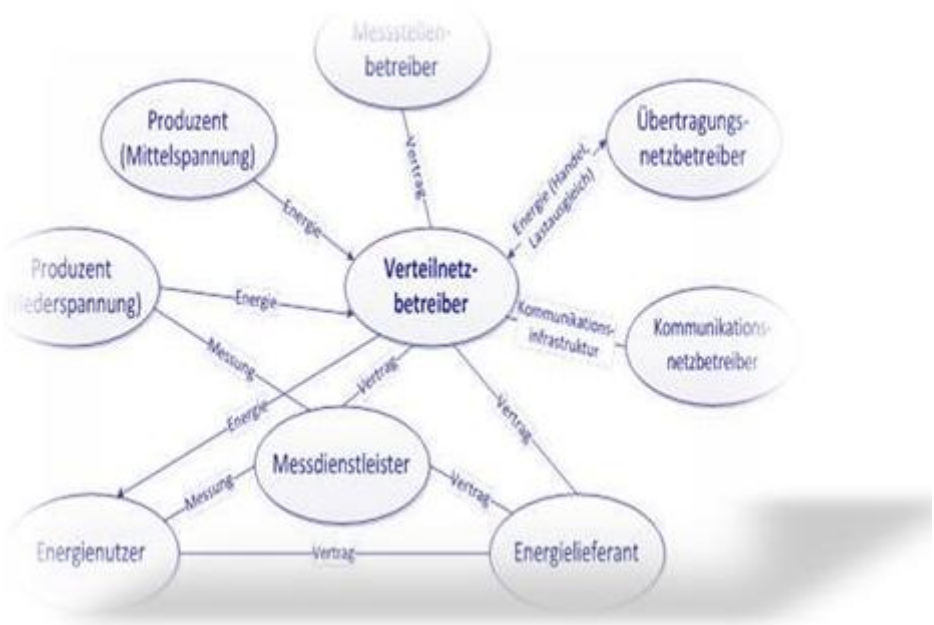
Alcatel-Lucent Stiftung für Kommunikations-forschung

Sicherheit im Smart Grid

Sicherheitsarchitekturen für die Domänen Privatkunde und Verteilnetz unter Berücksichtigung der Elektromobilität

Claudia Eckert, Christoph Krauß



Alcatel-Lucent Stiftung

Sicherheit im Smart Grid:

Sicherheitsarchitekturen für die Domänen Privatkunde und Verteilnetz unter Berücksichtigung der Elektromobilität

Inhalt

Impressum

Stiftungsreihe 96

Redaktion
Dr. Dieter Klumpp
Dr. Erich Zielinski
Petra Bonnet M.A.

Druck der Broschüre
DCC Kästl GmbH & Co. KG

Die Alcatel-Lucent Stiftung für Kommunikationsforschung ist eine nichtrechtsfähige Stiftung in der treuhänderischen Verwaltung des Stifterverbandes für die Deutsche Wissenschaft.

Angaben nach § 5 TMD/
§ 55 RfStv

Stifterverband für die Deutsche Wissenschaft e.V.
Barkhovenallee 1
45239 Essen
Telefon: (02 01) 8401-0
Telefax: (02 01) 8401-301
E-Mail: mail@stifterverband.de

Geschäftsführer:
Prof. Dr. Andreas Schlüter
(Generalsekretär)

ISSN 0932-156x

Sicherheit im Smart Grid:

Sicherheitsarchitekturen für die Domänen Privatkunde und Verteilnetz unter Berücksichtigung der Elektromobilität

Claudia Eckert, Christoph Krauß

Zusammenfassung

Dieser Artikel untersucht die Sicherheitsanforderungen der Domänen Privatkunde und Verteilnetz unter Berücksichtigung der Elektromobilität als relevante Teilsysteme von Smart Grids. Hierzu werden für jede Domäne relevante Anwendungsfälle vorgestellt und die relevanten Stakeholder in den jeweiligen Domänen werden als Rollen mit Rechten und Pflichten beschrieben. Ausgehend von den Rollen und den identifizierten Anwendungsfällen werden Rollen- und domänenspezifische Sicherheitsanforderungen abgeleitet. Diese Aufteilung erleichtert eine Konkretisierung und Umsetzung erheblich. Der Artikel entwickelt sodann für jede Domäne eine so genannte Referenzarchitektur und erläutert an diesen Architekturen mögliche konkrete Umsetzungen der Anforderungen.

Der Artikel hat zum Ziel, einen ersten Schritt in Richtung auf die Erstellung eines umfassenden Sicherheitskonzepts zu gehen, und eine mögliche systematische Vorgehensweise hierfür exemplarisch zu verdeutlichen.

1 Einleitung

Energie ist eine Grundlage des heutigen Lebens und der Bedarf steigt durch die fortschreitende Industrialisierung immer weiter an. Im Moment befindet sich die Energiewirtschaft in einem starken Umbruch. Katastrophen wie in Fukushima, die immer knapper werdenden fossilen Rohstoffe und der Klimawandel erfordern zunehmend die Einbindung dezentral erzeugter, erneuerbarer Energien wie Wind-, Sonne- oder Wasserkraft in die Prozesse der Energieerzeugung, -speicherung und -verteilung.

In der Energiewirtschaft ist die Versorgungssicherheit von zentraler Bedeutung. Diese muss auch bei einer verteilten Energieerzeugung und dem vermehrten Einsatz erneuerbarer Energien gewährleistet sein. Fluktuationen bei der Energieerzeugung und Lastspitzen müssen durch intelligente Steuerungen ausgeglichen bzw. proaktiv vermieden werden. Energie muss zwischengespeichert oder bedarfsgerecht transportiert werden, um eine effiziente Energienutzung zu erreichen. Erforderlich ist eine sehr viel detailliertere Erfassung der Daten zu Energieverbrauch, Nachfrage und verfügbarer Energie als bislang üblich. Diese Daten müssen sicher zwischen den Marktteilnehmern ausgetauscht werden, um in dezentralen Umgebungen möglichst proaktiv, zumindest aber reaktiv steuernd und kontrollierend eingreifen zu können. Hierfür wird eine Informations- und Telekommunikations- (IKT) Infrastruktur zur dynamischen Steuerung benötigt. Die Kombination der Energietechnik mit der IKT wird auch als Energieinformationsnetz oder im Englischen als Smart Grid bezeichnet.

Smart Grids sind kritische Infrastrukturen, deren Ausfall oder partielle Störung gravierende gesellschaftliche und wirtschaftliche Auswirkungen haben würde. Wie der Stuxnet Wurm [1] Mitte 2010 gezeigt hat, stellen erfolgreiche Angriffe auf Automatisierungstechnologien wie Supervisory Control and Data Acquisition (SCADA) Systeme eine große Bedrohung dar. Solche SCADA Systeme sind auch in der Leittechnik und der Prozesssteuerung von Energienetzen sehr viel im Einsatz. Um Smart Grids angemessen vor Störungen und Missbrauch zu schützen, ist ein sicheres Energieinformationsnetz unerlässlich. Das Energieinformationsnetz kann dabei sowohl Angriffsziel als auch Mittel zur Durchführung eines Angriffs, also eine Art Tatwaffe sein. Ist das Energieinformationsnetz selbst Ziel von Angriffen, so kann es zu Störungen und Manipulationen bei der Datenübertragung kommen, so dass beispielsweise falsche Steuerdaten oder veraltete Steuerdaten eingespeist werden können und es zu einer Störung der Betriebs- bis hin zur Versorgungssicherheit kommen kann. Als Tatwaffe kann das Netz verwendet werden, um unter falscher Identität kriminelle Angriffe auf Versorger durchzuführen oder z.B. physische Anlagen zu schädigen.

In einem Smart Grid agieren unterschiedliche Akteure mit sehr unterschiedlichen Aufgaben und Sicherheitsanforderungen, die zum Teil auch konträr sind. Aus Kundensicht ergeben sich beispielsweise Fragestellungen in Bezug auf dessen Privatsphäre, wenn sich aus den erhobenen Energieverbrauchsdaten sein Nutzungsverhalten ablesen lässt [8, 13]. Demgegenüber basieren neuere Geschäftsmodelle von Anbietern von Energie-Mehrwertdiensten häufig darauf, möglichst exakte Informationen über das Verbrauchsverhalten von Nutzern zu besitzen, um zugeschnittene Services anbieten zu können. Dies könnte damit auch für den Nutzer von Vorteil sein, wenn er solche personalisierten Dienstleistungen wünscht. Erforderlich sind somit Sicherheitsarchitekturen, die einen Interessensausgleich zwischen den unterschiedlichen Marktteilnehmern und deren Individualinteressen ermöglichen. Eine umfassende Einführung in die Thematik der IT-Sicherheit ist u.a. in [4] zu finden.

Sicherheit muss somit von Beginn an („Secure by Design“) und auch während der Laufzeit („Secure during Operation“) elementarer Bestandteil von Smart Grids sein [6, 5]. Unter dem Stichwort Privacy by Design und Secure by Design wird häufig jedoch eine sehr starke Reglementierung der Systeme verstanden. Das heißt, dass Systeme sehr stark abgeschottete sind, eine Datenweitergabe sehr restriktiv unterbunden wird oder aber auch dass dem Nutzer wenig Einfluss- und Eingriffsmöglichkeiten gewährt werden. In diesem Artikel plädieren wir für den Aufbau von Sicherheitsarchitekturen, die zwar Sicherheitsbasismechanismen und Kontrolldienste qua Design integrieren, die aber auch über eine klare Trennung von Mechanismus und Regelwerk es ermöglichen, diese Mechanismen flexibel, angepasst und anpassbar zu nutzen, um unterschiedliche Sicherheitsanforderungen zu erfüllen. Dies ist aus unserer Sicht für das Smart Grid und generell für zukünftige IKT-basierte Anwendungen, wie Smart Cities, Smart Mobility oder auch Smart Health unerlässlich.

Der Artikel ist wie folgt strukturiert. Kapitel 2 motiviert die Domänen-bezogene Sicht, die es ermöglicht, die unterschiedlichen Sichten und Bedürfnisse von Teilnehmern des Energiemarktes systematisch zu erfassen und damit die Komplexität der Aufgabenstellung zu reduzieren. In Kapitel 3 wird zunächst detailliert die Domäne Privatkunde betrachtet.

