Die Zukunft des sicheren Ladens

Moderne Authentifizierungslösung für das EV-Charging

Authentifizierungslösung, EV-Charging, Benutzerauthentifizierung, Zugangskontrolle

Mit der Zahl der Elektrofahrzeuge wächst der Bedarf an leistungsfähiger Ladeinfrastruktur – inklusive einer zuverlässigen Authentifizierungslösung, mit der sich sowohl der Zugang zu den Ladesäulen als auch die Abrechnung einfach und sicher regeln lassen. Hierfür sind RFID (Radio-Frequency Identification) und mobile Technologien wie NFC (Near Field Communication) oder BLE (Bluetooth® Low Energy) besonders geeignet. Doch in einer sich stark wandelnden Branche können sich die Anforderungen an eine Authentifizierungslösung schnell ändern. Damit ihre Wahl nachhaltig und zukunftssicher ist, müssen Betreiber und Hersteller von Ladeinfrastruktur daher wichtige Punkte beachten.

Johannes Weil

Die Betankung von Elektrofahrzeugen mit Strom soll sicher und komfortabel funktionieren. Um dies zu gewährleisten, müssen Betreiber von Ladestationen – ob öffentlich oder privat – eine Reihe an Überlegungen anstellen, die von vielen individuellen Gegebenheiten abhängen: Wer darf die Lademöglichkeit nutzen? Wie erfolgt die Abrechnung? Und wie wird die Nachvollziehbarkeit des Ladevorgangs sichergestellt?

Die Anforderungen an Nutzerauthentifizierung, Zugangsbeschränkung und Abrechnungsmodelle unterscheiden sich je nach Anwendung. Die Möglichkeiten reichen von Mitgliederprogrammen bis hin zu kostenfreien Angeboten. So lassen sich Flottenfahrzeuge beispielsweise mit Hilfe von Mitarbeiterausweisen laden, sodass nur autorisierte Nutzer Zugang zu den Lademöglichkeiten haben und ein sicherer Ladevorgang gewährleistet ist. Für die interne Abrechnung ist es in diesem Fall erforderlich, nachzuvollziehen, wer die Säule wann und wie lange genutzt hat. Unternehmen wie Kinos oder Einkaufszentren, die Ladesäulen als zusätzliche Einnahmequelle nutzen, aber auch große Netzbetreiber, die Lademöglichkeiten an Schnellstraßen oder Autobahnen bieten, müssen ihren Kunden komfortable Zugänge und transparente Abrechnungsmodelle bieten, die per Kreditkarte oder Smartphone-App funktionieren.

Erstausrüster (OEMs) müssen ihr Angebot an die Anforderungen von Betreibern und Nutzern anpassen. Das gilt nicht nur im Hinblick auf die Ladetechnik, mit der die Ladesäule arbeitet, sondern auch in Bezug auf die Optionen für Zugangskontrolle und Benutzerauthentifizierung.

Herausforderungen bei der Integration einer Authentifizierungslösung für OEMs und Betreiber

Ob Mitarbeiter, Mieter oder Flottenfahrer – Betreiber von Ladeinfrastruktur müssen wissen, wer auf ihr Angebot zugreift, den Zugang regeln und dabei sicherstellen, dass die Datensicherheit jederzeit gegeben ist. Betreiber sind auf eine Authentifizierungslösung angewiesen, die die maximale Sicherheit der sensiblen, personenbezogenen Nutzerdaten gewährleisten. Das gilt ganz besonders bei Authentifizierungs- und Zugangskontrolllösungen für gebührenpflichtige Ladestationen: Hier besteht ohne Verschlüsselung das Risiko, dass Signale, die zwischen Karte und Lesegerät ausgetauscht werden, beispielweise Kontodaten, abgefangen und missbraucht werden.

Bieten Hersteller von Ladestationen ihre Produkte überregional oder sogar länderübergreifend an, müssen sie berücksichtigen, dass der Markt für Ladeinfrastruktur stark fragmentiert ist, etwa hinsichtlich technischer Spezifikationen und Datenschutzgesetzen. Besonders bei der Integration von Authentifizierungs- und Zugangskontrolllösungen ist es wichtig, dass die gewählte Lösung die Verwaltung der Ladestationen vereinfacht. Muss eine große Anzahl an Lesegeräten in einem großflächigen, gegebenenfalls landesweiten Ladenetz vor Ort aktualisiert werden, kann ein Update oder eine Neukonfiguration erheblichen zeitlichen und finanziellen Aufwand bedeuten.

