktrollen.

Ansprechpartnerin:

Amelie Thürmer
Fachgebietsleiterin
Grundsatzfragen Ladeinfrastruktur
Geschäftsbereich Energienetze, Regulierung und Mobilität
Amelie.thuermer@bdew.de
Telefon: +49 (0)30 300199-1119