Hierzu werden zunächst Grundlagen und die relevanten Anwendungsfälle vorgestellt, Sicherheitsanforderungen abgeleitet und abschließend eine mögliche Sicherheitsarchitektur beschrieben. Der Schwerpunkt liegt auf technischen Fragestellungen; betriebswirtschaftliche Fragestellungen wie Bilanzkreismanagement sind nicht Gegenstand des Artikels. Analog zur Domäne Privatkunde wird in Kapitel 4 die Domäne Verteilnetz behandelt.

Dazu werden zunächst Grundlagen und Anwendungsfälle zum Verteilnetz beschrieben und anschließend Sicherheitsanforderungen und eine mögliche Sicherheitsarchitektur erarbeitet. Kapitel 5 geht dann noch einmal dediziert auf den Aspekt der Einbindung der Elektromobilität ein und erläutert eine mögliche Sicherheitsarchitektur. Der Artikel wird mit einer Zusammenfassung und einem Ausblick in Kapitel 6 abgeschlossen.

2 Domänen und Rollen im Smart Grid

Smart Grids sind in Bereiche aufgeteilt, in denen jeweils spezifische technische und ökonomische Geschäftsprozesse und Anwendungsfälle ablaufen. Solche Bereiche werden als **Domänen** bezeichnet (vgl Abbildung 1).

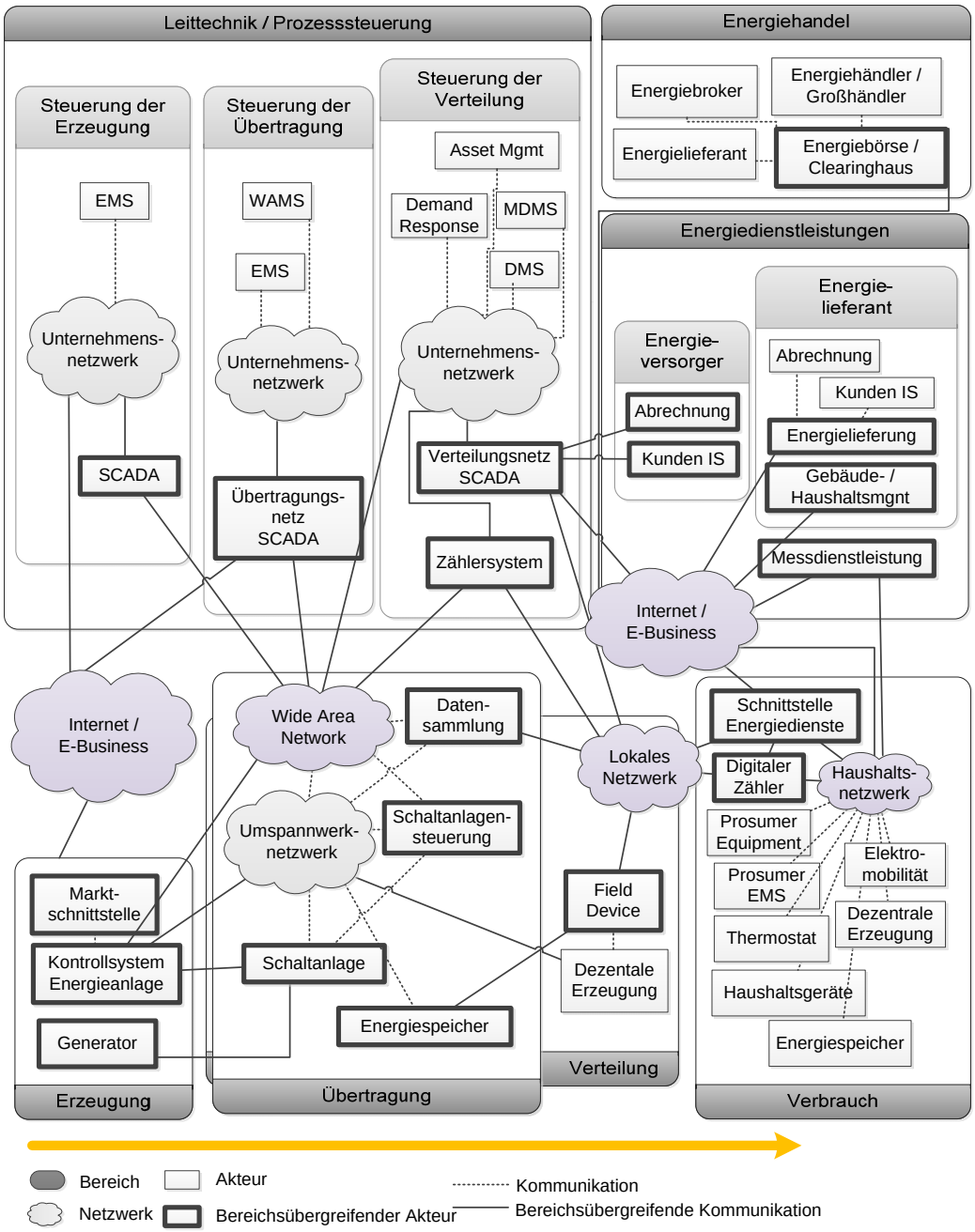


Abbildung 1: Konzeptuelles Modell eines Smart Grid
(Quelle der Graphik: P. Beenken, Schutz sicherheitsrelevanter Informationen in verteilten Energieinformationssystemen, Dissertationsschrift, 2010, Universität Oldenburg)

Unterschieden werden in der Regel die Domänen Erzeugung, Übertragung, Verteilung, Kunde, Märkte, Betrieb und Service [3]. Diese lassen sich noch in weitere Subdomänen unterteilen. Beispielsweise kann die Domäne „Kunde“ in Privat- / Haushaltskunde, Gewerbekunde oder Industriekunde untergliedert werden.

In den Domänen bzw. Sub-Domänen sind verschiedene Marktteilnehmer aktiv, die unterschiedliche Aufgaben und Verpflichtungen haben. Man spricht hierbei von **Rollen**.

Unterschieden werden die folgenden Rollen [3]. Direkt an Energieerzeugung, -verteilung und -verbrauch sind die Rollen *Produzent*, *Energienutzer*, *Übertragungsnetzbetreiber (TSO)* und *Verteilnetzbetreiber (DSO)* beteiligt. Die Rollen *Energielieferant, Bilanzkreisverantwortlicher, Bilanzkreiskoordinator, Energiehändler* und *Energiebörse (EEX)* beschäftigen sich mit dem Energie-Handel bzw. der Abrechnung von verbrauchten bzw. eingespeisten Energiemengen. Weitere relevante Rollen sind *Kommunikationsnetzbetreiber, Messstellenbetreiber (MSB), Messdienstleister (MDL), Energiemarktplatzbetreiber,* weitere *Energiedienstleister, Hersteller* (Gerätehersteller, Netzanlagenhersteller, Elektrofahrzeughersteller etc.).

Mit jeder dieser Rollen sind spezifische Sicherheitsanforderungen, sowie weitere, meist ökonomische Anforderungen verbunden. So möchte der Energienutzer beispielsweise seine Privatsphäre gewahrt haben, und der Energielieferant ist vordringlich an einer möglichst kostengünstigen Gesamtlösung interessiert. Dazu könnte auch gehören, dass der Energielieferant seinem Kunden zugeschnittene Mehrwertdienste anbieten möchte, wofür er ggf. detaillierte Informationen über das Nutzungsverhalten des Kunden benötigt. Dies könnte im Widerspruch zu den Wünschen des Kunden stehen, dass seine Privatsphäre geschützt wird. Die Umsetzung der oftmals entgegengesetzten (Sicherheits-) Anforderungen stellt eine große Herausforderung bei der Entwicklung von Sicherheitsarchitekturen in Smart Grids dar.

Um die Komplexität der Aufgabenstellung zu reduzieren, schlagen wir vor, die einzelnen Domänen differenziert zu betrachten und für jede Domäne generische Muster für Sicherheitsarchitekturen zu entwerfen, so dass auf dieser Basis systematische Handlungsempfehlungen für die verschiedenen Marktteilnehmer eines Smart Grid abgeleitet werden können. In diesem Artikel werden für die Domänen Privatkunde und Verteilnetz sowie die Elektromobilität, Vorschläge für derartige Architektur-Blaupausen vorgestellt.

Insbesondere in den Domänen *Privatkunde* (als Sub-Domäne der Domäne Kunde) und *Verteilnetz* wird ein großer Wandel vollzogen werden. Dies ist darin begründet, dass in Zukunft Energie vermehrt durch erneuerbare Energien und verteilt durch viele Produzenten erzeugt wird. Um mit der dezentralen Verarbeitung und den zu erwartenden höheren Schwankungen umgehen zu können und eine kontinuierliche Stromversorgung zu garantieren, ist ein vermehrter Einsatz von IKT notwendig. Es müssen Messungen von Angebot und Nachfrage von Energie durchgeführt werden und entsprechende Steuerungen durchgeführt werden. Auch die vermehrte Verbreitung der Elektromobilität spielt hierbei eine nicht unwesentliche Rolle, so dass wir in dem vorliegenden Artikel auch die Einbindung der *Elektromobilität* etwas genauer beleuchten werden. So werden Elektrofahrzeuge zu Hause beim Privatkunden oder an (halb-)öffentlichen Ladesäulen, die an Verteilnetze angeschlossen sind, geladen

oder sie können potentiell bei Nichtgebrauch als Energiespeicher genutzt werden, um Energie lokal für einen schnellen Abruf in Hauptbelastungszeiten zwischen zu speichern.

Aufgrund der besonderen Bedeutung der genannten Domänen für die Smart Grids, konzentriert sich der vorliegende Artikel deshalb auf die Erarbeitung von Architekturvorschlägen für die Domänen *Privatkunde* und V*erteilnetz* unter der Berücksichtigung der Einbindung der *Elektromobilität* in Smart Grids. Die entwickelten Sicherheitsarchitekturen sind bewusst generisch gestaltet, um nicht bereits in diesem Schritt durch Konkretisierungsannahmen, Vorentscheidungen für eine konkrete Umsetzung zu treffen. Das Ziel ist es, wichtige Rahmendbedingungen aufzuzeigen und Lösungsvorschläge für generische Anforderungen vorzustellen, jedoch noch genügend Flexibilität für eine Umsetzung bzw. Konkretisierung der Anforderungen beizubehalten.

