Vergleichende Betrachtung der Sicherheitskonzepte von Mobile Metering und Smart Meter Gateways

Jan Weil*, Jörg Neumann**

Einleitung

Als eine der Voraussetzungen für die Energiewende sieht die Bundesregierung intelligente Netze an, „die nicht nur Strom transportieren und verteilen, sondern stets auch das notwendige Gleichgewicht zwischen Erzeugung und Verbrauch sicherstellen müssen“ [1]. Teil solcher intelligenten Netze sind intelligente Zähler (Smart Meter), die bereits durch das Veranschaulichen des Verbrauchs Einsparpotenzial bieten sollen. Durch das Hinzufügen eines vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten Smart Meter Gateways (SMGW) ergibt sich ein intelligentes Messsystem, das die sichere Kommunikation der Messdaten gewährleistet. Dabei ist der Schutz der personenbezogenen Daten als Voraussetzung für die öffentliche Akzeptanz die primäre Motivation des SMGW.

Im Forschungsprojekt On-Board Metering [2] wurde unter anderem der Prototyp eines mobilen Elektrizitätszählers entwickelt, der Grundlage der gemessenen Abrechnung von Ladevorgängen für Elektrofahrzeuge ist. Wird ein solcher mobiler Zähler (Mobile Meter) zur Abrechnung verwendet, muss in den Ladepunkten keine Zähl- und Kommunikationstechnik verbaut werden. Dadurch werden nicht nur die Größe eines Ladepunkts, sondern auch seine Installations- und Betriebskosten deutlich reduziert, was den wirtschaftlichen Betrieb der Ladeinfrastruktur ermöglicht. Der mobile Zähler des OBM-Projekts enthält ein Steuer- und Kommunikationsmodul, das unter anderem den Schutz der Messdaten sicherstellt.

Im Folgenden werden die beiden den jeweiligen Systemen zugrunde liegenden Sicherheitskonzepte verglichen und die Unterschiede hervorgehoben.

Projekt On-Board Metering

On-Board Metering (OBM) ist ein vom Bundesministerium für Wirtschaft und Energie (BMWi) im Zeitraum 05.2010-05.2015 gefördertes Forschungsprojekt, in dessen Rahmen ein innovatives Konzept zur Bereitstellung, Messung und Abrechnung von geladenem Strom entwickelt wurde. Am Projekt waren die ITF-EDF Fröschl GmbH, der Fachbereich Metrologische Informationstechnik der PTB, die ubitricity Gesellschaft für verteilte Energiesysteme mbH und die VOLTARIS GmbH beteiligt. Das Projekt verlief in zwei Phasen: OBM I, bis 08.2012, beinhaltete Konzept und Validierung, OBM II die Feldtests. Das hier beschriebene Sicherheitskonzept spiegelt den Stand wider, wie er im Rahmen dieses Forschungsprojekts verwirklicht wurde. Das Mobile-Metering-System,

