MENNEKES Elektrotechnik
GmbH & Co. KG
Aloys-Mennekes-Str. 1
D-57399 Kirchhundem
Tel. 0 27 23 / 41-1
Fax 0 27 23 / 41-214
E-Mail info@MENNEKES.de
Internet www.MENNEKES.de

Stellungnahme

Datensicherheit von MENNEKES Ladeinfrastruktur

Kirchhundem, ***01.02.2018*** – Nach den Veröffentlichungen des Chaos Computer Clubs (CCC) zum Thema der Sicherheit beim Laden von Elektrofahrzeugen erhalten wir Fragen zur Sicherheit unserer Ladesysteme.
Aufgrund des reichweitenstarken medialen Echos können wir die Rückfragen unserer Kunden und der Öffentlichkeit absolut nachvollziehen. Mit dem steigenden Markt der Elektromobilität ist letztlich nicht auszuschließen, dass Fälle auftreten werden, in denen versucht wird, sich einen Vorteil durch gefälschte Identitäten oder durch manipulierte Geräte zu verschaffen. Mit den folgenden Informationen möchten wir als Hersteller von Ladesystemen die bisher an uns herangetragenen Fragen gerne beantworten, und aufzeigen, welche Möglichkeiten Betreiber schon heute haben die Ladevorgänge an und mit MENNEKES Ladesystemen sicher zu gestalten.
Um was geht es also?

RFID-Karten – Sicherheit und Verwendung

In den Veröffentlichungen wird darauf hingewiesen, dass die heute weit verbreiteten RFID-Karten nicht fälschungssicher sind.
Im Bereich der Elektromobilität wird heute die eindeutige Kartennummer der RFID-Karte (UID – Unique Identifier) zur Identifikation am Ladepunkt verwendet. Der Betreiber des Ladepunkts bzw. der eMobility Provider ordnet die Ladedaten mithilfe dieser RFID-Kartennummer dem jeweiligen Kunden zu.

MENNEKES-Gesprächspartner für die Presse:
Joachim See, Leiter Marketing & Unternehmenskommunikation, E-Mail joachim.see@MENNEKES.de

Lars Baier, Marketing & Unternehmenskommunikation, E-Mail l.baier@MENNEKES.de

Die Nutzung der UID stellt den kleinsten gemeinsamen Nenner dar, um Kunden verschiedener eMobility Provider die Nutzung von Ladestationen verschiedener Betreiber und Hersteller zu ermöglichen. Daher wird dieses Autorisierungsverfahren neben einer Smartphone-App-Autorisierung z.B. auch von der aktuellen Förderrichtlinie des BMVI als Mindeststandard gefordert (§7.3).

Open-Charge-Point-Protocol

Betreiber und Verbraucher fordern eine hohe Verfügbarkeit der Ladesysteme. Daher wurde im international veröffentlichten Kommunikationsstandard OCPP (Open-Charge-Point-Protocol) außerdem die optionale Nutzung einer lokalen Whitelist-Ablage beschrieben. Somit wird auch die Offline-Nutzung von Ladestationen bei Ausfall der Backend-Kommunikation sichergestellt.
Leider ist durch die mögliche Duplizierung der UID die Authentifizierung mittels RFID-Karte nicht vollkommen sicher.
Wie sehen sichere Lösungen bei MENNEKES aus?

Schon heute gibt es sichere Alternativen der Authentifizierung

1. APP & Adhoc-Laden

Eine Smartphone-App und das Adhoc-Laden (Laden ohne Vertrag o. Prepaid-Karte) sind z.B. zwei Möglichkeiten solcher Authentifizierungen. Im Übrigen: Auch diese beiden Verfahren werden von der Ladesäulenverordnung und der Förderrichtlinie für das Laden an öffentlichen Ladepunkten gefordert. Ein eMobility Provider bietet somit schon lt. Gesetz verschiedene Autorisierungsverfahren an. Der Verbraucher hat die Wahl, welches Verfahren er nutzen möchte.

MENNEKES-Gesprächspartner für die Presse:
Joachim See, Leiter Marketing & Unternehmenskommunikation, E-Mail joachim.see@MENNEKES.de

Lars Baier, Marketing & Unternehmenskommunikation, E-Mail l.baier@MENNEKES.de

2. Backend - chargecloud

Für den Betrieb vernetzter Ladeinfrastruktur bietet MENNEKES zusammen mit der chargecloud GmbH für den Betrieb von Ladepunkten, der Kundenverwaltung und der Abrechnung von Ladevorgängen eine cloudbasierte Softwarelösung inkl. Smartphone-App und Ad-hoc-Laden an. Die Entwicklung dieses Systems unter Berücksichtigung aktueller sicherheitstechnischer Aspekte, automatisches Einspielen von Sicherheitsupdates und verschlüsselte Datenübertragung, stellen ein hohes Maß an Datensicherheit dar.