Für die Domänen Privatkunde und Verteilnetz sowie für die Elektromobilität werden zunächst sicherheitsrelevante Anwendungsfälle (Use Cases) identifiziert. Anschließend werden für die an den Use Cases beteiligten Rollen die sich ergebenden Sicherheitsanforderungen abgeleitet, welche durch die Sicherheitsarchitektur erfüllt werden sollen. Als Basis für die generischen Sicherheitsarchitekturen werden Referenzmodelle der zugrundeliegenden Vernetzungstopologien entwickelt, um an definierten Referenzpunkten die wichtigsten Sicherheitsmechanismen und deren Eigenschaften zu spezifizieren. Die Modelle sind so konzipiert, dass sich die Referenzpunkte mit ihren Sicherheitsmechanismen leicht auf andere Topologien übertragen lassen können, falls zukünftige Netztopologien anderes aussehen sollten als in den vorgeschlagenen Referenzmodellen.

3 Privatkunde

Die Subdomäne Privatkunde[1] der Domäne Kunde stellt aufgrund der vielen Hausanschlüsse eine wesentliche Komponente von Smart Grids dar. Smart Meter sind eine der zentralen technischen Komponenten der Domäne, die direkt beim Endkunden installiert werden. Die Smart Meter ermöglichen eine zeitgenaue Verbrauchsdatenerfassung. In diesem Kapitel wird zunächst ein kurzer Überblick über diese Domäne gegeben, indem die beteiligten Rollen, die verschiedenen Arten von ausgetauschten Daten und eine typische Netztopologie kurz beschrieben werden. Anschließend werden Anwendungsfälle, die sich ergebenden Sicherheitsanforderungen der einzelnen Rollen und eine Sicherheitsarchitektur beschrieben.

3.1 Grundlagen

In der Domäne Privatkunde sind die folgenden Rollen relevant und können auch gleichzeitig in ihr aktiv sein: Energienutzer, Verteilnetzbetreiber, Energielieferant, Kommunikationsnetzbetreiber, Messstellenbetreiber, Messdienstleister, Hersteller und ggf. weitere Energiedienstleister. Abbildung 2 stellt die Rollen und deren Beziehungen untereinander

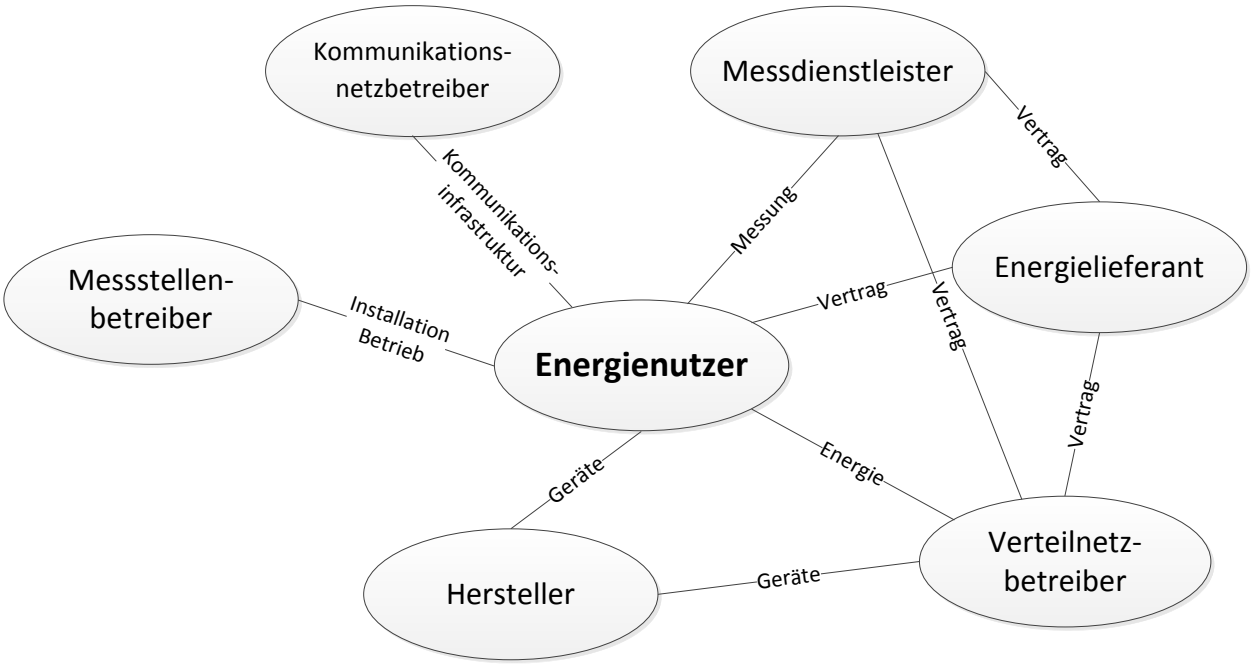


Abbildung 2: Rollen in der Domäne Privatkunde und deren Beziehungen

vergröbert dar. Der Fokus liegt dabei auf dem Energienutzer, da dieser im Mittelpunkt der Domäne Privatkunde steht. Nicht direkt relevante Beziehungen werden zur besseren Übersicht halber nicht dargestellt.

[1] Im Folgenden sprechen wir als Vereinfachung auch häufig von der Domäne Privatkunde, auch wenn wir sie als eine Subdomäne der übergeordneten Domäne Kunde betrachten. Diese Unterscheidung ist aber für die weiteren Ausführungen unerheblich, so dass wir darauf verzichten.

Der Privatkunde steht in der Rolle *Energienutzer* im Mittelpunkt dieser Domäne. In seinem häuslichen Umfeld sind Smart Meter und Gateways installiert. Diese Installation zählt zu dem Aufgabenbereich der Rolle *Messstellenbetreiber,* die auch den Betrieb gewährleisten und deren Rollenmitglieder, also die Mitarbeiter des jeweiligen Messstellenbetreibers, Wartungsarbeiten an den Smart Metern und Gateways durchführen. Im Rahmen der Aufgabenerledigung in der Rolle Messstellenbetreiber können beispielsweise für Wartungszwecke mittels Fernzugriff regelmäßig System-Updates auf die digitalen Zähler, die Smart Meter, in den Haushalten aufgespielt werden, so dass eine zeit- und kostenaufwändige Vor-Ort-Wartung durch einen Servicetechniker weitestgehend entfallen kann. Die durch die Smart Meter erfassten Messwerte werden über ein Gateway an eine in der Rolle *Messdienstleister* agierende Instanz gesendet, die diese einer in der Rolle *Energielieferanten* agierenden Instanz zu Abrechnungszwecken zur Verfügung stellt. Zwischen dem Energielieferanten und dem Energienutzer besteht ein Vertragsverhältnis über den Bezug von Energie. Hierbei tritt der Energielieferant als eine Art Wiederverkäufer auf, so dass auch ein Vertragsverhältnis mit einem *Verteilnetzbetreiber* besteht, welcher die Energie an den Energienutzer liefert. Alternativ könnte der Privatkunde auch direkt einen Vertrag mit einem Verteilnetzbetreiber abschließen, z.B. einem Stadtwerk, von dem er die Energie bezieht. Auch ist denkbar, dass der Messdienstleister dem Verteilnetzbetreiber direkt Messwerte zur Verfügung stellt, die dieser für interne Zwecke verwendet. Die Kommunikation aller Rollen untereinander wird durch einen oder mehrere *Kommunikationsnetzbetreiber* realisiert, die entsprechende Kommunikationsinfrastrukturen bereitstellen. Relevante Mitglieder der Rolle *Hersteller* sind beispielsweise Hersteller von Smart Metern oder von Geräten zur Heimautomatisierung.

In Zukunft könnte man sich auch vorstellen, dass auch die Rollen *Energiehändler* und *Energiemarktplatzbetreiber* in dieser Domäne aktiv werden, wenn Kunden als so genannte Prosumer ihre erzeugte Energie selbst auf dem Markt anbieten und nicht wie bisher feste Verträge mit einem Verteilnetzbetreiber haben. Ein Prosumer ist ein Kunde (consumer), der auch selbst Strom z.B. mittels einer Photovoltaik-Anlage erzeugt und ins Stromnetz einspeist (producer).

Eine mögliche Netztopologie der Domäne Privathaushalt ist in Abbildung 3 dargestellt. Die linke Seite stellt einen Privatkunden in den Rollen Energienutzer und Energielieferant, also als Prosumer, dar.

Beim Privatkunden sind Energieverbraucher (z.B. eine Waschmaschine), Energieerzeuger (z.B. die o.g. Photovoltaik-Anlage), Speicher (nicht dargestellt), Smart Meter, ein Gateway und ein internetfähiges Gerät, wie beispielsweise ein PC, installiert. Der Energieversorger repräsentiert zur Vereinfachung die Rollen Energielieferant, Verteilnetzbetreiber, Messstellenbetreiber und Messdienstleister. Mit dem Energieversorger hat der Privatkunde einen Vertrag und bezieht über das Stromnetz Energie. Die Messwerte über die verbrauchte und erzeugte Energie werden durch Smart Meter erfasst, an das Gateway gesendet und von dort zum Energieversorger weitergeleitet. In einem Mehrfamilienhaus kann beispielsweise ein einzelnes Gateway die Daten vieler Smart Meter bündeln und weiterleiten [11]. Alternativ können beispielsweise in einem Einfamilienhaus auch Smart Meter direkt in das Gateway integriert sein

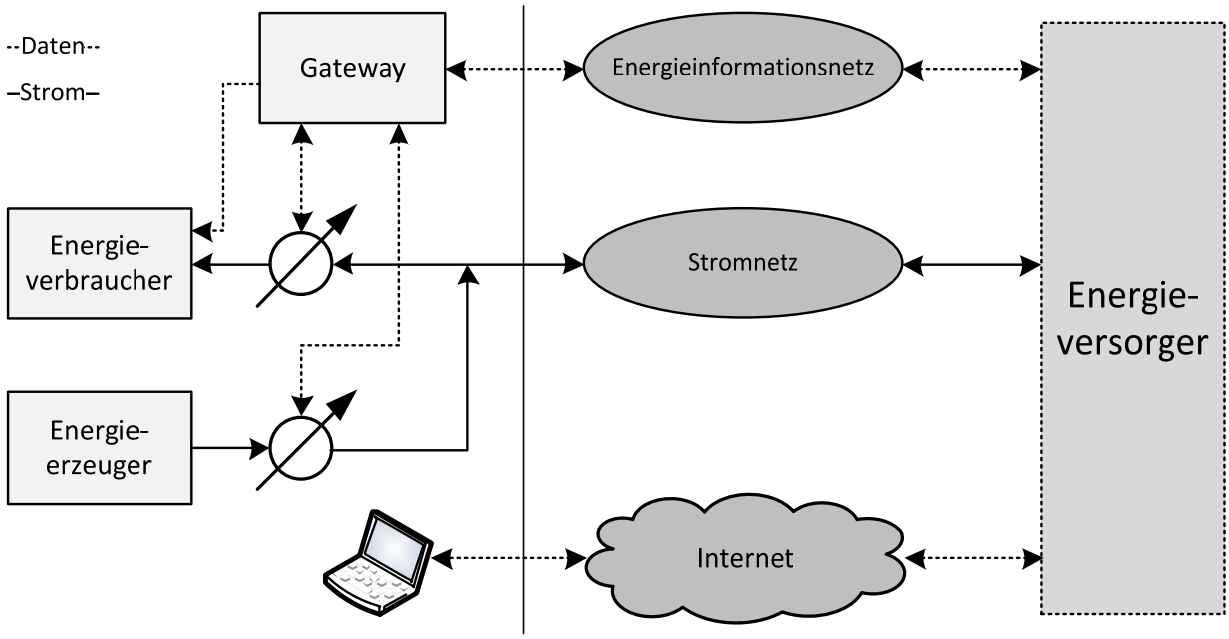


Abbildung 3: Netztopologie der Domäne Privathaushalt

[2]. Das dargestellte Gateway kann neben den Funktionalitäten eines Smart Meter Gateways [2] ggf. auch Funktionalitäten eines Energy Management Gateways zur Heimautomatisierung bereitstellen.

