Ostfalia
Hochschule für angewandte Wissenschaften

Fakultät Elektrotechnik

Sichere Zeitführung einer Ladesäule

Network Time Security in der Elektromobilität

Kai Heine, Rainer Bermbach

Ostfalia
Hochschule für angewandte Wissenschaften

Eichrechtliche Vorgaben

- MessEG und MessEV:
  - Wesentliche Anforderungen an Messgeräte für den geschäftlichen und amtlichen Verkehr

- Ergänzende Dokumente für Messeinrichtungen in der Elektromobilität:
  - Dokument 6-A des Regelermittlungsausschusses
    - Konkretisierung der MessEV für die Elektromobilität
  - VDE-Anwendungsregel 2418-3-100
    - Referenzarchitektur für den inneren logischen Aufbau von Ladeeinrichtungen

Ostfalia
Hochschule für angewandte Wissenschaften

Eichrechtliche Vorgaben

- Abrechnungsrelevante Daten:
  - Identifizierung des Kunden (z.B. EMAID) oder des Geschäftsvorgangs (Transaktions-ID)
  - Anfangs- und Endzählerstände mit physikalischer Einheit
  - Zeitstempel aus einer gesichert synchronisierten Uhr
  - Digitale Signatur über den gesamten Datensatz

➔ Eindeutige Anzeige

➔ Dauerhafte Speicherung

➔ Prüfbarkeit

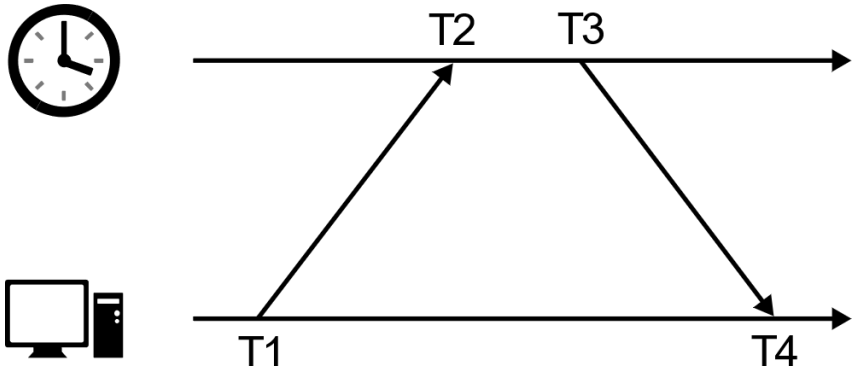
Ostfalia
Hochschule für angewandte Wissenschaften

Eichrechtliche Vorgaben

- Synchronisation der Uhr mit der gesetzlichen Zeit
  - Maximale Abweichung: 3% der Messperiode
- Schutz vor Manipulation
  - „Rückwirkungsfreie Schnittstellen“
  - Kryptografischer Schutz der Integrität und Authentizität
- Einhaltung von Fehlergrenzen
  - Richtlinie 2014/32/EU
- Einfache Bedienung
  - Ungewollte Falschbedienung darf nicht möglich sein

Sichere Zeitsynchronisation

- Zeitsynchronisation über das Netzwerk typischerweise mit dem *Network Time Protocol* (NTP)
  - Funktionsweise: Austausch von Zeitinformationen zwischen Client und Server



  - Aus den ermittelten Zeitstempeln können Offset (θ) und Round-Trip-Delay (δ) berechnet werden:

$$\vartheta = \frac{(T_2 - T_1) - (T_4 - T_3)}{2} \qquad \delta = (T_4 - T_1) - (T_3 - T_2)$$

  - Mit diesen Informationen kann der Client seine Uhr stellen und anpassen.

