Anlage [Technische Anforderungen und IT-Sicherheit]

Anforderungen an die Technik von Ladeinfrastrukturen:
AC-Laden:
1-phasiges und 3-phasiges AC-Laden (bis zu 43 kW):
Die Ladestation ist mit einer oder mehreren Typ 2-Ladepunkten ausgestattet. Die Ladestation ermöglicht das 1-phasige AC-Laden mit bis zu 7,4 kW sowie das 3-phasige AC-Laden mit bis zu 43 kW. Die Ladestation passt sich der vom Fahrzeug benötigten Ladeleistung an.
1-phasiges AC-Laden (bis zu 3,7 kW):
Die Ladestation ist mit einer oder mehreren Typ 2-Ladepunkten ausgestattet. Der Anschluss ermöglicht 1-phasiges AC-Laden mit bis zu 3,7 kW.

DC-Laden:
Combined Charging System:
Das Combined Charging System (CCS) integriert einphasiges und schnelles dreiphasiges AC-Laden, DC-Laden zuhause und ultra-schnelles DC-Laden an öffentlichen Ladestationen in einer fahrzeugseitigen Ladedose (Vehicle Inlet). In Europa basiert der Stecker genannt „Combo 2" auf dem AC-Typ 2-Stecker und auf dem Combo 2-Stecker (siehe Configuration FF in der IEC 62196-3) zum Gleichstromladen.
CHAdeMO:
Mit dem CHAdeMO Standard (siehe ISO/IEC 61851-23 und ISO/IEC 61851-24) wird ebenfalls schnelles DC-Laden unterstützt. Dazu setzt CHAdeMO einen CHAdeMO-Ladestecker für Elektrofahrzeuge und CHAdeMO-Ladestationen voraus, um das Fahrzeug basierend auf Gleichspannung zu laden. Weitere Technologien kann Hubject festlegen.

Zertifizierung von Ladeinfrastrukturen:
Im Hinblick auf die sichere Verwendung der Ladeinfrastruktur muss eine Zertifizierung gemäß den Anforderungen bestehender Normen und Standards und entsprechend der Konzeptentwicklung der Ladetechnologie erzielt werden. Der Betreiber bzw. Hersteller sollte die elektrische Sicherheit und Übereinstimmung mit den Standards sicherstellen. Die Mindeststandards, nach denen die Ladestation zertifiziert werden sollte, sind folgende: CE-Zertifizierung, Einhaltung der EMV-Richtlinie, DIN-Spezifikation 70121 und IEC 61439-7.
Für DC-Ladesäulen bzw. Ladesystem sollten darüber hinaus die folgenden Standards berücksichtigt werden: IEC 61851-23 (Allgemeine Anforderungen an eine DC-Ladestation), IEC 62196-3 (Definition von DC-Ladesteckverbindungen sowie DIN SPEC 70121 (Kommunikation für das Gleichstromladen zwischen Ladestation und Elektrofahrzeug, basierend auf ISO/IEC 15118) und die ISO/IEC-Norm 15118 für die zertifikatsbasierte Kommunikation zw. Elektrofahrzeug, Ladestation und IT-Systemen.

Anforderung an Ladestations- bzw. Kunden-bzw. Standortdatenmanagement-Systeme:

Schnittstelle zwischen Ladesäule und Ladestationsmanagement-System:
Die bidirektionale Kommunikationsfähigkeit der Ladesäulen mit dem Backend muss gegeben sein. Hubject legt keine Anforderungen für die Kommunikationsprotokolle zwischen Ladestationsmanagement-System und Ladesäulen fest.

Schnittstelle zwischen Ladestationsmanagement-System und Hubject-System:
Die Kommunikation zwischen Ladestationsmanagement-System und Hubject-System erfolgt über definierte Schnittstellen mittels Webservices, siehe **Anlage [OICP]**.