Neben Stromzählern können auch weitere Zähler, wie Gas- oder Wasser-Zähler, an ein Multi-Utility-Gateway angeschlossen sein, welches die Messwerte von Strom, Gas und Wasser sammelt und weiterleitet. Gas- und Wasserzähler werden nach heutigem Stand der Diskussion größtenteils batteriebetrieben sein und über eine Funkschnittstelle wie beispielsweise Wireless M-Bus mit solch einem Gateway kommunizieren. Die Ausweitung des SmartGrid Ansatzes auf die so genannten *Hybridnetze* wird derzeit intensiv diskutiert, da erhebliche Synergien zu erwarten sind, wenn man die verschiedenen Versorgungsnetze (Gas, Wasser etc.) gemeinsam betrachtet. Da diese Diskussion noch nicht weit gediehen ist, fokussiert der vorliegende Artikel ausschließlich das Smart Grid im bekannten Umfang.

Eine weitere Ausweitung der Betrachtung auf die gesamte Heimautomatisierung und den Möglichkeiten, die sich durch die flächendeckende Digitalisierung der Haushalte über Smart Meter u.a. für den Bereich der ambulanten Pflege ergeben könnten (Ambient Assisted Living), wird im Folgenden jedoch nicht weiter verfolgt. Offensichtlich ergeben sich aus der IKT-Anbindung von Haushalten mittels unterschiedlicher Sensoren, die Daten über Profile der Nutzer übertragen können, eine Vielzahl interessanter Anwendungsfälle, insbesondere im eHealth Bereich, die ganz erhebliche zusätzliche Sicherheitsanforderungen mit sich bringen. Deren Betrachtung würde den Rahmen des vorliegenden Artikels jedoch deutlich sprengen.

In Zukunft muss der Verbrauch von Energie noch viel stärker an das aktuelle Angebot an Energie angepasst werden, da sich durch die verteilte Erzeugung aus erneuerbaren Ener-

gien stärkere Schwankungen ergeben. Hierzu ist ein Ansatz Energieverbraucher, deren Einsatzzeiten in gewissen Grenzen variabel sind, entsprechend der verfügbaren Energie fernzusteuern. Derzeit wird dies mit Hilfe der Rundsteuertechnik schon praktiziert, um beispielsweise Nachtspeicherheizungen nachts, wenn viel Strom verfügbar ist, aufzuheizen und tagsüber wird die Wärme abgegeben. In Smart Grids wird es solche Steuerungen ebenfalls gegeben, wobei man hier zwischen direkter und indirekter, anreizbasierter Steuerung unterscheidet [3]. Die direkte Steuerung per Fernzugriff ist eher bei größeren Anlagen im industriellen oder gewerblichen Umfeld zu erwarten. Beispielsweise können bei einem Überangebot von Windenergie, Kühlhäuser stark herunter gekühlt werden, so dass diese bei Engpässen für eine Zeit lang ohne Energie auskommen [15]. Die indirekte Steuerung wird eher beim Privatkunden zu erwarten sein. Hierzu werden beispielsweise dynamische Preissignale gesendet, die den Nutzer in seinem Energieverbrauch beeinflussen sollen. Beispielsweise bietet Miele Smart Grid-fähige Hausgeräte an, die automatisch gestartet werden, wenn der Strom zu günstigen Preisen verfügbar ist [20]. Ob eine direkte Steuerung beim Privatkunden ebenfalls möglich ist, wird zurzeit untersucht [3]. Die direkte Steuerung wird in Kapitel 4.2 im Anwendungsfall *Steuerung und Überwachung* diskutiert und die indirekte Steuerung in Kapitel 3.2 im Anwendungsfall *Echtzeit-Tarifierung*.

Daten, wie z.B. Messwerte oder Steuersignale, werden zwischen Gateway und Energieversorger über das Energieinformationsnetz ausgetauscht, welches von einem oder mehreren Kommunikationsnetzbetreibern betrieben wird.

Der Energieversorger sorgt dafür, dass der Energienutzer mit Strom versorgt wird, Messwerte erfasst werden und Rechnungen gestellt werden. Er empfängt aktuelle Messwert oder sendet Daten wie aktuelle Verbrauchswerte oder Preisinformationen über das Energieinformationsnetz oder über das Internet an den Energienutzer.

3.2 Anwendungsfälle

Im Folgenden wird eine repräsentative Auswahl an Anwendungsfällen (engl. Use Cases) für die Domäne Privatkunde beschrieben und relevante Schutzziele beschrieben, um daraus anschließend die Sicherheitsanforderungen der einzelnen Rollen abzuleiten. Die Anwendungsfälle basieren größtenteils auf den in [10] beschriebenen sicherheitsrelevanten Anwendungsfällen. In den Anwendungsfällen muss berücksichtigt werden, dass den Rollen auch gewisse Rechte und Pflichten zugeordnet sind, die sie erfüllen müssen. Beispielsweise sind gewisse Datenschutzanforderungen oder Protokollierungen gesetzlich vorgeschrieben.

Use Case: Messwerterfassung und -übertragung

Dieser Anwendungsfall beschreibt die Erfassung von Messwerten der verbrauchten oder ggf. eingespeisten Energie (vgl. auch Anwendungsfall *Einspeisen von Energie* in Kapitel 3.2) durch die beim Privatkunden installierten Smart Meter und die Übertragung durch das Gateway. Die Messwerte werden an den Messdienstleister gesendet. Der Messdienstleister kann dem Privatkunden die aktuellen Verbrauchsdaten, z.B. über das Internet, zur Verfügung stellen, um dem Kunden eine Verbrauchstransparenz zu ermöglichen. Zur Abrechnung stellt der Messdienstleister die Messwerte dem Energieliefe-

ranten zur Verfügung. Auch können die Messwerte dem Verteilnetzbetreiber zur Verfügung gestellt werden, die zur Netzsteuerung und -optimierung genutzt werden können.

In den Kapiteln 2.3 und 2.4 wird detailliert betrachtet in welcher Form die Messwerte den einzelnen Rollen zur Verfügung gestellt werden dürfen, um Sicherheitsanforderungen wie den Datenschutz einzuhalten. Beispielsweise sind zur Abrechnung des Energielieferanten keine sekundengenauen Messwerte nötig und für den Verteilnetzbetreiber sind auf ein Netzsegment aggregierte und anonymisierte Messwerte ausreichend.

Use Case: Fernanschaltung / Fernabschaltung

Um die Managementkosten zu reduzieren, streben die Energieversorger eine Wartung von Geräten mittels Fernzugriffen an. Anstatt durch einen Mitarbeiter vor Ort, soll die Energieversorgung unter Nutzung der installierten Smart Meter über das Energieinformationsnetz aktiviert oder aber auch deaktiviert werden können, z.B. wenn ein Mieter neu in ein Haus ein- oder auszieht. Hierzu werden entsprechende Steuernachrichten durch den Messstellenbetreiber an das Smart Meter bzw. Gateway gesendet. Es ist offensichtlich, dass derartige Aktivitäten, die einen direkten Einfluss auf die Energieversorgung eines Privatkunden haben, so zu schützen sind, dass kein unberechtigter Dritter gefälschte Aktivierungs- oder deaktivierungsnachrichten an den Meter senden darf.

Use Case: Erkennung und Behandlung von Ausfällen

Dieser Anwendungsfall beschreibt das rechtzeitige Erkennen von Ausfällen oder auch Fehlsteuerungen des Stromflusses, die schnellstmöglich gemeldet werden sollen. So kann beispielsweise bei einem Stromausfall das Gateway automatisiert eine Störungsmeldung senden. Alternativ könnte auch der Nutzer manuell über das Internet einen Störungsbericht senden. Da von einem Stromausfall ggf. auch IKT-Komponenten, die für den Austausch von Benachrichtigungen genutzt werden, betroffen sind, sollte bei diesem Anwendungsfall auch ein Ausfall der Kommunikation berücksichtigt werden. Die Störungsmeldungen werden über den Messstellenbetreiber an den Verteilnetzbetreiber gesendet, der dann entsprechende Gegenmaßnahmen einleiten kann. Die zu schützenden Daten sind hierbei Steuerungsdaten, die rechtzeitig und von autorisierten Stellen versandt werden müssen.

Use Case: Wartung

Smart Meter und Gateways müssen regelmäßig gewartet werden, z.B. müssen Firmware-Updates oder Patches installiert werden. Hierzu sendet der Messstellenbetreiber Steuersignale sowie Wartungsdaten wie Updates und Patches an die Geräte, um beispielsweise Sicherheitslücken zu schließen oder Konfigurationen an sich geänderte Bedingungen anzupassen.

Use-Case: Echtzeit-Tarifierung

Entsprechend der Angebots- und Nachfragesituation werden Energie-Preise variabel gestaltet und diese Preisinformationen über das Energieinformationsnetz, Internet oder ande-

re Datenkanäle an den Kunden gesendet. Dadurch erhält der Kunde die Möglichkeit, seine Energienutzung an den aktuellen Preis zu koppeln und seine Kosten zu reduzieren. Dieser Use-Case muss seit 30. Dezember 2010 nach dem Energiewirtschaftsgesetz (EnWG) [21] gemäß § 40 (5) EnWG[2] von Energieversorgungsunternehmen umgesetzt werden.

