Eichrechtlich konforme Messwert-erfassung in Ladesäulen

Eichrecht und Ladesäulen

Die jährlichen Zulassungszahlen von Elektrofahrzeugen steigen immer weiter und auch die Bundesregierung verfolgt das Ziel, ca. 1 Million Elektrofahrzeuge bis zum Jahr 2022 auf deutsche Straßen zu bringen.

Dazu ist eine entsprechend ausgebaute Ladesäuleninfrastruktur notwendig. Dies stellt zwar auch eine technische, vor allem aber eine gesetzliche Hürde dar: Soll an der Ladesäule nach Verbrauch abgerechnet werden, muss diese dem Eichrecht entsprechen.

Hier hakt es im Wesentlichen an zwei Punkten:

- Das MessEG fordert die Nachprüfbarkeit von Messergebnissen. Für Ladesäulen in einer öffentlichen Ladeinfrastruktur bedeutet das, dass der Kunde in der Lage sein muss, die Angaben auf seiner Rechnung, die möglicherweise erst zu einem späteren Zeitpunkt kommt, nachträglich zu prüfen.

- Darüber hinaus müssen Schnellladesäulen seit dem 1. April 2019 mit geeichten Gleichstromzählern ausgestattet sein.

Arbeiten und Lösungen

Dieser Stand präsentiert das Ergebnis der Forschungsarbeiten zum Thema „Eichrechtlich konforme Messwerterfassung und NTS-gesicherte Zeitstempelung in Ladesäulen für E-Fahrzeuge“, die an der Ostfalia Hochschule für angewandte Wissenschaften in Kooperation mit der Physikalisch-Technischen Bundenstalt entstanden sind. Sie berücksichtigen die gesetzlichen Vorgaben und stellen ein Konzept sowie eine Softwarearchitektur für eichrechtlich konforme Ladesäulen vor. Das Ergebnis ist ein Testaufbau einer Ladesäule, der dieses Konzept praktisch umsetzt.

Ostfalia
Hochschule für angewandte Wissenschaften
Fakultät Elektrotechnik

Ostfalia Hochschule für angewandte Wissenschaften
Fakultät Elektrotechnik
Salzdahlumer Str. 46/48
38302 Wolfenbüttel
https://www.ostfalia.de/e

Kai Heine, M. Eng.
Embedded Systems Group
Telefon: 05331-939-43650
E-Mail: ka.heine@ostfalia.de

Prof. Dr.-Ing. Rainer Bermbach
Embedded Systems Group
Telefon: 05331-939-42620
E-Mail: r.bermbach@ostfalia.de

PTB

Physikalisch-Technische Bundesanstalt
Bundesallee 100
38116 Braunschweig

Dr. Christoph Leicht
2.34 | Messeinrichtungen und -systeme für Elektrizität

Telefon: 0531 592-2340
E-Mail: christoph.leicht@ptb.de
www.ptb.de

Stand: 04/19

PTB
Physikalisch-Technische Bundesanstalt
Nationales Metrologieinstitut

Sichere Zeitführung einer Ladesäule

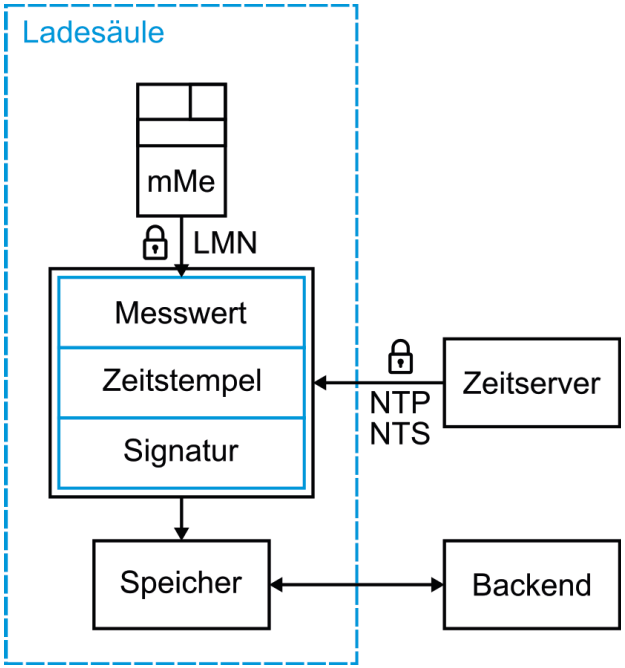
Network Time Security in der Elektromobilität

Gesamtkonzept für eichrechtlich konforme Ladesäulen

Das entwickelte Gesamtkonzept sieht im Kern den unten dargestellten Ablauf vor.