Ostfalia
Hochschule für angewandte Wissenschaften

Sichere Zeitsynchronisation

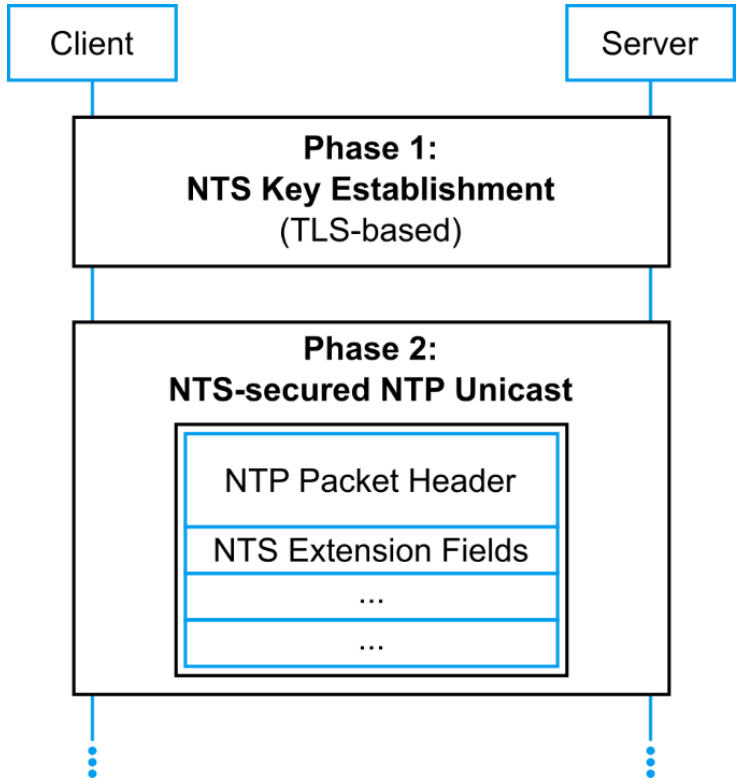
- Problem: NTP ist ohne Weiteres völlig ungesichert
  - Angreifer können unbemerkt Pakete manipulieren und verzögern ➔ Client stellt seine Uhr falsch
  - Bisherige Ansätze zur Absicherung existieren, sind aber ungeeignet:
    - Autokey-Verfahren: nutzt unsichere Kryptografie
    - Symmetric-Key-Verfahren: sicher, aber nicht skalierbar (manueller Schlüsselaustausch)

- Abhilfe schafft *Network Time Security* (NTS)

Sichere Zeitsynchronisation

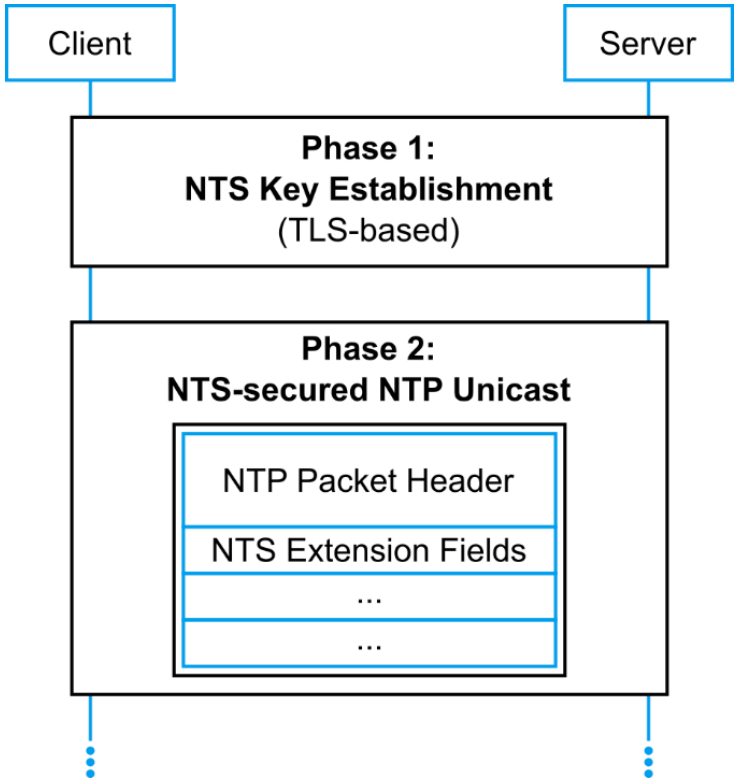
- Network Time Security (NTS)
  - Erweiterung für Zeitprotokolle wie NTP
  - Aktuell im Draft-Status bei der IETF (draft-ietf-ntp-using-nts-for-ntp-18)
  - Ziel: Sicherheit + Skalierbarkeit ohne Verlust von Genauigkeit