Insbesondere für den Verteilnetzbetreiber kann dieser Anwendungsfall relevant sein, um das Nutzungsverhalten des Energienutzers entsprechend der verfügbaren Energie zu beeinflussen. Für den Privatkunden können sich finanzielle Vorteile ergeben. Derzeit sind diese Vorteile zwar noch relativ gering [14], durch Einbindung von Elektrofahrzeugen ist aber zu erwarten, dass sich dies ändern wird. So können die Ladezeiten von Elektrofahrzeugen in gewissem Rahmen variiert werden, z.B. kann der Ladezeitraum in der Nacht relativ frei gewählt werden, so lange das Fahrzeug am Morgen aufgeladen ist. Aus diesem Grunde ist die Betrachtung der Elektromobilität wirtschaftlich von besonderem Interesse und wird in Kapitel 5 noch detailliert betrachtet

Bei der Abrechnung muss berücksichtigt werden, dass der Energielieferant den jeweiligen Messwerten die korrekten Preisinformationen zu Grunde legt. Hierzu ist es ggf. nicht mehr ausreichend, dass der Messdienstleister dem Energielieferanten aggregierte Messwerte zur Verfügung stellt. Dies muss in der Sicherheitsarchitektur bei der Umsetzung eines Datenschutzkonzeptes entsprechend berücksichtigt werden.

[2] In der Fassung vom 04.08.2011 (geändert durch Artikel 1 G. v. 26.07.2011 BGBl. I S. 1554)

3.3 Sicherheitsanforderungen

Basierend auf den sicherheitsrelevanten Anwendungsfällen, die im vorigen Kapitel vorgestellt wurden, werden nun die Sicherheitsanforderungen für die Rollen Energienutzer, Verteilnetzbetreiber, Energielieferant, Kommunikationsnetzbetreiber, Messstellenbetreiber, Messdienstleister und Hersteller beschrieben. Nicht betrachtet werden die Rollen weiterer Energiedienstleister, da deren Aufgaben, Rechte und Pflichten derzeit noch offen sind, so dass keine konkreten Sicherheitsannahmen getroffen werden können.

Der Fokus der nachfolgenden Betrachtungen liegt auf den IKT-Sicherheitsanforderungen, d.h. den Anforderungen zum Schutz der verschiedenen Arten von Daten bei der Kommunikation und in den datenverarbeitenden Systemen. Zur differenzierten Betrachtung wird zwischen den nachfolgend beschriebenen Arten von Daten unterschieden, die zwischen den Mitgliedern der verschiedenen Rollen ausgetauscht werden bzw. gespeichert sind:

- Messwerte
- Daten zur Abrechnung
- Aktuelle Verbrauchsdaten
- Preisinformationen
- Rechnungsdaten
- Steuerungsdaten
- Wartungsdaten
- Statusdaten
- Weitere Daten.

Bei den vom Kunden an den Messdienstleister bzw. vom Messdienstleister an den Energieversorger gesendeten *Messwerten* über verbrauchte bzw. eingespeiste Energie ist aus Sicherheitssicht, insbesondere aus

Sicht des Datenschutzes, interessant, in welcher Genauigkeit sie auftreten. So können Messwerte beispielsweise für einen einzelnen Kunden sekundengenau oder auch in größeren Intervallen (z.B. alle 15 Minuten, täglich, monatlich) erfasst werden. Auch können Messwerte mehrerer Kunden aggregiert werden.

Zur *Abrechnung* werden auch weitere Daten wie z.B. Name des Anschlussinhabers, Kontaktdaten, Kontodaten, Zählernummer etc. benötigt, die beim Energieversorger gespeichert sind. Auch werden einige Daten vom Energienutzer an den Energieversorger gesendet. Zur Zuordnung der Messwerte zu einem Energienutzer kann beispielsweise die Zählernummer oder eine andere eindeutige ID zur Identifikation mitgesendet werden. Weitere Daten zur Abrechnung können auch Daten zur Annahme eines Tarifs sein. Bei der Elektromobilität können auch Zahlungsinformationen, wie Kreditkartendaten, bei einem entsprechenden Zahlungsmodell übertragen werden müssen (vgl. Kapitel 5).

Aktuelle Verbrauchsdaten können dem Kunden beispielsweise über das Internet vom Energielieferanten zur Verfügung gestellt werden, um eine Verbrauchstransparenz zu ermöglichen.

Über erhaltene *Preisinformationen* kann der Kunde sein Nutzungsverhalten anpassen und beispielsweise seine häuslichen Elektrogeräte (automatisiert) einschalten, wenn der Preis gerade niedrig ist. Auch ist denkbar, dass dem Kunden Prognosedaten über die mögliche Preisentwicklung zur Verfügung gestellt werden, so dass dieser seine Energienutzung in gewissem Rahmen planen kann. Die Preisinformationen können entweder direkt an das Gateway oder über das Internet an den PC[3] des Kunden gesendet werden.

Rechnungsdaten werden derzeit größtenteils per Post an den Kunden gesendet. In Zukunft wird dies voraussichtlich fast ausschließlich elektronisch über das Internet erfolgen.

Steuerungsdaten werden zur entfernten Kontrolle und zur Steuerung z.B. von Smart Metern, Verbrauchern, Speichern oder Erzeugern gesendet. Beispielsweise kann ein Messstellenbetreiber Nachrichten zum Ein- und Ausschalten von Smart Metern senden. Auch im Verteilnetz ist der Schutz von Steuerungsdaten bzw. auch von Regelungsdaten von großer Bedeutung, da erfolgreiche Angriffe hier direkte Auswirkungen auf die Versorgungssicherheit einzelner Privatkunden oder einer ganzen Gruppe von Kunden haben können.

Der Messstellenbetreiber sendet *Wartungsdaten* wie Updates und Patches, die auf Smart Metern und Gateways installiert werden, um neue Funktionalitäten zu ermöglichen und um bekannt gewordene Sicherheitslücken zu schließen.

Bei den *Statusdaten* handelt es sich beispielsweise um Informationen über die Eigenschaften von Erzeugern oder Speichern sowie deren aktuellen Zustand. Bei einem Speicher könnten Statusdaten beispielsweise die maximale Speicherkapazität und den aktueller Ladezustand enthalten. Bei Erzeugungsanlagen könnten Statusmeldungen beispielsweise die aktuell verfügbare Leistung, die ins Stromnetz eingespeist werden kann, angeben. Bei der Elektromobilität (vgl. Kapitel 5) könnten Statusmeldungen die verfügbaren

[3] In Zukunft ist eine Darstellung auf mobilen Endgeräten sicherlich eine sehr viel nahe liegendere Präsentationsalternative.

Speicherkapazitäten oder Informationen, wie lange das Fahrzeug voraussichtlich an diesem Ladepunkt angeschlossen sein wird, umfassen.

Der Punkt *weitere Daten* umfasst alle noch nicht erfassten Daten, die für weitere mögliche Use-Cases benötigt werden. Dies können beispielsweise Warnmeldungen bei Ausfällen sein.

Im Folgenden werden die 7 Rollen beschrieben, die für die Domäne Privatkunde aus Sicherheitssicht dominant sind, und deren Sicherheitsanforderungen abgeleitet.

(1) Rolle: Energienutzer

Der Privatkunde in der Rolle als Energienutzer hat in der Regel hohe Anforderungen an den Datenschutz und an die Wahrung seiner Privatsphäre. Somit müssen Vertraulichkeit und der Schutz aller personenbezogenen bzw. personenbeziehbaren (Energie)-Daten gewährleistet sein, um die Erstellung von Nutzungsprofilen zu verhindern. Dies umfasst die Messwerte, Daten zur Abrechnung wie die Adaption an geänderte Preisinformationen, aktuelle Verbrauchsdaten, Statusmeldungen und Rechnungsdaten. Zum einen müssen die Daten gegen unberechtigte externe Dritte geschützt werden, angefangen bei der Erfassung, über die Übertragung, bis zur (ggf. langfristigen) Speicherung und Verarbeitung der Daten in (Rechnungs-) Datenbanken des Energielieferanten oder Messdienstleisters. Zum anderen sollten auch der Energielieferant und der Messdienstleister nicht in der Lage sein, personenbezogene bzw. personenbeziehbare Daten des Energienutzers auszuwerten. Diese Anforderung erscheint jedoch zu restriktiv und erschwert oder verhindert zukünftige Geschäftsmodelle, die auch einen interessanten Mehrwert für Kunden haben könnten. So sind Szenarien denkbar, in denen der Energienutzer seinem Lieferanten ganz bewusst personenbeziehbare Daten verfügbar macht und damit Profilbildungen durch diesen Lieferanten nicht nur in Kauf nimmt, sondern sogar unterstützt, weil für den Kunden damit Anreize wie Rabattierungs-Modelle etc. verbunden sind. Damit ergibt sich die Anforderung nach Maßnahmen und Dienstleistung, die eine nutzerkontrollierbare Weitergabe von personenbeziehbaren Energiedaten ermöglichen. Dies stellt besondere Anforderungen an das Design von Smart-Metern bzw. Gateways und den Zugangsgeräten zu diesen Komponenten. Es muss auf einfache Weise möglich sein, Datenschutz-Regeln zu formulieren und deren Einhaltung nachvollziehbar zu kontrollieren.

Eine weitere zentrale Anforderung der Rolle Energienutzer betrifft die Korrektheit der Abrechnungen, d.h. Messwerte müssen korrekt erfasst und, ebenso wie Daten zur Abrechnung, unverändert und vollständig, sowie zeitlich korrekt an den Energielieferanten oder Messdienstleister übertragen werden. Auch müssen die vom Kunden empfangenen Preisinformationen korrekt, aktuell und verbindlich sein. Alle Daten müssen eindeutig dem richtigen Kunden zugeordnet werden können. Die beim Energienutzer installierten IKT-Komponenten wie Smart Meter und Gateways müssen hierfür vor Manipulationen geschützt werden, d.h. die Integrität dieser Systeme muss gewährleistet sein. So muss die genutzte Software nachweislich authentisch und unverfälscht über die gesamte Lebenszeit der Komponenten ihre Aufgaben erfüllen. Das bedeutet, dass die Komponenten insbesondere geeignete, nicht umgehbare Konzepte zur Abwehr von Manipulationsangriffen umfassen müssen, sowie auch die

Möglichkeit unterstützen müssen, dass man die Fehlerfreiheit und Unverfälschtheit der Komponenten jederzeit, auch über Fernzugriffe, überprüfen kann. Die erforderlichen Schutzmaßnahmen müssen auch Angriffe, die einen physischen Zugriff erfordern, abwehren können, da ein solcher Zugriff u.a. für die Kunden stets möglich ist. Die Forderung der Unverfälschtheit erstreckt sich über die gesamte Zeit des Einsatzes der Komponenten und schließt natürlich die korrekte Installation und Wartung durch den Messstellenbetreiber mit ein.