* Jan Weil, Arbeitsgruppe 8.52 “Metrologische IKT-Systeme”,

** Jörg Neumann, Arbeitsgruppe 8.52 “Metrologische IKT-Systeme”, E-Mail: joerg.neumann@ptb.de

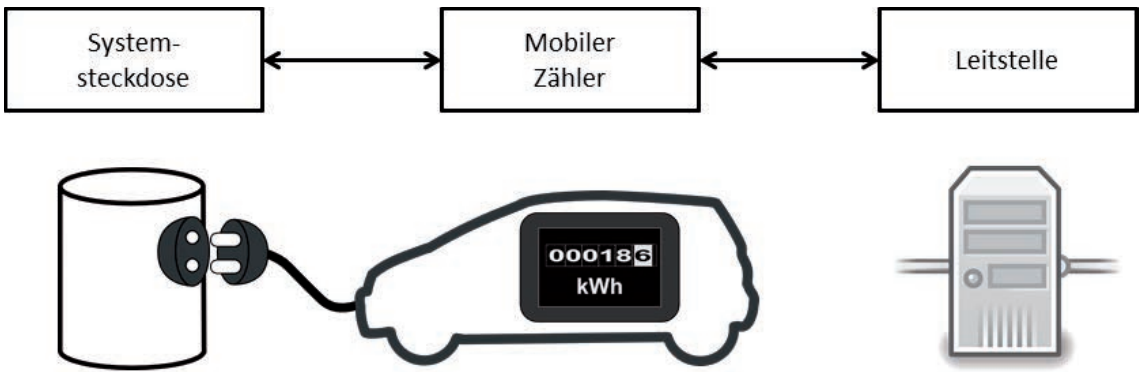

Bild 1:
OBM-Systemarchitektur (reduziert)

wie es von den beteiligten Firmen im Anschluss an das Forschungsprojekt marktreif ausgestaltet wird, basiert auf den Ergebnissen des Forschungsprojektes, unterscheidet sich jedoch in Details der Spezifikation.

OBM-Systemarchitektur

Das Bild 1 stellt einen Teil der OBM-Systemarchitektur in vereinfachter Form dar. Das OBM-Konzept sieht vor, die Komplexität der Ladepunkte möglichst weitgehend zu reduzieren und so deren Installations- und Betriebskosten deutlich zu senken. Dazu wird insbesondere die in konventionellen Ladesäulen meist enthaltene Zähl- und Kommunikationstechnik ins Fahrzeug verlagert. Die als Ladepunkt verbleibende Komponente wird im OBM-Kontext Systemsteckdose genannt. Sie ist schaltbar und enthält im Wesentlichen einen Mikrocontroller, eine Kommunikationsschnittstelle zum mobilen Zähler und ein Sicherheitsmodul zur Personalisierung und zur Absicherung der Kommunikation.

Der mobile Zähler kann in der Terminologie der PTB-Anforderungen 50.7 [3] als Elektrizitätszähler mit Zusatzeinrichtung aufgefasst werden. Er enthält neben dem geeichten Elektrizitätszähler einen Mikrocontroller, eine Echtzeituhr, Kommunikationsschnittstellen zur Systemsteckdose (kabelgebunden) und zur Leitstelle (Mobilfunk) und ebenfalls ein Sicherheitsmodul. Abgesehen vom geeichten Elektrizitätszähler und dem Sicherheitsmodul sind alle Komponenten des mobilen OBM-Zählers in modernen Fahrzeugen typischerweise bereits vorhanden. Deshalb erreicht das OBM-System in seiner On-Board-Variante die höchste Kosteneffizienz. Allerdings ist es sehr aufwendig, neue Komponenten im Automotive-Lieferantenmarkt zu etablieren, weswegen im OBM-Projekt ebenfalls eine Variante realisiert wurde, in der der mobile Zähler im Ladekabel verbaut ist. Ein solches intelligentes Ladekabel ermöglicht es normkonformen Elektrofahrzeugen, ohne weitere Modifikation an OBM-Ladepunkten zu laden.

Die Leitstelle dient als Schnittstelle ins Back-End, in dem die Messdaten zur Rechnungsstellung und zur marktkonformen Kommunikation aufgearbeitet werden. Jeder mobile Zähler ist mit genau einer Leitstelle verknüpft. Aspekte des Energiedatenmanagements im OBM-Konzept sind in [4] beschrieben.

OBM-Marktrollen und -Geschäftsprozesse

Am wesentlichen Geschäftsprozess des OBM-Konzepts, der Abrechnung eines Ladevorgangs, sind vereinfacht dargestellt folgende Marktteilnehmer beteiligt: Letztverbraucher, Mobilstromlieferanten und Ladepunktanbieter. Ein Letztverbraucher schließt einen Vertrag mit einem Mobilstromlieferanten, erhält einen mobilen Zähler und kann damit Ladevorgänge im Netz der OBM-Ladepunkte durchführen. Ein Ladepunktanbieter stellt an seinen Ladepunkten elektrische Energie für das OBM-System zur Verfügung. Der Mobilstromlieferant stellt dem Letztverbraucher eine Rechnung über die durchgeführten Ladevorgänge. Der Ladepunktanbieter bekommt die an seinen Ladepunkten konsumierte Energie vergütet. Somit müssen sowohl der Letztverbraucher als auch der Ladepunktanbieter darauf vertrauen können, dass die Messwerterfassung und -abrechnung korrekt erfolgt.