- Agiert in zwei Phasen:
  1. TLS-basierter Schlüsselaustausch
  2. NTS-gesicherter NTP-Unicast-Betrieb



Sichere Zeitsynchronisation

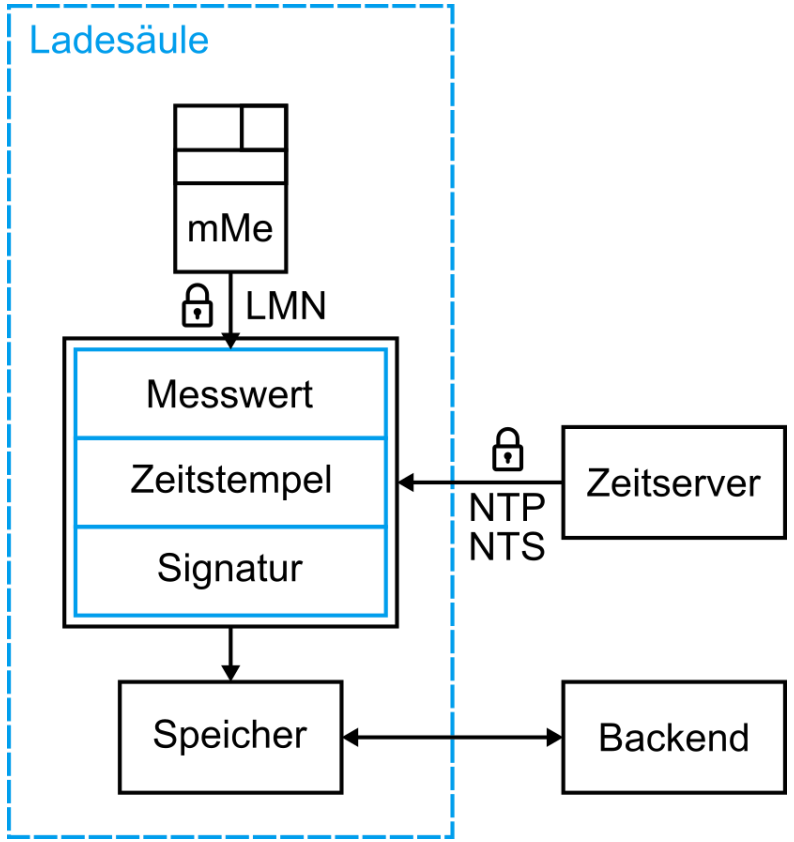
- Phase 1: TLS-basierter Schlüsselaustausch (NTS Key Establishment)
  - Aushandlung von Schlüsseln, Algorithmen (AEAD-Verfahren) und Cookies
  - Cookies lagern den Zustand des Servers auf den Client aus