Zusätzlich zur korrekten und unverfälschten Erfassung, Speicherung und ggf. Vorverarbeitung der Messdaten ist zu fordern, dass diese Daten sicher zu autorisierten Empfängern übertragen werden. Dazu ist wiederum erforderlich, dass geeignete Maßnahmen ergriffenwerden, die sicherstellen, dass die Daten unverfälscht, vollständig und rechtzeitig bei den korrekten Empfängern ankommen und dass der Datenursprung überprüfbar ist. Eine absichtlich oder unabsichtlich erfolgte, erneute Einspielung korrekter Datensätze muss ebenfalls erkannt und abgewehrt werden.

Die Forderung nach Authentizität und Integrität der Datenkommunikation bezieht sich nicht nur auf die von den Smart Metern bzw. Gateways gesendeten Daten, sondern natürlich auch auf die Daten, die vom Energieversorger an die Smart Meter bzw. Gateways oder über das Internet an Rechner des Kunden gesendet werden. Dies umfasst die aktuellen Verbrauchsdaten, Rechnungsdaten aber auch insbesondere kritische Steuernachrichten, bei denen ggf. auch noch die Aktualität wichtig ist, um beispielsweise Smart Meter zu aktivieren bzw. zu deaktivieren. Auch Wartungsdaten wie Firmware-Updates und Patches, die der Messstellenbetreiber oder der Energielieferant an die Geräte sendet und installiert, müssen einen Ursprungsnachweis führen und unverfälscht sein, damit Manipulationsversuche durch absichtlich oder unabsichtlich eingeschleuste Schadsoftware frühzeitig erkannt und abgewehrt werden können.

Neben den IKT-Komponenten von Smart Grids muss auch das eigentliche Stromnetz geschützt und die Versorgungssicherheit gewährleistet sein. Seit Jahren werden hierfür in der Energiewirtschaft etablierte Verfahren eingesetzt, auf die in diesem Artikel jedoch nicht weiter eingegangen wird. Durch die sehr starke Durchdringung der klassischen Energieversorgungsnetze mit IKT-Komponenten zur Steuerung und Überwachung der Energieverteilnetze unterliegt jedoch auch die Bedrohungs- und Risikolage dieser Netze einem starken Wandel. So kann die eingesetzte IKT nicht nur angegriffen werden, sondern sogar als Tatwaffe gezielt missbraucht werden, um die Energieversorgung zu unterbrechen oder sogar mittelfristig zu gefährden. Das bedeutet, dass der Absicherung der eingesetzten IKT-Komponenten in Zukunft ein sehr hoher Stellenwert zukommen wird, da es durch Angriffe auf die IKT-Komponenten bzw. durch die missbräuchliche Nutzung dieser IKT-Komponenten potentiell zu Ausfällen oder Fehlsteuerungen der Energieversorgung für einzelne Regionen oder ggf. sogar kaskadierend für weite Landstriche kommen kann. Hierauf wird nachfolgend bei der Beschreibung der Sicherheitsanforderungen der Verteilnetzbetreiber in Kapitel 4 eingegangen.

Zusammengefasst sind die Sicherheitsanforderungen für den Energienutzer die folgenden:

- Vertraulichkeit und Datenschutz (bzw. nutzerkontrollierbare Weitergabe) von Mess-

werten, Daten zur Abrechnung, aktuellen Verbrauchsdaten, Statusmeldungen, Rechnungsdaten

- Authentizität und Integrität von Messwerten, Daten zur Abrechnung und Wartungsdaten
- Authentizität, Integrität und Aktualität von Steuerdaten
- Authentizität, Integrität, Aktualität und Verbindlichkeit von Preisinformationen
- Integrität der Systeme von Smart Metern, Gateways etc.
- Versorgungssicherheit.

(2) Rolle: Verteilnetzbetreiber

Wichtigste Anforderung eines Verteilnetzbetreibers ist sicherlich die Gewährleistung der Versorgungssicherheit, um die Energieversorgung im vertraglich zugesicherten Umfang sicherzustellen. Neben den etablierten Verfahren der Energiewirtschaft müssen auch Verfahren der IT-Sicherheit etabliert werden, um den neuen und erweiterten Angriffsmöglichkeiten, die sich aus der genutzten IKT ergeben können, Rechnung zu tragen.

Eine korrekt arbeitende IKT ist essentiell, um die notwendigen Steuerungen im Verteilnetz und allgemein in Smart Grids durchzuführen. Zum einen umfasst dies die Steuerungen von Systemen wie Umspannwerken innerhalb des Verteilnetzes. Hierzu kann der Verteilnetzbetreiber Messstellen innerhalb seines Verteilnetzes nutzen, um Messungen durchzuführen und auf deren Basis Steuerungen vorzunehmen. Alternativ könnten auch Messwerte der Smart Meter für Steuerungen verwendet werden. Die Problematik der Steuerungen innerhalb des Verteilnetzes wird detailliert in Kapitel 4 betrachtet und hier nicht weiter behandelt.

Zum anderen wird der Verteilnetzbetreiber auch verstärkt mit Energienutzern bzw. Energieerzeugern (Prosumer) kommunizieren, um angemessen auf Angebot und Nachfrage reagieren zu können. Beispielsweise können Preismodelle und das Dienstleistungsangebot an das aktuelle Angebot bzw. die aktuelle oder absehbare Nachfrage angepasst werden, um Verbraucher mit überzeugenden Mehrwertdiensten dazu anzuregen, ihr Energieverbrauchsverhalten dem verfügbaren Stromangebot anzupassen. Auch ist vorstellbar, dass Netzbetreiber mit den Kunden spezielle Service-Verträge abschließen, die es den Betreibern unter speziellen Rahmenbedingungen erlauben, selber, zum Beispiel durch Fernabschaltung von Geräten, in den Verbrauch beim Kunden regulierend einzugreifen. Hierzu könnten beispielsweise Nachrichten mit Preisinformationen an den Energienutzer gesendet werden und dieser kann z.B. mit der Annahme eines passenden Tarifs antworten. Da kaum zu erwarten ist, dass ein Endkunde derartige Entscheidungen explizit in Realzeit selber treffen möchte, werden Konzepte wie der smarte Energiebutler, wie sie derzeit in den E-Energy-Modellregionen erprobt werden, umzusetzen sein, um eine regelbasierte, automatisierte Entscheidung zu ermöglichen. Hierfür ist es natürlich notwendig, dass derartige Regeln einfach formuliert werden können und korrekt umgesetzt werden. Auch ist zu erwarten, dass der Kunde (natürlich nicht der Endkunde selber, sondern dies erfolgt automatisiert durch seine IKT-Komponenten) Statusmeldungen über den Zustand von vorhandenen Speichern und Erzeugungsanlagen an den Verteilnetzbetreiber sendet, so dieser beispielsweise seine Lastflusssteuerung an die von den Pro-

sumern eingespeiste Energie anpasst. Somit muss die Authentizität, Integrität, Verfügbarkeit und Aktualität von Steuerdaten und Statusmeldungen sichergestellt sein.

Weiterhin hat der Verteilnetzbetreiber die Anforderung, dass die Abrechnung mit dem Energielieferanten bzw. direkt mit dem Energienutzer korrekt erfolgt. Hierzu erhält der Verteilnetzbetreiber vom Messdienstleister die notwendigen Daten. Aus Sicht des Datenschutzes muss hier geklärt werden, welche Daten für Abrechnungszwecke nötig sind. So sind sicherlich keine sekundengenauen Messwerte individueller Kunden notwendig. Jedoch muss bei variablen Preisen gewährleistet sein, dass die jeweils aktuellen Preise für die Abrechnung verwendet werden. Hier ließen sich beispielsweise Messwerte für einzelne Preisstufen monatlich aggregieren. Auch müssen diese Daten, genauso wie weitere Daten zur Abrechnung, wie sie beispielsweise zur Annahme eines Tarifs gesendet werden, korrekt, vollständig und vom richtigen Kommunikationspartner stammen.

Gleiches gilt für Rechnungsdaten, die an den Kunden gesendet werden. Zur Erstellung von Abrechnungen müssen diese Daten zwar verfügbar sein, aber die Erfüllung von Echtzeitanforderungen ist nicht erforderlich. Wenn bestimmte Daten jedoch dazu führen, dass in die Steuerung der Verteilnetze koordinierend eingegriffen wird, um z.B. Angebot und Nachfrage besser aufeinander abzustimmen, so ist die Aktualität und Vollständigkeit der Daten besonders wichtig, d.h. solche Daten unterliegen gewissen Echtzeitanforderungen. Welche Daten dem Verteilnetzbetreiber hierfür zur Verfügung gestellt werden, sollte der Energienutzer entsprechend der oben erwähnten Datenschutz-Regeln entscheiden können. Beispielsweise kann der Verteilnetzbetreiber sekundengenaue Messwerte erhalten, deren Ursprung aber anonymisiert wurde, so dass sie nur noch dem entsprechenden Netzsegment zuordenbar sind und nicht mehr dem individuellen Energienutzer.

Da Smart Meter und Gateways direkt beim Kunden installiert sind, können diese theoretisch leicht manipuliert werden. Somit ist für eine korrekte Abrechnung, wie bereits oben erwähnt, ebenfalls wieder die Integrität von Smart Metern und Gateways sowie Authentizität und Integrität von Wartungsdaten erforderlich.

Zusammengefasst umfassen die Sicherheitsanforderungen für den Verteilnetzbetreiber folgende Punkte:

- Versorgungssicherheit im vertraglich zugesicherten Umfang
- Authentizität, Integrität, Verfügbarkeit und Aktualität von Preisinformationen, Steuerdaten und Statusdaten
- Authentizität und Integrität von aggregierten oder anonymisierten Messwerten und Daten zur Abrechnung
- Integrität der Systeme von Smart Metern, Gateways etc.
- Authentizität und Integrität von Wartungsdaten.