Wie auch bei konventionellen Ladesäulen haben jedoch zum Zeitpunkt der Rechnungsstellung nicht beide beteiligten Parteien Zugriff auf die verwendeten Zähler, um die der Rechnung zugrunde liegenden Messdaten zu kontrollieren. Im OBM-System könnte der Letztverbraucher die Ladevorgänge gegebenenfalls im Archiv des mobilen Zählers kontrollieren, sofern sie noch gespeichert sind. Dem Ladepunktanbieter ist der Zugriff auf all die mobilen Zähler, die im Abrechungszeitraum an seinen Ladepunkten verwendet wurden, nicht möglich. Bei konventionellen Ladesäulen wiederum wird der Letztverbraucher nicht in der Lage sein, die in den Ladesäulen verbauten Zähler einzusehen, über die er im Rechnungszeitraum geladen hat. Eines der Hauptziele des OBM-Sicherheitskonzepts ist es deshalb, sowohl für den Letztverbraucher als auch für den Ladepunktanbieter das Vertrauen in die Messdaten zu gewährleisten.

OBM-Sicherheitskonzept

Das OBM-Sicherheitskonzept basiert in seinen Grundzügen auf den Ergebnissen des SELMA-Projekts [5]. Kern des Sicherheitskonzepts ist eine sichere Signaturerstellungseinheit, ein Sicherheitsmodul, das Daten durch das Hinzufügen von digitalen Signaturen auf einzelne Geräte rückführbar macht. Sowohl die mobilen OBM-Zähler als auch die Systemsteckdosen enthalten jeweils ein Sicherheitsmodul, das starke kryptographische Funktionen zur Verfügung stellt. Im OBM-Projekt wurden Chipkarten verwendet, alternativ können auch dedizierte Crypto-Controller, die direkt in die elektronische Schaltung integriert sind, verwendet werden. Das OBM-Sicherheitsmodul ist funktional nahezu identisch zum Sicherheitsmodul des SMGW.

Mobile Zähler und Systemsteckdosen sind in eine Public-Key-Infrastruktur (PKI) eingebunden, siehe Bild 2. Jedes Gerät erhält von der Certification Authority (CA) seines Herstellers ein individuelles digitales Zertifikat, das einen öffentlichen Schlüssel mit der Identität des Geräts verknüpft.