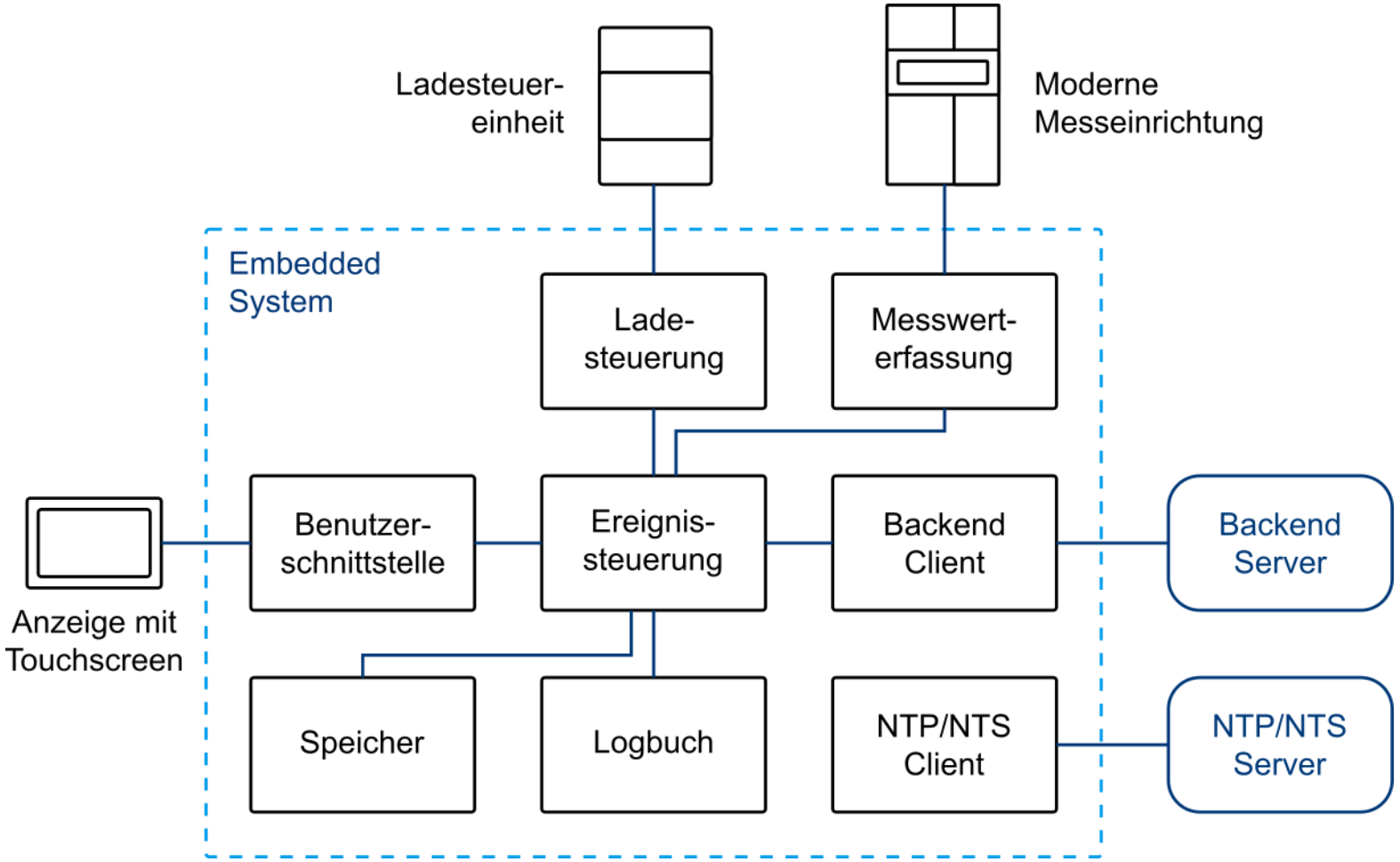
- Phase 2: NTS-gesicherter NTP-Betrieb
  - Austausch von NTP-Paketen mit NTS-Erweiterungsfeldern:
    - Eindeutige Paketkennung
    - Cookies
    - Feld zur Integritätssicherung
  - Server kann anhand der Cookies seinen Zustand wiederherstellen
  - Client sendet Cookie-Platzhalter mit und wird vom Server mit neuen Cookies versorgt

Aufbau und Konzept der Ladesäule

- Eichrechtlich konforme Messwerterfassung
  - Auslesen einer modernen Messeinrichtung über die TLS-gesicherte LMN-Schnittstelle
- Sichere Zeitsynchronisation und Zeitstempelung
  - Einsatz von NTP und NTS
- Signierung und Speicherung des Messwerttupels
  - Lokal und Transport ins Backend über OCPP