(3) Rolle: Energielieferant

Der Energielieferant als „Wiederverkäufer“ der vom Verteilnetzbetreiber gelieferten Energie hat implizit ähnliche Sicherheitsanforderungen wie der Verteilnetzbetreiber, d.h. die Versorgungssicherheit und korrekte Abrechnung mit Verteilnetzbetreibern und Energienutzern. Ausnahmen bilden Steuerdaten und Statusdaten sowie ggf. fein-granulare ano-

nymisierte Messwerte, die nur für den Verteilnetzbetreiber zum Betrieb seiner Infrastruktur notwendig sind.

Zusammengefasst sind die Sicherheitsanforderungen für den Energielieferanten die folgenden:

- Versorgungssicherheit im vertraglich zugesicherten Umfang
- Authentizität, Integrität, Verfügbarkeit und Aktualität von Preisinformationen
- Authentizität und Integrität von aggregierten Messwerten und Daten zur Abrechnung
- Integrität der Systeme von Smart Metern, Gateways etc.
- Authentizität und Integrität von Wartungsdaten.

(4) Rolle: Messstellenbetreiber

Das Geschäft des Messstellenbetreibers ist die korrekte Installation, sowie der Betrieb und die Wartung von Messstellen wie Smart Metern und Gateways. Um sicherzustellen, dass nur Berechtigte auf die Messstellen zugreifen können, muss eine Authentifizierung und Autorisierung stattfinden. Die bei Wartungsarbeiten an die Messstellen gesendeten Steuerdaten und Wartungsdaten müssen authentisch und unverfälscht sein. Auch darf im Zuge von Wartungsarbeiten an den Geräten der Messstellenbetreiber keinen unautorisierten Zugang zu vertraulichen, privaten oder sonstigen sicherheitsrelevanten Daten des Kunden erhalten. Dies umfasst Messwerte, Daten zur Abrechnung, aktuelle Verbrauchsdaten, und Rechnungsdaten. Als Basis für die Arbeiten des Messstellenbetreibers muss sichergestellt werden, dass dessen Arbeitsumgebung vertrauenswürdig ist. Andernfalls könnten beispielsweise auf einem Server des Messstellenbetreibers Firmware Updates manipuliert werden, die anschließend korrekt signiert vom Messstellenbetreiber auf den Geräten installiert werden. Die Messstellen selbst, d.h. Smart Meter und Gateways, müssen gegen Manipulationen geschützt werden. Dies beinhaltet sowohl Manipulationen mittels physischem Zugriff als auch über Kommunikationsschnittstellen.

Zusammengefasst sind die Sicherheitsanforderungen für den Messstellenbetreiber die folgenden:

- Authentifizierung und Autorisierung von Zugriffen auf Messstellen
- Authentizität und Integrität von Steuerdaten und Wartungsdaten
- Schutz der Vertraulichkeit personenbeziehbarer Daten vor dem Messstellenbetreiber
- Vertrauenswürdige Arbeitsumgebung beim Messstellenbetreiber
- Integrität der Systeme von Smart Metern, Gateways etc.

(5) Rolle: Messdienstleister

Die Sicherheitsanforderungen des Messdienstleisters sind die Authentizität, Integrität und die Verfügbarkeit der Messwerte, die vom Energienutzer mittels Smart Metern erfasst werden, und ggf. weiterer benötigter Daten zur Abrechnung. Diese sind für eine korrekte Abrechnung mit dem Energielieferanten bzw. Verteilnetzbetreiber notwendig. Der Messdienstleister muss seinerseits diese Daten korrekt speichern, verarbeiten und vertraulich an autorisierte Stellen weiterreichen und die Datenschutzanforderungen einhalten. Auch hier sind wieder die Energienutzer-

spezifischen Datenschutz-Regeln zu berücksichtigen. So sind für Abrechnungen sicherlich wieder aggregierte Messwerte ausreichend. Der Nutzer kann jedoch auch dem Messdienstleister detailliertere Messwerte zur Verfügung stellen, wenn dies für ihn einen Mehrwert wie günstigere Tarife oder eine Echtzeitanzeige des Verbrauchs über das Internet bietet. Diese Daten könnten entsprechend seiner festgelegten Datenschutz-Regeln auch dem Energielieferanten oder Verteilnetzbetreiber (ggf. anonymisiert) zur Verfügung gestellt werden. Die gestellten Verfügbarkeitsanforderungen umfassen jedoch keine Echtzeitanforderungen und keine rund um die Uhr Verfügbarkeit.

Zusammengefasst sind die Sicherheitsanforderungen für den Messdienstleister die folgenden:

- Authentizität, Integrität und Verfügbarkeit der (aggregierten) Messwerte und Daten zur Abrechnung
- Vertrauenswürdige Verarbeitung, Speicherung und Weiterleitung der (aggregierten und/oder anonymisierten) Messwerte an autorisierte Dritte.

(6) Rolle: Kommunikationsnetzbetreiber

Ein oder mehrere Kommunikationsnetzbetreiber stellen die Infrastrukturen für die Kommunikation in Smart Grids bereit. Diese werden, mit Ausnahme der Hersteller, von allen relevanten Rollen zur Kommunikation innerhalb von Smart Grids verwendet. Der oder die Kommunikationsnetzbetreiber müssen hierbei verschiedene Regularien aus dem Telekommunikationsumfeld wie beispielsweise das Telekommunikationsgesetz (TKG) [16] einhalten. Auf diese Regularien und Gesetze gehen wir im Rahmen der in diesem Artikel durchgeführten Betrachtungen jedoch nicht weiter ein.

Für Smart Grids ist Verfügbarkeit und korrekte Funktionsweise der Kommunikationsnetzinfrastruktur, um einen zuverlässigen Austausch von Daten zu gewährleisten, die wichtigste Anforderung. Die sich hieraus ergebenden Anforderungen im Bereich der Telekommunikation wie z.B. Authentizität der Nutzer der Kommunikationsnetzinfrastruktur etc. sollen hier nicht weiter betrachtet werden. Auch sollen hier keine Anforderungen aus möglichen Geschäftsmodellen eines Kommunikationsnetzbetreibers wie z.B. dedizierte Leitungen zum Schutz der ausgetauschten Daten vor Manipulationen, Abhören etc. aufgelistet werden, da dies den Rahmen dieses Artikels sprengen würde. Im Zusammenspiel mit den anderen Rollen in Smart Grids ist jedoch die Anforderung nach korrekter Abrechnung mit diesen Rollen, welche die Kommunikationsnetzinfrastruktur nutzen, relevant. Somit müssen Authentizität und Integrität von Abrechnungsdaten für die Nutzung des Kommunikationsnetzes gewährleistet sein.

Zusammengefasst sind die Sicherheitsanforderungen für den Kommunikationsnetzbetreiber die folgenden:

- Verfügbarkeit der Kommunikationsnetzinfrastrukturen
- Authentizität und Integrität von Abrechnungsdaten für die Nutzung des Kommunikationsnetzes.

(7) Rolle: Hersteller

Die Sicherheitsanforderungen der Hersteller sind nicht Schwerpunkt dieses Artikels, sie sollen aber hier trotzdem kurz betrachtet werden Ein Hersteller von Smart Metern und

Gateways für die Endkunden-Domäne möchte in erster Linie seine Geräte verkaufen. Um diese in zukünftigen sich abzeichnenden Märkten national und europaweit verkaufen zu können, müssen sie mit hoher Wahrscheinlichkeit weitaus höhere Sicherheitsanforderungen erfüllen, als dies derzeit noch der Fall ist. Zwar müssen die Geräte bereits heute bestimmte gesetzliche Bestimmungen, Normen oder Standards erfüllen, wie die Einhaltung von Normen zur Funktionssicherheit (z.B. IEC 61850, ISO 9506, IEC 61508), jedoch gibt es derzeit noch keine Auflagen hinsichtlich der zu garantierenden IT Sicherheit. Es ist zu erwarten, dass sich dies mit der Verabschiedung des derzeit noch in der Bearbeitung befindlichen Schutzprofils für Smart Meter Gateways [2] durch das BSI im Auftrag des BMWi möglicherweise bereits schon im Jahr 2012 ändern wird.

Derzeit schreibt das BSI-Schutzprofil den Einsatz eines speziellen Hardwareschutzes in Form eines so genannten Hardware-Sicherheits-Modul (HSM), das in Komponenten zum Schutz vor Manipulationen zusätzlich zu integrieren ist, lediglich für Gateways vor. Für einen Smart Meter, der nicht in ein Gateway integriert ist, ist solch ein HSM nach derzeitigem Stand der Diskussion[4] nicht verpflichtend. Wie umfangreiche Sicherheitsanalysen in den Laboren des Fraunhofer AISEC[5] in München jedoch gezeigt haben, sind solche ungeschützten Smart Meter leicht angreifbar. Mittels sehr einfacher Angriffe konnten handelsübliche Smart Meter bzw. Gateways so manipuliert werden, dass Daten eingeschleust, verändert, abgehört oder unterdrückt werden. So ist es beispielsweise leicht möglich, die Firmware inklusive aller gespeicherten kryptographischen Schlüssel auszulesen und beliebige Manipulationen vorzunehmen. Hierdurch kann sich ein Angreifer beispielsweise kostenlose Energie verschaffen. Ein erheblich schwerwiegenderer Angriff wäre möglich, wenn Steuerungen im Verteilnetz auf Basis von Smart Meter Daten durchgeführt werden. Manipulierte Smart Meter könnten dann einen sehr hohen Energiebedarf vorspiegeln, um damit das Netzsegment zu überlasten oder sogar aufgrund kaskadierender Effekte weitere Bereiche des Stromnetzes gefährden.

In der öffentlichen Diskussion nimmt die Problematik des Datenschutzes einen hohen Stellenwert ein. Bereits 2009 wurde in einer kanadischen Studie zum Datenschutz in Smart Grids aufgezeigt, wie sich aus einer feingranularen Verbrauchsdatenerfassung Nutzungs- und damit auch Verhaltensprofile von Energieverbrauchern ableiten lassen können [17]. In den Niederlanden hat eine öffentliche Diskussion zu den Fragen des Datenschutzes und der Akzeptanz von Smart Metern auch bereits 2009 eingesetzt, nachdem das Tilburg Institute for Law and Technology (TILT) in seiner Sicherheitsanalyse zu dem Ergebnis gekommen war, dass die Vorgaben des holländischen Smart-Meter-Gesetzes eine Verletzung europäischer Datenschutzbestimmungen darstellen. Das Bewusstsein für datenschutzrechtliche Probleme im Zusammenhang mit Smart Metern ist bei Verbrauchern und bei der Politik sehr stark ausgeprägt, so dass zu erwarten ist, dass zumindest ein Teil der Hersteller kurz- bis mittelfristig stärkere Sicherheitsmaßnahmen in ihre Produkte integrieren werden, um die Akzeptanz ihrer Produkte bei den Kunden zu erhöhen, auch wenn diese Maßnahmen derzeit nicht gesetzlich gefordert sind. Im sicherheits- und datenschutzbewussten deut-

[4] Januar 2012

[5] Vgl. http://www.aisec.fraunhofer.de

schen, und teilweise europäischen Markt könnte das Anbieten entsprechend abgesicherter Geräte ein Marktvorteil für diese Hersteller sein.