Obligatorische Anforderungen:
a) Remote-Aktivierung von Ladevorgängen und Remote-Beenden von Ladevorgängen sowie Aktivierung und Beenden von Ladevorgängen mittels weiteren Authentifizierungsmethoden
b) Übertragung von abrechnungsrelevanten Daten (Liefermitteilung / Charge Detail Record)
c) Übertragung von statischen Standortdaten der Ladestationen (Point-of-Interest-Informationen)
d) Übertragung von dynamischen Standortdaten der Ladestationen (Point-of-Interest-Informationen)

Schnittstelle zwischen Kundenmanagement-System und Hubject-System:
Die Kommunikation zwischen Kundenmanagement-System und Hubject-Backend-System erfolgt über definierte Schnittstellen mittels Webservices, siehe **Anlage [OICP]**.

Obligatorische Anforderungen:
a) Remote-Aktivierung von Ladevorgängen und Remote-Beenden von Ladevorgängen sowie Aktivierung und Beenden von Ladevorgängen mittels weiteren Authentifizierungsmethoden
b) Empfang von abrechnungsrelevanten Daten (Liefermitteilung / Charge Detail Record)
c) Empfang von Ladestationsdaten (Point-of-Interest-Informationen)

Schnittstelle zwischen Standortdatenmanagement-System und Hubject-System:
Die Kommunikation zwischen Standortdatenmanagement-System und Hubject-System erfolgt über definierte Schnittstellen mittels Webservices, siehe **Anlage [OICP]**.

Obligatorische Anforderungen:
Empfang von Ladestationsdaten (Point-of-Interest-Informationen)

Anforderung an die IT-Sicherheit zwischen Ladestationsmanagement-System/Kundenmanagement-System/ Standortdatenmanagement-System und Hubject-System
Die Plattform wird von Partnern über Ladestationsmanagement-Systeme und Kundenmanagement-Systeme sowie Standortdatenmanagement-Systeme genutzt. Die Kommunikation zwischen den Systemen ist durch die Standard Internet-Infrastruktur möglich. Deswegen muss die Kommunikation gesichert werden, um folgende Ziele der Informationssicherheit zu erfüllen:
- Vertraulichkeit: Nachrichten können nur vom vorgesehenen Empfänger gelesen werden
- Integrität: Daten müssen während der Übertragung gegen Veränderung (beabsichtigt oder aufgrund technischer Fehler) geschützt sein
- Authentizität: Nachrichten müssen exklusiv einem Absender zuordenbar sein. Der Sender darf nicht leugnen können, eine Nachricht geschickt zu haben.

Eingehende Verbindungen von Partner-Backends werden über das Internet an einen Load-Balancer der Plattform gesendet, der gleichzeitig als Reverse-Proxy eingesetzt wird. Die Anfragen werden an einen Cluster von verarbeitenden Serviceknoten weitergeleitet. Die Verbindungsanfragen müssen eine zweischichtige Firewall durchlaufen, wenn sie das Netzwerk der Plattform erreichen wollen.
Der Reverse-Proxy und die Firewall bieten durch ein IP-Whitelisting eine Zugriffskontrolle an, indem nur bekannten IP-Adressen der Zugriff erlaubt wird. Die Firewall im Netzwerk und in der Transportschicht beschränkt die Verbindung auf bestimmte Quell- und Ziel-IP-Adressen und -Ports. Der Proxy in der Applikationsschicht ist auf spezielle URLs beschränkt. Ausgehende Verbindungen von der Plattform werden direkt zum Partner-Backend-System gesendet und passieren dabei ebenso die Firewall.
Die Webservices werden über das HTTP-Protokoll übermittelt. Die SSL/TLS gesicherte HTTPS-Variante verkapselt das HTTP. Der SSL-Tunnel garantiert die oben beschriebenen Ziele der Informationssicherheit: Vertraulichkeit durch Verschlüsselung, Integrität durch zertifizierte Prüffunktionen und Authentizität durch digitale Signaturen und Zertifikate.
„HTTPS strong server" und Client-Authentifizierung durch Zertifikate werden genutzt, um die tatsächliche Verbindung jedes Service-Calls zu authentifizieren.
Der Reverse-Proxy/Load-Balancer erledigt die zentrale HTTPS-Verschlüsselung und Authentifizierung aller eingehenden Verbindungen zu der Plattform. Dies beinhaltet Anfragen an das Portal, das von den Nutzern über einen Web-Browser genutzt wird.
Um neue Partner der Plattform hinzuzufügen, sind keine Änderungen am System erforderlich.