Nutzer der Ladeinfrastruktur können zudem unterschiedliche Karten- oder mobile Technologien im Einsatz haben. Denn am internationalen Markt ist eine Vielzahl von Transpondertechnologien mit jeweils eigenen Datenformaten, Kommunikationsfrequenzen und Sicherheitsfunktionen verfügbar. Die meisten Lesegeräte sind jedoch lediglich in der Lage, nur einige wenige Kartentechnologien zu lesen. Das bedeutet für OEMs, die ihre Marktchancen erhöhen wollen, dass sie gegebenenfalls unterschiedliche Lesegeräte für verschiedene Kunden vorrätig halten müssen. Auch für Anbieter von Ladenetzen, die über Stationen in mehreren Regionen oder Ländern verfügen, kann es eine Herausforderung sein, ein Lesegerät zu finden, das für den Einsatz in al-

Foto: AdobeStock / Elatec

So funktionieren RFID, NFC und BLE

RFID-Karten haben einen eingebetteten Chip (oder Tag), der aus zwei Hauptkomponenten besteht:

- einer integrierten Einheit, die Informationen speichern und verarbeiten kann; und
- einer Antenne zum Senden oder Empfangen eines Signals

Auf jeder RFID-Karte ist ein eindeutiger Datensatz – beispielsweise eine Nummer – gespeichert; er dient der Identifizierung der Karte und damit auch der Person, die sie bei sich trägt. Befindet sich eine Karte mit einem eingebetteten RFID-Tag in der Nähe eines RFID-Lesegeräts, sendet dieses ein Funksignal aus, um den Tag abzufragen. Das Funksignal aktiviert den Tag, der dann die Energie des Funksignals nutzt, um dem Lesegerät seine eindeutige ID mitzuteilen.

Sowohl BLE als auch NFC sind Technologien für den kontaktlosen Datenaustausch. Ihr Hauptunterschied zu RFID besteht darin, dass die Informationsträger (z. B. Smartphones) aktive Funksender sind und eine Stromquelle benötigen.

- NFC basiert auf hochfrequenter RFID-Technologie (13,56 MHz) und ermöglicht einen kontaktlosen Datenaustausch in der Nahfeldkommunikation (< 10 cm).
- BLE ist eine Kurzstrecken-Funktechnologie für Entfernungen bis zu zehn Metern im Frequenzbereich von 2,4 GHz.

Werden Smartphones für die Benutzerauthentifizierung und Zugangskontrolle verwendet, fungieren sie als Kartenemulatoren und senden eine eindeutige Benutzer-ID an das Lesegerät.

len Zielmärkten zertifiziert ist und alle an den jeweiligen Standorten bevorzugten Technologien unterstützt.

Nicht zuletzt ändern sich auch die Anforderungen am Markt und gesetzliche Regelungen permanent. Smartphone-basierte Lösungen werden immer beliebter und lösen die klassische Karte in vielen Bereichen und Anwendungsszenarien ab. Die meisten Lesegeräte lassen sich jedoch nur eingeschränkt aufrüsten und an aktuelle Kundenbedürfnisse anpassen und müssten daher im Zweifelsfall kostspielig ausgetauscht werden.

Die Lösung: Authentifizierung auf der Basis von RFID und mobilen Technologien

Eine einfache, komfortable und sichere Möglichkeit für die Benutzerauthentifizierung und Zugangskontrolle bietet eine moderne Authentifizierungslösung auf der Basis von RFID und mobilen Technologien. An öffentlichen und privaten Ladestationen können Nutzer entweder mit einer RFID-Karte oder einem Token eindeutig identifiziert werden. Möglich ist auch der Einsatz von digitalen Berechtigungsnachweisen, sogenannten mobile Credentials. Sie basieren auf den Technologien NFC oder BLE, mit denen ein Großteil aller mobilen Endgeräte wie Smartphones ausgestattet ist. Der Einsatz einer solchen Authentifizierung schützt Ladestationen vor unbefugtem Zugriff und sorgt dafür, dass sensible Informationen wie die Zahlungsdaten der Nutzer nicht in falsche Hände geraten.

