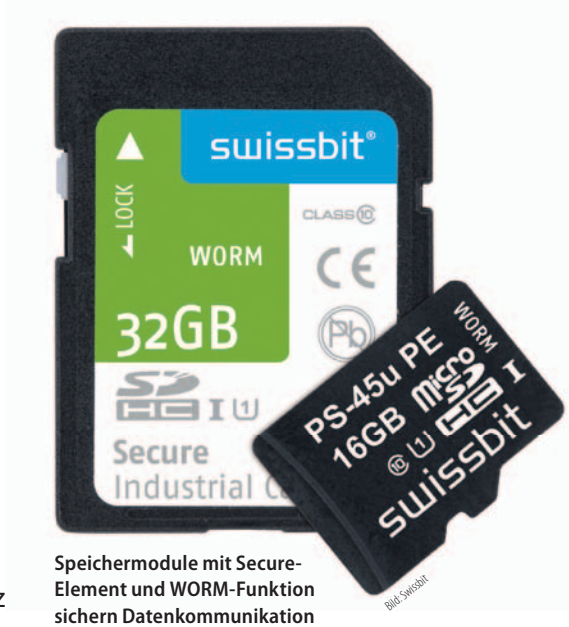
Wie färbt man Strom?
Technische Aspekte der E-Mobilitätsbesteuerung

Mit über 31 Milliarden Euro machte die Mineralölsteuer 2017 über zehn Prozent der gesamten steuerlichen Einnahmen des Bundes aus – Einnahmen, die mit dem Siegeszug der E-Mobilität künftig wegfallen. Der Zeitpunkt naht, an dem Strom für E-Mobilität anders als der übrige Stromverbrauch besteuert werden muss. Heizöl hat man – im Gegensatz zu Diesel – eingefärbt, aber wie färbt man Strom?

Autor: Hubertus Grobbel



Speichermodule mit Secure-Element und WORM-Funktion sichern Datenkommunikation und -Speicherung bei Ladesäulen ab.

Bild: Swissbit

KEYWORDS

Abrechnung / Ladeinfrastruktur / Security

In Deutschland ist Elektromobilität bisher eine Randerscheinung, von Industrie und Politik nur halbherzig gefördert. Doch nicht erst seit China eine feste Quote für elektrisch betriebene Autos eingeführt hat, steht fest: Die Welt nimmt langsam aber sicher Abschied vom Verbrennungsmotor. Damit werden auch wichtige staatliche Einnahmequellen verschwinden. Neben der Mineralölsteuer selbst sind das Steuereinnahmen von Tankstellen und all den Unternehmen, die von der bisherigen Motorentechnik leben. Auch wenn die Politik noch mit Steueranreizen wirbt: Um die Kosten der Verkehrsinfrastruktur künftig tragen zu können, muss in E-Mobilen verbrauchter Strom besteuert werden – deutlich höher als der für andere Verbraucher in Haushalten.

VERBRAUCHSABHÄNGIGE BESTEUERUNG

Der große Vorteil der aktuellen Mineralölsteuer besteht darin, dass im Gegensatz zur Kfz-Steuer oder einer pauschalen Maut nicht das Vorhalten eines Fahrzeugs oder die Möglichkeit der Nutzung, sondern der Umfang der konkreten Nutzung besteuert wird. Wer mehr Energie verbraucht, die Umwelt belastet und die Straßen (ab)nützt, zahlt automatisch mehr.

Und so stellt sich die Frage, wie man den Strom besteuern könnte, der in ein E-Mobil geladen wird. Hier gibt es eine ganze Reihe von ungeklärten Fragen. Wir wissen nicht, wann der Zeitpunkt kommt, an dem hier eine Lösung bereitstehen muss. Eine Unbekannte ist die Ladeinfrastruktur, die dann vorherrschen wird. Fest steht: Aktuell gibt es noch nicht mal eine einheitliche verbrauchsabhängige Abrechnung von Strom für E-Mobile.