Alternatives Backend

Betreiber können ihren Kunden auch Lösungen von zu MENNEKES Ladesystemen kompatiblen Backends anbieten. Details zu diesen softwarebasierten Systemen können nur die jeweiligen Hersteller selbst geben.

3. Zukünftige Authentifizierungsverfahren

Zukünftig wird es weitere Authentifizierungsverfahren geben, bei denen eine direkte Datenübertragung zwischen Ladestation und Elektrofahrzeug mit entsprechenden Verschlüsselungsmechanismen eingesetzt wird. Dies setzt allerdings eine Ausrüstung der Ladestationen und Elektrofahrzeuge mit der notwendigen Hardware und die Umsetzung des ISO 15118 – Standards voraus.

Mechanischer Schutz vor Manipulation an Ladesystemen

Im Zusammenhang mit dem Vortrag des CCC wurde auch auf die Möglichkeit der Veränderung von Systemdaten oder das Auslesen von RFID-Kartennummern an einigen Ladesystemen hingewiesen.

MENNEKES Ladesysteme im öffentlichen Bereich sind immer mit einem Schloss gesichert und besitzen einen sehr hohen mechanischen (Einbruchs-) Schutz. Selbst wenn die erforderliche Menge an krimineller Energie aufgewendet wird, um an das Innere der Geräte zu gelangen, ist der Zugang zum

MENNEKES-Gesprächspartner für die Presse:
Joachim See, Leiter Marketing & Unternehmenskommunikation, E-Mail joachim.see@MENNEKES.de

Lars Baier, Marketing & Unternehmenskommunikation, E-Mail l.baier@MENNEKES.de

Kommunikationsgateway und Ladepunktcontroller durch ein Passwort und ein Verschlüsselungsverfahren geschützt. Die Mischung aus mechanischen Hürde und Softwarebarriere, stellt den optimalsten Schutz dar.

Für Ladesysteme im privaten Bereich kann der mechanische Schutz geringer ausgeprägt sein, denn im privaten Umfeld sind Ladesysteme häufig schon dadurch geschützt, indem sie in Garagen oder anderen zugangsgeschützten Bereichen auf den jeweiligen Privatgrundstücken aufgestellt sind. Daher lassen sich die Ladesysteme für diesen Anwendungsbereich mit einem Werkzeug öffnen. Dennoch ist es auch hier für den Kriminellen erforderlich, das Passwort des Gerätes zu kennen. Zusätzlich müssen noch verschiedene PIN bekannt sein, um an Gerätedaten, Ladevorgangsdaten und RFID-Daten zu gelangen oder die Gerätekonfiguration zu ändern.

Ausblick Plug and Charge

Zum Laden von Elektrofahrzeugen ist es erforderlich, dass Ladeinfrastruktur und Fahrzeuge sicher kommunizieren können. Dies wird zukünftig ermöglicht durch die ISO 15118. Bei diesem Standard haben beide Seiten, Ladestation und Elektrofahrzeug, Protokolle normenkonform implementiert, um miteinander zu kommunizieren. Voraussetzung beidseitig (Ladepunkt/Fahrzeug) ist dabei die Verschlüsselung der Daten mittels Software-Zertifikaten.
MENNEKES wird zukünftig solch ein Verfahren anbieten.

Zusammenfassung

Die Hinweise des CCC sind durchaus berechtigt. MENNEKES als Hersteller von Ladesystemen setzt Lösungen um, die vom Markt oder durch gesetzliche Vorschriften und Normen gefordert werden. Wir bieten aktuell drei und zukünftig vier Möglichkeiten zur Autorisierung: RFID, APP, adhoc-Laden und demnächst plug and charge.
Letztlich können somit heute schon die Betreiber und eMobility-Provider (im Rahmen der gesetzlichen Vorgaben) wählen, welche Möglichkeiten der Authentifizierung sie Ihren Kunden anbieten.

MENNEKES-Gesprächspartner für die Presse:
Joachim See, Leiter Marketing & Unternehmenskommunikation, E-Mail joachim.see@MENNEKES.de

Lars Baier, Marketing & Unternehmenskommunikation, E-Mail l.baier@MENNEKES.de

Unserer Erfahrung nach werden alternativ zur RFID-Karte häufig Lösungen mit einer Smartphone-App und einem Ad-hoc-Zugang angeboten. Dadurch ist auch der Endverbraucher (Elektroautofahrer) in der Lage, selbst zu entscheiden, welches Verfahren er nutzen möchte.

Die Elektromobilität entwickelt sich rasant weiter. Mithilfe des Feedbacks aus dem Markt, von renommierten Institutionen und auch des CCC wird MENNEKES zusammen mit seinen Partnern auch weiter hart daran arbeiten, mögliche Hürden zu überwinden, um der Mobilität der Zukunft den Weg zu ebnen.

MENNEKES-Gesprächspartner für die Presse:
Joachim See, Leiter Marketing & Unternehmenskommunikation, E-Mail joachim.see@MENNEKES.de

Lars Baier, Marketing & Unternehmenskommunikation, E-Mail l.baier@MENNEKES.de