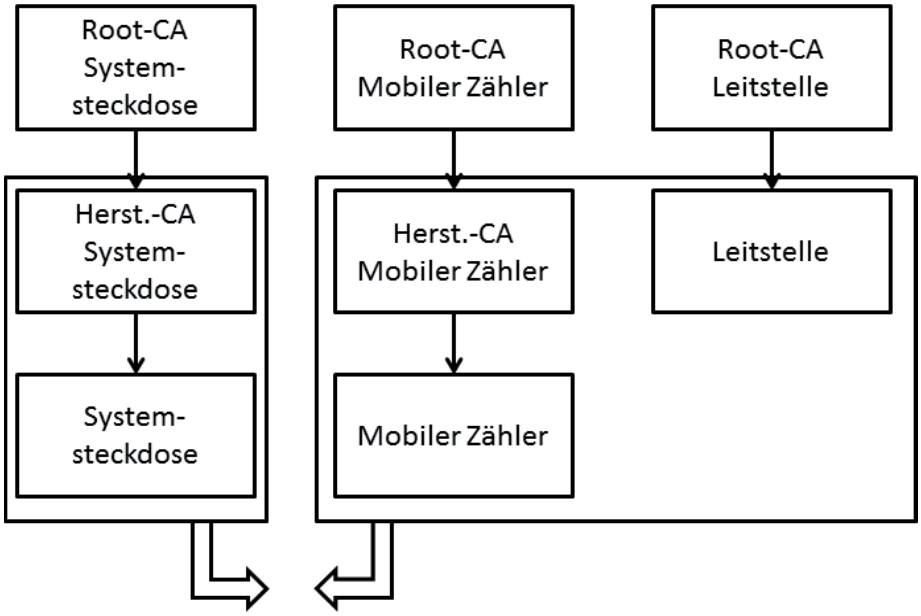

Bild 2:
OBM-Vertrauensketten der PKI

Der dazu gehörige private Schlüssel ist im Sicherheitsmodul des jeweiligen Geräts gespeichert, sodass Vervielfältigung und Missbrauch weitestgehend ausgeschlossen sind. Damit ein mobiler Zähler und eine Systemsteckdose authentifiziert miteinander kommunizieren können, tauschen sie zu Beginn eines Ladevorgangs ihre Gerätezertifikate sowie die Zertifikate ihrer Hersteller-CAs aus. Der mobile Zähler überträgt außerdem das Zertifikat seiner Leitstelle, die ebenfalls in die PKI eingebunden ist, an die Systemsteckdose.

Die Leitstelle ist für die Systemsteckdose die autorisierende Instanz. Die Systemsteckdose schaltet die Spannung also nur dann frei, wenn der angeschlossene mobile Zähler von der Leitstelle als ladeberechtigt ausgewiesen wurde. Dazu generiert die Systemsteckdose einen digital signierten Freigabeanforderungsdatensatz, der zusätzlich vom mobilen Zähler signiert und anschließend an die Leitstelle kommuniziert wird. Die Leitstelle antwortet mit einem digital signierten Freigabeantwortdatensatz, der vom mobilen Zähler an die Systemsteckdose weitergeleitet und von dieser ausgewertet wird.

Die Grundlage für die Abrechnung eines Ladevorgangs ist der dazu gehörige Ladevorgangsdatensatz. Der Ladevorgangsdatensatz enthält die Kennungen von mobilem Zähler und Systemsteckdose, Zeitstempel für den Beginn und das Ende des Ladevorgangs, die Zählerstände des Wirkenergie-Registers zu Beginn und zum Ende des Ladevorgangs sowie die Sequenznummern des mobilen Zählers und der Systemsteckdose. Die Sequenznummern werden jeweils für jeden neuen Ladevorgang inkrementiert. Teil des Ladevorgangsdatensatz ist außerdem der Ladelastgang, der den Zählerstand des Wirkenergie-Registers zu jeder vollen Registrierperiode (in der Regel 15 Minuten) enthält. Der Ladevorgangsdatensatz wird vom mobilen Zähler digital signiert. Die Sequenznummer der Systemsteckdose ist von besonderer Bedeutung für den Ladepunktanbieter. Sie stellt sicher, dass bei der Rechnungsstellung die Vollständigkeit der Datensätze nachvollzogen werden kann. Im Anschluss an einen Ladevorgang wird der Ladevorgangsdatensatz an die Leitstelle übertragen. Auf Transportebene wird die Kommunikation dabei verschlüsselt, um die Vertraulichkeit der Datensätze zu gewährleisten.

Als Teil des Sicherheitskonzepts wurde im OBM-Projekt prototypisch ein anbieterunabhängiges Verifikations-Tool für Letztverbraucher und Ladepunktanbieter entwickelt. Das OBM-Verifikations-Tool Overto analysiert die von mobilen OBM-Zählern generierten Daten auf Plausibilität, Authentizität und Integrität. Overto ist ein Kommandozeilen-Programm, das eine Menge von signierten Ladevorgangsdatensätzen analysiert und einen HTML-Report zur Ansicht mit einem Standard-Webbrowser generiert. Erkannte Fehler in den Daten werden im HTML-Report dargestellt. Overto überprüft im Wesentlichen die Monotonie und Stetigkeit von Zählerständen, Zeitstempeln und Sequenznummern. Es wird also überprüft, ob die Messdaten vollständig sind und ob Zählerstände und Zeitpunkte plausibel sind. Darüber hinaus überprüft Overto die Authentizität und Integrität der Daten durch die Verifikation der von den OBM-Zählern hinzugefügten digitalen Signaturen. Dazu werden die digitalen Zertifikate der relevanten Zähler von einem LDAP-Server geladen und die Gültigkeit der Zertifikate und die Signatu-