Stand heute wäre auch völlig unklar, wie hier eine Steuer aufzuschlagen wäre. Ladestationshersteller und Betreiber gehen ganz unterschiedliche Wege, und das hat seinen Grund. Theoretisch wäre die Abrechnung nach Kilowattstunden die einfachste Lösung. Der Nutzer bezahlt, was er entnimmt. Doch Strom ist im Verhältnis zu den Kosten für Ladeinfrastruktur und Abrechnungssystem zu billig, eine Amortisation über den bloßen Stromverbrauch nicht wirtschaftlich. Autos, die vollgeladen weiter an der Ladesäule stehen, belegen den Platz und verhindern Umsatz. Die Konsequenz: Ein bunter Mix von Abrechnungsmodellen. Einige Betreiber nehmen Pauschalbeträge, andere rechnen den Strom in Parkgebühren ab. Viele Geschäfte subventionieren den Stromverbrauch am E-Parkplatz über den Einkauf. Es gibt auch aufwendigere Mischformen, die den Stromverbrauch und die Platzbelegung berücksichtigen. Hier werden also Stromverbrauch und andere Leistungen (Parken und

ähnliches) miteinander vermischt – schwierige Voraussetzungen für eine zielgerichtete, verbrauchsabhängige Besteuerung von E-Mobilität.

EXTREM ANFÄLLIG

Ein andere Herausforderung: Beim Kongress 34c3 des Chaos Computer Clubs wurde öffentlich gemacht, wie extrem ungeschützt vor Betrug und Manipulationen die derzeitige Ladestelleninfrastruktur ist. Die Identifikation des Nutzers erfolgt über eine unverschlüsselt übertragene, einfach auszulesende Nummer auf einer RFID-Karte. Das Abfischen kann bei der Übertragung erfolgen, aber die übertragene Nummer ist zudem auch einfach über die Logfiles der Ladestation auslesbar. Der Chaos Computer Club zeigte, wie einfach diese Kundennummer ausgelesen und fast beliebig kopiert werden konnte. Mit einer Kartenkopie lässt sich dann bequem auf Kosten anderer tanken. Weitere Manipulationschancen: Auch die Ladestellenbetreiber selbst könnten Kunden über gefälschte Ladevorgänge unberechtigt Stromkosten in Rechnung stellen. Wer weiß schon auf die Kilowattstunde genau, wann er bei den vielen Ladevorgängen wo geladen hat. Vom Open-Charge-Point-Protocol über ungeeignete RFID-Tokens bis hin zu ungeschützten USB-Schnittstellen in der Ladesäulenhardware reichen die Schwachpunkte. Hier besteht Handlungsbedarf – natürlich auch hinsichtlich zukünftiger fiskalischer Prozesse, die auf Ladeabrechnungen basieren sollen.

SICHERE KOMMUNIKATION

Es muss also nachgebessert werden. Die Kommunikation bei der Abrechnung an Stromtankstellen muss sicherer werden. Die leistungsfähigeren Gleichstromladeverfahren Chademo und CCS sehen bereits eine Kommunikation zwischen Auto und Ladesäule vor, weil sich beide Teilnehmer über den jeweils möglichen Ladestrom und Sicherheitsmechanismen „absprechen" müssen. Es bietet sich also an, auf diesem Kommunikationsweg einen Identifikations- und Authentisierungsprozess ablaufen zu lassen. Dieser würde eine eindeutige, fälschungssichere Zuordnung von Fahrzeug und Ladestelle sowie eine sichere Kommunikation für Abrechnungsvorgänge erlauben. Die gesamte Kommunikation sollte dabei verschlüsselt ablaufen, um Man-in-the-Middle-Angriffe zu unterbinden. Reine Softwarelösungen sind dabei immer problematisch. Analog zum physischen Token – beispielsweise einem Smartcard-Mitarbeiterausweis für die Zwei-Faktor-Authentisierung – brauchen Geräte, die sicher kommunizieren sollen, ebenfalls ein Secure-Element als „Ausweis". Bisher muss man, wenn man ein Gerät mit einem Secure-Element versehen will, entweder eine identifizierbare Hardwarekomponente in Form eines TPM (Trusted Platform Module) in den Baugruppen auflöten oder Prozessoren einsetzen, die über integrierte Elemente eindeutig identifizierbar sind (Trusted Execution Environment – TEE).