Messwerte zu einem Ladevorgang werden dabei TLS-gesichert über die LMN-Schnittstelle einer *modernen Messeinrichtung* (mMe) ausgelesen. Dazu kommt ein Zeitstempel aus einer Uhr, die über das *Network Time Protocol* mit der gesetzlichen Zeit synchronisiert ist und dabei mittels *Network Time Security* abgesichert wird. Gemeinsam mit allen weiteren abrechnungsrelevanten Daten wird das Messwerttupel anschließend mit einer digitalen Signatur versehen, welche die Integrität und Vertrauenswürdigkeit sicherstellt.

Die Ladesäule speichert diesen Datensatz, überträgt ihn zum Ladesäulenbackend und stellt ihn auf Anfrage über eine Anzeige bereit.

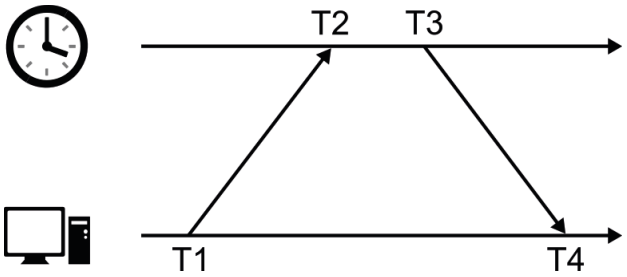


Vereinfachter Aufbau der Ladesäule

Synchronisation der Uhrzeit mit dem Network Time Protocol NTP

Wie in vielen computergesteuerten Systemen ist auch in Ladesäulen eine genaue Uhrzeit von entscheidender Bedeutung. Für die Zeitsynchronisation über das Netzwerk kommt dabei typischerweise das *Network Time Protocol* (NTP) zum Einsatz.

NTP beschreibt ein Netzwerkprotokoll zur Synchronisation der Uhrzeit eines Clients mit der eines Zeitservers. Entsprechend der Abbildung ermittelt der Client durch den Informationsaustausch mit dem Server mehrere Zeitstempel, aus denen er seinen eigenen Zeitversatz berechnen und damit seine Uhr stellen kann. Dieser Mechanismus erlaubt prinzipiell sehr hohe Genauigkeiten.



Zeitsynchronisation mit NTP

Ohne weitere Maßnahmen ist NTP jedoch völlig ungesichert. Ein Angreifer kann daher unbemerkt Pakete manipulieren oder verzögern und somit indirekt die Uhrzeit des Clients verstellen. Zwar gab es bereits in der Vergangenheit Ansätze, NTP abzusichern, jedoch haben diese sich als unsicher herausgestellt oder skalieren schlecht auf eine hohe Anzahl von Systemen.

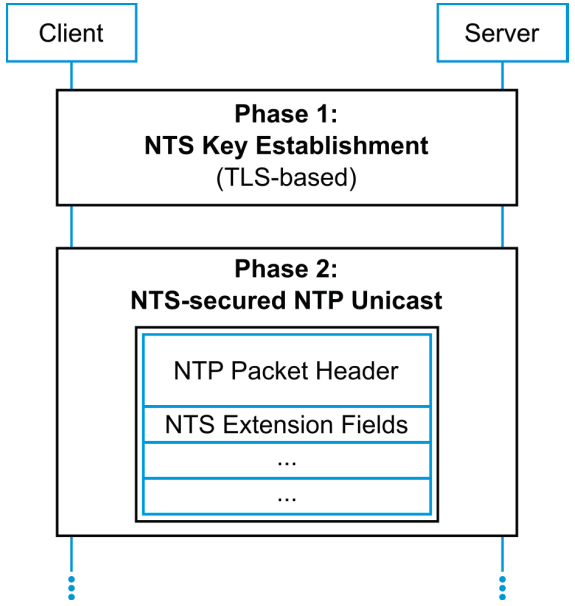
Abhilfe schafft das Protokoll *Network Time Security* (NTS).

Absicherung von NTP mit Network Time Security (NTS)

Network Time Security (NTS) ist eine Erweiterung zu Zeitprotokollen wie NTP mit dem Ziel, die Daten vor Manipulation zu schützen und gleichzeitig skalierbar zu sein.

Dazu agiert NTS in zwei Phasen: In der ersten Phase tauschen Client und Server über einen sicheren TLS-Kanal Schlüssel und Algorithmen aus, die anschließend zur Sicherung der NTP-Pakete genutzt werden. Der Server versorgt den Client mit kryptographisch gesicherten Cookies, mit denen der Client sich einerseits gegenüber dem Server authentifizieren kann und aus denen der Server jederzeit alle ausgehandelten Parameter herausziehen kann. Somit kann der Server anschließend zustandslos arbeiten.

In der zweiten Phase werden ganz normale NTP-Pakete ausgetauscht. Letztere enthalten Erweiterungsfelder, die zum Transport der Cookies und zur Absicherung des Paketes dienen.



Ablauf der NTS-gesicherten Zeitsynchronisation