Aufbau und Architektur der Ladesäule

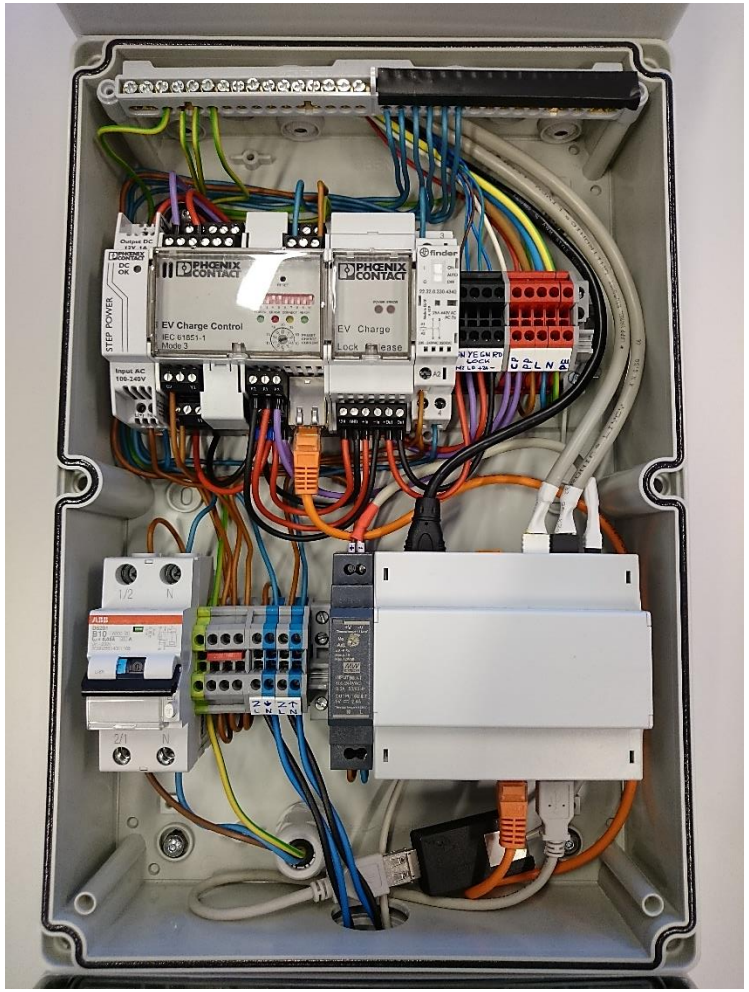


Aufbau und Architektur der Ladesäule

- Test-Aufbau als einphasige AC-Ladesäule
  - Ladesteuerung über vorgefertigte Hardwarekomponenten
- Ausführung der Software auf einem Embedded Linux System
  - Kapselung und Isolierung von Softwarekomponenten in Containern für Sicherheit und Wiederverwendbarkeit
  - Netzwerkbasierte Kommunikation untereinander über REST-Schnittstellen
- Rudimentäre Backend-Anbindung
  - Platzhalter für öffentliche Ladeinfrastruktur

Aufbau und Architektur der Ladesäule

- Test-Aufbau als einphasige AC-Ladesäule
  - Ladesteuerung über vorgefertigte Hardwarekomponenten
- Ausführung der Software auf einem Embedded Linux System
  - Kapselung und Isolierung von Softwarekomponenten in Containern für Sicherheit und Wiederverwendbarkeit
  - Netzwerkbasierte Kommunikation untereinander über REST-Schnittstellen
- Rudimentäre Backend-Anbindung
  - Platzhalter für öffentliche Ladeinfrastruktur



Ostfalia
Hochschule für angewandte Wissenschaften

Zusammenfassung

- **Konzept für eine eichrechtlich konforme Ladesäule**

- Manipulationsschutz und Sicherheit:
  - Auslesen einer mMe über die LMN-Schnittstelle im Vorgriff auf den Einsatz eines SMGw
  - Gesicherte Synchronisation der Systemzeit mit NTP und NTS
- Prüfbarkeit:
  - Dauerhafte Speicherung mit digitaler Signatur lokal und im Backend
  - Anzeige des Messergebnisses mit allen relevanten Informationen
- Softwarekonzept:
  - Embedded Linux mit Containerisierung
  - Rückwirkungsfreie REST-Schnittstellen

Ostfalia
Hochschule für angewandte Wissenschaften

Ende

Haben Sie Fragen?

Ostfalia Hochschule für angewandte Wissenschaften
– Hochschule Braunschweig/Wolfenbüttel
Salzdahlumer Str. 46/48 · 38302 Wolfenbüttel
Fakultät Elektrotechnik