Eine alternative, leicht zu integrierende und zudem nachrüstbare Lösung sind industrietaugliche Flash-Memory-Karten, in denen ein Secure-Element als Identifizierungsmerkmal verbaut ist, das die Funktion eines TPM übernimmt. Dabei sind die Speicher-Schnittstellen standardisiert, und Flash-Speicher mit TPM-Funktion sind in verschiedenen Formfaktoren als SD-, Micro-SD-Karten oder als USB-Sticks verfügbar. Die sicheren Flash-Memory-Module basieren auf Karten, die bereits seit Jahren für den Industrieeinsatz spezifiziert sind. Ihre Spezifikationen umfassen beispielsweise deutlich erweiterte Temperaturbereiche sowie eine längere Lebensdauer und Verfügbarkeit. Die Idee, das Identifizierungsmerkmal mit einem Standarddatenspeicher zu kombinieren, hat auch deshalb Charme, weil die Ladesäule sowieso Speicher für ihr Betriebssystem und Logdaten benötigt. Die sicheren Speicherkarten bestehen aus einem Flash-Speicherchip, einer Smartcard und einem Flash-Controller, dessen spezielle Firmware mit integriertem AES-Enkryptor eine ganze Reihe von Anwendungsszenarien ermöglicht.


Bild: Fotolia

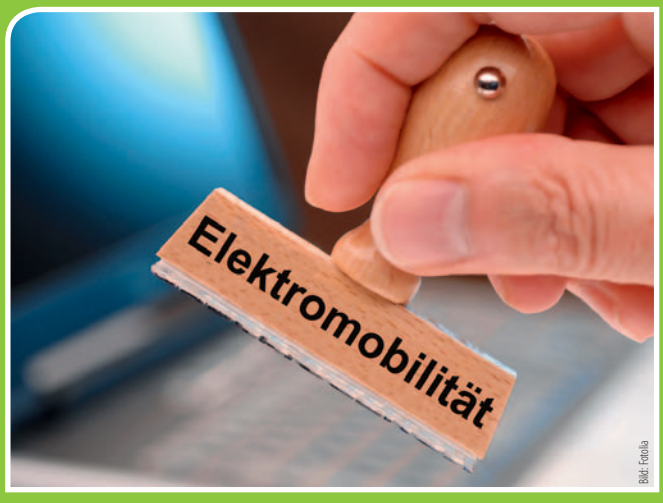


Bild: Fotolia


Bild: Fotolia

FÄLSCHUNGSSICHER

Kommen wir zurück zur Frage der Erhebung einer Mobilitätsenergiesteuer auf Basis tatsächlicher Strommengen. Um sicherzustellen, dass nur korrekt versteuerter Strom fließt, muss der Stromzähler der Ladesäule manipulationssicher sein. Auch hierfür bieten die genannten Flash-Speicher eine Lösung: Mit ihrer WORM-Funktion (Write Once Read Multiple) werden Daten digital signiert archiviert. Diese Karten kommen international bereits in Bodycams von Polizeikräften zum Einsatz, um Beweisvideos manipulationssicher zu machen. Eine weitere aktuelle Anwendung sind die Registrierkassen für den französischen Einzelhandel. Hier sind es Manipulationen in Bezug auf die Umsatzsteuer, die durch Sicherheitsspeichermedien verhindert werden. Was für die Registrierkassen gilt, lässt sich fast eins zu eins auf Ladesäulen umsetzen: Die Registrierkasse kann keine Transaktionen durchführen, bevor die SD-WORM-Karte eingelegt ist, wodurch sichergestellt ist, dass alle Transaktionen aufgezeichnet werden. Außerdem ist die SD-Karte dauerhaft kryptografisch mit der Kasse verbunden, auf der sie initialisiert wurde. Die Herkunft der Daten ist daher für die Steuerverwaltung absolut sicher. Alle Transaktionen werden gleichzeitig mit der Ausgabe eines Kassenbelegs auf der SD-Karte aufgezeichnet. Auch bei einem Geräteausfall geht keine Transaktion verloren. Die Verwendung von WORM-Flash-Karten ist zuverlässig, da der auf der Karte gespeicherte Inhalt weder absichtlich noch versehentlich verändert oder gelöscht werden kann. Eine digitale Signatur mit dem ECDSA-521-Bit-Algorithmus ermöglicht die gesetzlich vorgeschriebene sichere Archivierung der Daten ohne Manipulationsrisiko.