ren der Messdaten verifiziert. Ein Overto-Report kann für Letztverbraucher oder für Ladepunktanbieter generiert werden. Für Letztverbraucher sind die Ladevorgänge nach Zählerkennungen sortiert, für Ladepunktanbieter nach den Kennungen der Systemsteckdosen. Es steht somit ein Werkzeug zur Überprüfung einer Rechnung mit einfachen Mitteln, basierend auf den zugrunde liegenden Messdaten, zur Verfügung.

BSI-Schutzprofil Smart Meter Gateway

Das BSI-Schutzprofil [6] für das Smart Meter Gateway (SMGW) beschreibt das SMGW als Target of Evaluation (TOE) eines Protection Profile gemäß Common Criteria [7]. Es dient dabei seiner Umgebung als Kommunikationsmodul und verbindet die Domäne des lokalen Letztverbrauchernetzwerks mit dem nicht vertrauenswürdigen Weitverkehrsnetz (Wide Area Network – WAN). Das lokale Netz ist aufgeteilt in das metrologische Netz (Local Metrology Network – LMN), über das Messgeräte angeschlossen werden, und das Heimnetz (Home Area Network – HAN), über das steuerbare Verbraucher (Controllable Local Systems – CLS) sowie Benutzerschnittstellen angeschlossen werden können. Für das SMGW sind folgende externe Schnittstellen zwingend vorgeschrieben: IF_GW_CON, die Schnittstelle für den Zugriff des Letztverbrauchers auf die Messdaten; IF_GW_MTR, die Schnittstelle für die Kommunikation mit den im LMN angeschlossenen Zählern; IF_GW_SM, die Schnittstelle zum Sicherheitsmodul; IF_GW_CLS, die Schnittstelle zur Kommunikation zwischen lokalen steuerbaren Systemen und externen Marktteilnehmern; IF_GW_WAN, die Schnittstelle zur Übertragung der Messdaten an externe Marktteilnehmer; IF_GW_SRV, die Schnittstelle für Service-Techniker.