Für die Nutzer genügt es, einfach den Berechtigungsnachweis in Form von Karte oder Smartphone an die Ladesäule zu halten. Das integrierte Lesegerät ermöglicht dann den sicheren, hygienischen und kontaktlosen Zugang zur Nutzung der Ladeinfrastruktur – ohne den Einsatz von Kreditkarten oder Passwörtern und PINs, die nur schwer im Gedächtnis bleiben.

Zugangskontrolle und Benutzerauthentifizierung nachhaltig und sicher gestalten: Das gilt es zu beachten

Wollen Betreiber und Hersteller mit ihrer Ladeinfrastruktur fortschrittlich, flexibel und sicher am Markt aufgestellt sein, sollte die Authentifizierungslösung folgende Kriterien erfüllen:

Sicherheit für Infrastruktur und Daten

Eine Zugangskontrolle mit Authentifizierungslösung erhöht das Sicherheitsniveau. Sie schützt vor Missbrauch – sowohl in Bezug auf Daten als auch auf die wertvolle Ladeinfrastruktur. Denn so erhalten nur autorisierte Nutzer mit ihrem Ausweis die Möglichkeit, Strom zu tanken. Ihr Ladeverhalten lässt sich so zudem problemlos nachvollziehen. Um die Datensicherheit zu erhöhen, sollte sich ein Lesegerät so programmieren lassen, dass es Verschlüsselungstechnologien einschließlich kryptografischer Methoden unterstützt, die eine hohe Rechenleistung erfordern. Entsprechende Geräte erlauben es Herstellern oder Betreibern, kundenspezifische Verschlüsselungsverfahren und andere komplexe Funktionen.

Flexibilität und Komplexitätsreduktion

Den Herausforderungen, die der stark fragmentierte Markt für Ladeinfrastruktur und die Vielzahl an gängigen Transpondertechnologien mit sich bringen, können Betreiber und Hersteller mit Multifrequenz-Lesegeräten begegnen. Am Markt sind universelle Reader verfügbar, die mehr als 60 weltweit gängige Transpondertechnologien verarbeiten können und für den Einsatz in bis zu 110 Ländern zertifiziert sind. Diese Lesegeräte, die beispielsweise der Lösungsanbieter Elatec im Portfolio hat, sind praktisch mit jeden von Anwendern genutzten Kartentechnologien kompatibel und können mobile Berechtigungsausweise verarbeiten. Sie sind damit ideal für den Einsatz im Bereich EV-Charging geeignet. So bieten sie mit einem einzigen, einfach zu integrierenden Gerät eine Lösung, die Vertrieb und Bestandsverwaltung vereinfacht. Für Hersteller bedeutet dies, dass sie nur eine Version ihres Systems für alle potenziellen Kunden vorrätig halten müssen. Die Komplexität wird mit einer solchen Lösung deutlich reduziert.

Zukunftssicherheit durch Remote-Updates und -Upgrades

Anforderungen und IT-Infrastrukturen verändern sich im Laufe der Zeit und machen Anpassungen erforderlich. Nur mit einem flexiblen System, das Optimierungen, Adaptionen und Upgrades vorsieht, sind Anbieter und Betreiber von Ladeinfrastruktur auch in Zukunft auf der sicheren Seite. Die Möglichkeit einer Remote-Konfiguration der Reader ist im Bereich Ladeinfrastruktur daher ein Muss. So können Betreiber und OEMs schnell auf sich ändernde IT-Infrastrukturen und Anforderungen reagieren und problemlos Optimierungen, Adaptionen und Upgrades vornehmen. Mit Remote-Updates und -Upgrades können alle installierten Lesegeräte zudem unabhängig von ihrem Standort einfach und schnell aktualisiert werden, ohne dass hohe Kosten für Techniker anfallen.

Fazit

Nicht nur Großkonzerne und staatliche Stellen mit eigenen Flotten, sondern zunehmend auch kleine Unternehmen und Vermieter werden den Ausbau der Ladeinfrastruktur in den kommenden Jahren voraussichtlich stark vorantreiben. Betreiber und OEMs, die auf eine sichere, skalierbare und marktübergreifend anwendbare Authentifizierungslösung setzten, sind klar im Vorteil und haben die Chance, einen entscheidenden Beitrag für eine stabile Ladeinfrastruktur zu leisten. ■

Johannes Weil
Head of Industry Team Europe,
Elatec GmbH, Puchheim
info-rfid@elatec.com