Eine zuverlässige Lösung für Ladesäulen hat ganz ähnliche Anforderungen und lässt sich auf ähnliche Weise sichern. So kann beispielsweise die Physikalisch-Technische Bundesanstalt Module für diese Funktion als „Fiskalmodule“ zertifizieren. Verschiedene Hersteller und Betreiber sind dann in der Lage, diese Fiskalmodule in die Ladesäulen zu integrieren. Betrieb und Technik der Ladesäule wären unabhängig von der manipulationssicheren Besteuerung.

DAS PRINZIP UMKEHREN

Die vorangegangenen Überlegungen beziehen sich auf das Laden an öffentlichen Säulen, also Ladestellen in Verbindung mit einem Parkplatz oder Schnellladestellen, als Ersatz für die Tankstellen. Zusätzlich stellt sich die Frage, wie mit dem Laden am heimischen Drehstromnetz umzugehen ist. Will man hier eine unterschiedliche Versteuerung des geladenen Stroms durchsetzen, müssten zertifizierte fälschungssichere Entnahmestellen vorgeschrieben werden und die Autos dürfen nur an diesen laden können. Dem Strom auf diese Weise eine Farbe zu geben, wäre extrem aufwendig und schwierig in der politischen Umsetzung. Es widerspricht auch den im Zusammenhang mit der Energiewende vorgeschlagenen Smart-Grid-Konzepten, bei denen die Batterien der Automobile einen Teil des Puffers für ein Stromüberangebot aus regenerativen Quellen darstellen sollen. Eine denkbare Alternative: Man verlegt die gesamte Erfassung des zu versteuernden E-Mobilstroms in die Fahrzeuge, indem diese ihren Stromverbrauch manipulationssicher protokollieren – wieder analog zur Registrierkasse. In diesem Fall müsste die Steuer allerdings über die Verbraucher eingetrieben werden und nicht über die Energieanbieter.

Wie immer auch die Lösung aussehen wird, wenn das Finanzministerium dereinst eine Alternative für die Mineralölsteuer sucht: Kommunikation und Datenspeicherung gegen Manipulationen abzusichern, muss nicht aufwendig sein.

FAZIT

Trotz aller aktuellen Steuersubventionen: Spätestens, wenn die Einnahmen der Mineralölsteuer wegen einer steigenden Anzahl von E-Automobilen wegfallen, wird der Staat wohl auf die in Elektrofahrzeugen verbrauchte Energie eine zusätzliche Steuer aufschlagen müssen. Ladesäulen – derzeit noch äußerst manipulationsgefährdet – werden dann zuverlässig die Strommengen dokumentieren müssen, wenn diese Grundlage der Besteuerung werden. USB-, SD- und Micro-SD-Speichermodule mit Secure Element und WORM-Funktionalität sind eine einfache und günstige Möglichkeit zur Absicherung von Datenkommunikation und Speicherung. Ladesäulen lassen sich so analog zu fälschungssicheren Registrierkassen mit „Fiskalmodulen“ nachrüsten. *(av)* //

Autor
Hubertus Grobbel
Leiter des Geschäftsbereichs Security Products bei Swissbit