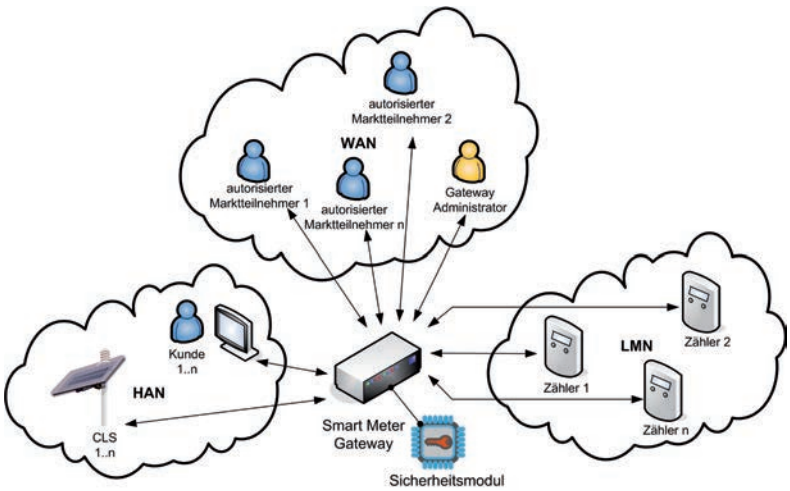

Bild 3:
Das SMGW in seiner Einsatzumgebung

Auch für den Betrieb des SMGW ist eine PKI vorgesehen [8]. Dabei wird zwischen folgenden Rollen unterschieden, für die jeweils digitale Zertifikate erstellt werden: Externe Marktteilnehmer, Gateway-Administrator, Gateway-Hersteller, SMGW. Der Gateway-Administrator ist dafür zuständig, im SMGW Regelwerke in Form von Auswertungsprofilen zu hinterlegen. Diese beschreiben, wie die von den angeschlossenen Zählern erzeugten Daten verarbeitet und letztendlich an berechtigte externe Marktteilnehmer übertragen werden. Das SMGW kann außerdem als Proxy-Server für steuerbare lokale Systeme dienen, die so sichere Kommunikationskanäle zu externen Marktteilnehmern aufbauen können.

Das SMGW soll im Wesentlichen den sicheren Zugriff von externen Marktteilnehmern auf die von intelligenten Zählern generierten Daten ermöglichen, wobei seine Auswertungs- und Kommunikationsprofile im Sinne der Datensparsamkeit individuell nur die Daten zur Verfügung stellen, die tatsächlich gebraucht werden. Durch die Vermittlung verschlüsselter Daten über den SMGW-Administrator ist es sogar möglich, die Daten zu pseudonymisieren, sodass sie nicht auf den Letztverbraucher zurückführbar sind. Wie auch bei den mobilen OBM-Zählern werden die Authentizität und die Integrität der Daten durch digitale Signaturen gewährleistet.

Vergleich der Konzepte

Das SMGW, wie es im Schutzprofil des BSI spezifiziert ist, und das Steuermodul der mobilen OBM-Zähler haben viele Gemeinsamkeiten. Beide verwenden ein Sicherheitsmodul, um die Messdaten zur Kommunikation kryptographisch zu sichern und die Kommunikation der gesicherten Messdaten an zugriffsberechtigte Externe vorzusehen. Das SMGW ist einerseits in seiner Anwendung allgemeiner und flexibler spezifiziert, ist andererseits aber erkennbar für die feste Installation innerhalb eines Haushalts/Gebäudes vorgesehen. Elektrofahrzeuge erscheinen lediglich als ein mögliches steuerbares lokales System. Der Anwendungsfall des mobilen Zählens wie im OBM-Konzept ist in der Spezifikation des SMGW nicht abzubilden. Dies zeigt sich bereits in einer der im Schutzprofil beschriebenen Annahmen: „It is assumed that the TOE is installed in a non-public environment within the premises of the consumer which provides a basic level of physical protection. This protection covers the TOE, the Meter(s) that the TOE communicates with and the communication channel between the TOE and its Security Module."

Für die Verwendung eines intelligenten Ladekabels im öffentlichen Raum sollte dieses mit einem wirksamen physikalischen Schutz ausgestattet

sein, der Manipulation und Datenzugriff ohne Zerstörung des Gerätes weitestgehend ausschließt. Außerdem ist für den Anwendungsfall des mobilen Zählens die Kennung der Systemsteckdose ein fundamentaler Bestandteil des Ladevorgangsdatensatzes. Das SMGW ist zur festen Installation vorgesehen und weder die spezifizierten Schnittstellen noch die in der PKI abgebildeten Rollen ermöglichen es, einen Ladepunkt wie die OBM-Systemsteckdose zu authentifizieren. Darüber hinaus ist auch der Prozess der Autorisierung eines Ladevorgangs nicht ohne Weiteres auf die für das SMGW beschriebenen Schnittstellen abzubilden.

Das Anwendungsszenario der mobilen OBM-Zähler ist im Vergleich zu dem des SMGW wesentlich spezifischer. Deshalb ergeben einige der Schnittstellen, die für das SMGW zwingend vorgeschrieben sind, für die mobilen OBM-Zähler keinen Sinn. Dies gilt insbesondere für die Schnittstelle zum Anschluss weiterer Messgeräte und die Proxy-Schnittstelle für lokale steuerbare Systeme. Auch der flexible Zugriff auf Messdaten durch externe Marktteilnehmer ist im OBM-Konzept nicht vorgesehen. Ein mobiler Zähler kommuniziert zur Übertragung der Messdaten ausschließlich mit seiner Leitstelle. Dabei wird die Kommunikationsverbindung immer vom mobilen Zähler aufgebaut. Für das SMGW gilt ebenfalls, dass die Kommunikationsverbindung in der Regel vom Gateway aufgebaut wird. Es ist jedoch zusätzlich der sogenannte Wake-Up-Service vorgesehen, der es dem Gateway-Administrator ermöglicht, den Aufbau einer Kommunikationsverbindung anzustoßen.

Das OBM-Konzept hat sich zum Ziel gesetzt, Elektrofahrzeuge als steuerbare Verbraucher und perspektivisch als Regelenergiespeicher in intelligente Netze zu integrieren. Zu diesem Zweck wurden im Kommunikationsprotokoll zwischen mobilem Zähler und Leitstelle Steuerungsbefehle definiert, die es ermöglichen, die Ladeleistung zu drosseln bzw. einen Ladevorgang temporär zu unterbrechen. Um Anreize für Letztverbraucher zu schaffen, ihre Elektrofahrzeuge solcherart regeln zu lassen, müssen Steuerungsvorgänge in der Tarifierung berücksichtigt werden. Dementsprechend müssen sie vom mobilen Zähler quittiert und wie die Messdaten auch digital signiert werden. Vergleichbar dazu ist im SMGW mit dem informativen Tarif-Anwendungsfall 11 eine Tarifierung basierend auf der Steuerung von unterbrechbaren Verbrauchseinrichtungen und Erzeugungsanlagen vorgesehen. Dabei werden jedoch lediglich von angeschlossenen Zählern generierte Messwerte mit Zeitstempeln und Ereignissen annotiert. Es ist nicht vorgesehen, Steuerungsbefehle direkt durch das SMGW zu bestätigen.

Die Spezifikation des SMGW legt großen Wert auf die Vertraulichkeit der Messdaten und Datensparsamkeit. Das ist begründet in der Tatsache, dass ein hochaufgelöster Lastgang für die typische Anwendung in einem Haushalt nachgewiesenermaßen auf Verhaltensweisen und Gewohnheiten der Bewohner, bis hin zur Wahl des Fernsehprogramms [9], schließen lässt. Dieser Aspekt spielt im Anwendungsfall der OBM-Zähler eine weniger ausgeprägte Rolle. Pro Ladevorgang ist, um die Abrechnung zu ermöglichen, mindestens die konsumierte Energiemenge zu kommunizieren. Der detailliertere Lastgang dient als Grundlage für komplexere Tarifmodelle basierend auf Zeit, Energiemenge oder Leistung. Aber auch in diesem Fall sind Datenschutzaspekte von geringerer Bedeutung, da der Lastgang lediglich ein Abbild der Ladesteuerung des jeweiligen Fahrzeugs darstellt. Im Zusammenhang mit Ladevorgängen eines Elektromobils stellt sich mit Bezug auf Datenschutzaspekte eher die Frage, ob es möglich ist, Bewegungsprofile von Letztverbrauchern anzulegen. Bei der Abrechnung der Ladevorgänge ist dies tatsächlich eine Herausforderung. Im Rahmen des SecMobil-Projekts wurde für konventionelle Ladesäulen mit integrierter Zähltechnik kürzlich ein komplexes Verfahren konzipiert, das mithilfe der Pseudonym-Funktion des elektronischen Personalausweises ein Anlegen von Bewegungsprofilen verhindert [10]. Im OBM-Konzept muss es jedem Ladepunktanbieter möglich sein, im Zweifelsfall nachzuvollziehen, welcher geeichte Zähler für einen bestimmten Ladevorgang verwendet wurde. Die Kennung dieses Zählers ist effektiv ein Pseudonym für den Letztverbraucher. Um das Anlegen von Gewohnheitsprofilen (Zähler A lädt immer montags zwischen 10 h und 11 h an einem meiner Ladepunkte) zu erschweren, könnte die Auflistung der Zählerkennungen in den regelmäßigen Rechnungen fehlen. Nur im Zweifelsfall, wenn eine Rechnung angemahnt wird, müssen die Original-Messdaten, die die Zählerkennung zwingend enthalten müssen, zur Verfügung stehen und zur Klärung herangezogen werden. Für in diesem Zusammenhang vergleichbare Systeme, wie z. B. das eTicket-System des Verbands Deutscher Verkehrsunternehmen (VDV) [11], ein einheitliches Ticketsystem auf elektronischer Basis, sind die personalisierten Chipkarten jederzeit im Gesamtsystem zu verfolgen. Vor diesem Hintergrund erscheint das OBM-System unkritisch.

Zusammenfassung

Auf technischer Ebene sind die Sicherheitsfunktionen des SMGW und die der mobilen OBM-Zähler durchaus vergleichbar und zeigen viele Gemeinsamkeiten. Beide Systeme verwenden u. a. ähnliche Methoden, um Daten kryptographisch abzusichern. So wird die Vertrauenswürdigkeit und die Vertraulichkeit der Messdaten gewährleistet. Das

SMGW ist jedoch klar für den Anwendungsfall des Smart Metering im Haushalt des Letztverbrauchers ausgelegt, wohingegen das OBM-Konzept auch für den öffentlichen Raum konzipiert wurde. Der spezielle Anwendungsfall des mobilen Zählens beim Laden von Elektrofahrzeugen lässt sich also auf diese Architektur nicht direkt abbilden. Einerseits fehlen in der Spezifikation des SMGW für das OBM-System fundamental wichtige Funktionen, wie die authentifizierte Kommunikation mit einem Ladepunkt und die Autorisierung des Ladevorgangs. Andererseits schreibt das SMGW eine Reihe von Schnittstellen zwingend vor, die durch die für das SMGW vorgesehenen Anwendungsfälle vorgegeben sind, die für die mobilen OBM-Zähler hingegen nicht benötigt werden.

Literatur

[1] Baustein für die Energiewende: 7 Eckpunkte für das „Verordnungspaket Intelligente Netze“, BMWi

[2] http://www.projekt-obm.net (letzter Aufruf: 26. Oktober 2015)

[3] PTB-Anforderungen 50.7 (PTB-A 50.7) Elektronische und softwaregesteuerte Messgeräte und Zusatzeinrichtungen für Elektrizität, Gas, Wasser und Wärme, 4/2002

[4] Berg, A., Zisky, N., On-Board Metering: Mobiles Messen von Tankstrom in Elektrofahrzeugen – sicher, eichgültig und abrechnungsrelevant, in Kahmann/Zayer: Elektrizitätsmesstechnik, 2012, ISBN 978-3-8022-1058-7, EW Medien und Kongresse GmbH, Frankfurt am Main, S. 283–300

[5] Das SELMA-Projekt, Konzepte, Modelle, Verfahren, Norbert Zisky (Hrsg.), PTB-Bericht IT-12

[6] Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, BSI

[7] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2012, Version 3.1, Revision 4

[8] Technische Richtlinie BSI TR-03109-4, Smart Metering PKI – Public Key Infrastruktur für Smart Meter Gateways, BSI

[9] Identifikation von Videoinhalten über granulare Stromverbrauchsdaten, Ulrich Greveler, Benjamin Justus, Dennis Löhr, Labor für IT-Sicherheit, Fachhochschule Münster

[10] http://rubin.rub.de/de/ich-weiss-wo-du-letzten-sommer-geladen-hast (letzter Aufruf: 25. September 2015)

[11] http://www.eticket-deutschland.de/kurzbeschreibung----eticket-deutschland-v-2-0-2014-10-06.pdfx (letzter Aufruf: 25. September 2015)