3.4 Sicherheitsarchitektur

Im Folgenden wird eine generische Sicherheitsarchitektur für die Domäne Privatkunde vorgestellt, welche die in Kapitel 3.3 beschriebenen Sicherheitsanforderungen erfüllt. Hierzu werden auf einem, in diesem Schritt zwangsläufig noch relativ hohem, Abstraktionsniveau die wesentlichen Sicherheitsmechanismen und deren Schnittstellen anhand eines Netz-Referenzmodells auf der Basis von definierten Referenzpunkten beschrieben. Weiterhin werden schon einige Konzepte zur Umsetzung erläutert.

Referenzmodell

Abbildung 4 verallgemeinert Abbildung 3 und zeigt das Referenzmodell der Domäne Privathaushalt. Dargestellt sind die Komponenten Verbraucher, Smart Meter, Gateway, PC[6] und der Energieversorger, sowie deren Beziehungen zueinander. Die Verbraucher stehen repräsentativ auch für Speicher und Erzeugungsanlagen, die potentiell bei einem Kunden installiert sein können, da die Sicherheitsbetrachtungen auf dem hier betrachteten Niveau analog sind.

Anhand der Referenzpunkte 1 bis 7 werden nachfolgend die Sicherheitsmechanismen der Sicherheitsarchitektur für die Komponenten und Schnittstellen beschrieben.

Referenzpunkt 1

Referenzpunkt 1 beschreibt die Kommunikation zwischen Verbrauchern (bzw. Speicher oder Erzeuger) und Gateway, z.B. wenn das Gateway aufgrund eines niedrigen Preises entscheidet, einen Verbraucher einzuschalten. Hier müssen entsprechende Zugriffskontrollen etabliert werden, so dass dies nur die dazu berechtigten Komponenten durchführen dürfen. Die entsprechenden Steuerdaten müssen authentifiziert, autorisiert und integer sein. Dies gilt ebenfalls für die andere Kommunikationsrichtung. Falls Speicher oder Erzeuger Statusmeldungen über das Gateway an den Energieversorger senden, sollten diese auch auf diesem Kommunikationsabschnitt geschützt sein, d.h. die Authentizität und Integrität sollte gewährleistet sein. Somit sind die umzusetzenden Sicherheitsmechanismen:

- Mechanismen zur Authentifizierung, Autorisierung und zum Integritätsschutz von Steuerdaten
- Mechanismen zur Authentifizierung und zum Integritätsschutz von Statusmeldungen.

Die Umsetzung der Authentifizierung und Autorisierung wird an dieser Stelle voraussichtlich mit relativ einfachen Mechanismen realisiert, da die eingebetteten Systeme in den Verbrauchern stark in ihren Ressourcen (z.B. Rechenleistung, Speicher) eingeschränkt sein werden. Hier bieten sich Verfahren basierend auf symmetrischer Kryptographie wie Message Authentication Codes (MAC) an (vgl [4]), um Daten zu authentifizieren. Dies würde gleichzeitig die Integrität der Daten sicherstellen. Ein noch zu lösendes Problem ist hierbei die Frage der sicheren und effizienten Verteilung der benötigten symmetrischen Schlüssel. Während die Frage der Authentisierung bereits relativ konkret diskutiert wird,

[6] Als Platzhalter für andere Präsentationsgeräte beim Nutzer

erscheint derzeit die Problematik der Autorisierung, also der Überprüfung von Zugriffsberechtigungen, noch weitestgehend offen zu sein. Aufgrund der beschränkten Ressourcen der beteiligten Komponenten erscheint es derzeit eher fraglich, ob Maßnahmen zur Autorisierung überhaupt umgesetzt werden sollten.

Referenzpunkt 2

Die Sicherheitsmechanismen für Smart Meter leiten sich im Wesentlichen aus den Anforderungen nach korrekter Abrechnung und der Einhaltung des Datenschutzes ab. Es muss sichergestellt werden, dass Smart Meter nicht manipuliert werden und nur Mitglieder von solchen Rollen zugreifen dürfen, welche die entsprechenden Berechtigungen haben. Da die von Smart Metern erfassten Messwerte personenbeziehbare Daten sind, könnte man hier oder auch im Gateway Mechanismen zum Schutz dieser Daten etablieren. Diese Mechanismen dienen der Umsetzung der oben erwähnten Datenschutz-Regeln und müssen in ein Gesamtkonzept zum Datenschutz integriert sein. Die umzusetzenden Sicherheitsmechanismen sind somit:

- Mechanismen zum Schutz gegen Manipulationen
- Mechanismen zur Authentifizierung und Autorisierung zugreifender Rollen
- Mechanismen zum Schutz personenbezogener Daten.

Zur Umsetzung des ersten Punktes kann beispielsweise spezielle Hardware eingesetzt werden. Da Smart Meter direkt beim Energienutzer aufgestellt sind (vgl. Abbildung 3), können diese leicht durch direkten physikalischen Kontakt angegriffen werden, um die Firmware zu manipulieren oder um Daten wie kryptographische Schlüssel auszulesen. Ein Angreifer kann hier beispielsweise über zu-

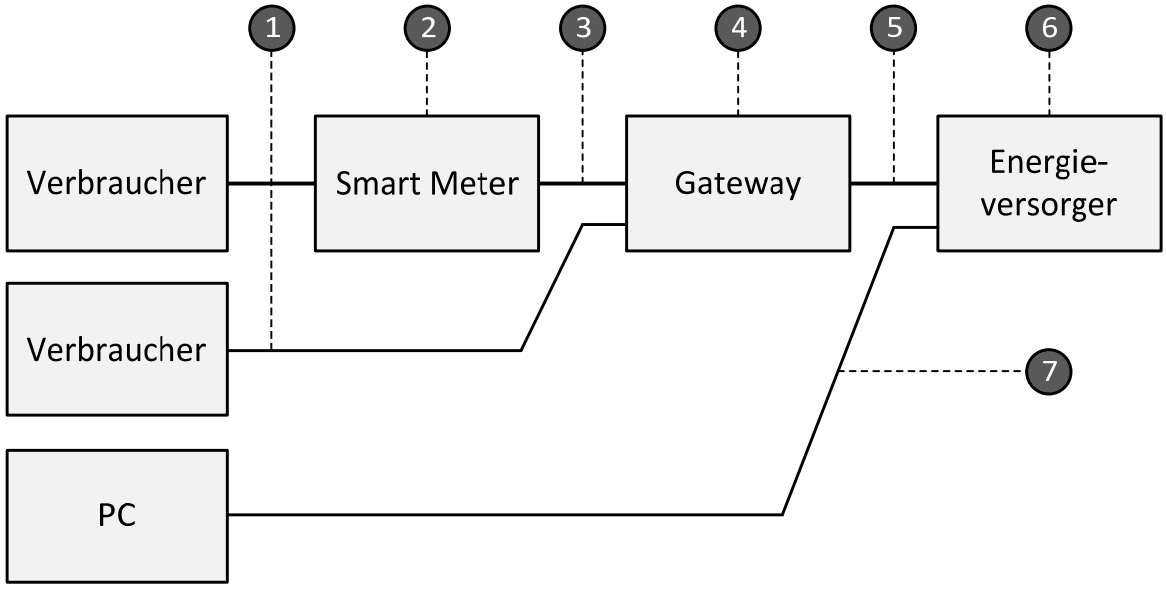


Abbildung 4: Referenzmodell der Subdomäne Privathaushalt mit Referenzpunkten

gängliche Schnittstellen (z.B. JTGA, USB) angreifen oder auch fortgeschrittene Angriffstechniken wie Seitenkanalangriffe nutzen [18, 19].

Bei klassischen Zählern erfolgt der Schutz vor Manipulationen über die Kontrolle der Unversehrtheit von Plomben, die das Gehäuse des Zählers versiegeln. Dies erfordert grundsätzlich eine regelmäßige Überprüfung der Unversehrtheit der Plombe, was einen erheblichen Aufwand und damit Kosten bedeutet. Für Smart Meter bietet sich als Alternative der Einsatz von Hardware-Sicherheits-Modulen, wie oben bereits angesprochen, an, die eine sichere Ausführungsumgebung für kryptographische Operationen und sichere Speicherbereiche z.B. für kryptographische Schlüssel bieten. Um Manipulationen an Software, die sich außerhalb des HSMs befindet, zu erkennen, bieten existierende HSMs Funktionen wie z.B. Plattformintegritätstests oder Funktionen wie Remote Attestation an. Damit lässt sich die Unversehrtheit der installierten Software gegenüber Dritten nachweisen.

Durch den Einsatz von HSMs entstehen jedoch zusätzliche Kosten, was der Anforderung der Betreiber nach einer möglichst kostengünstigen Lösung widerspricht. Hier ist ein entsprechender Kompromiss zwischen Sicherheit und Wirtschaftlichkeit zu finden. Eine naheliegende Möglichkeit besteht in der Konzentration der Sicherheitsfunktionen auf das Gateway. Handelt es sich dabei um ein Multi-Utility-Gateway, so könnten über eine Sicherheitskomponente neben Stromzählern auch weitere Zähler wie Gas- und Wasserzähler angeschlossen und deren Daten für die Interaktion nach Außen abgesichert werden. Dies setzt jedoch voraus, dass diese Sensoren keine weiteren Schnittstellen besitzen, über die sie direkt unter Umgehung des Gateways, der hier als Sicherheitsfilter fungieren würde, von außen kontaktiert werden können.

Eine Authentifizierung kann durch kryptographische Protokolle umgesetzt werden, die beispielsweise die Kenntnis eines Passworts oder eines kryptographischen Schlüssels überprüfen. Die anschließende Autorisierung kann beispielsweise über Zugriffskontrolllisten oder Rollen-basierte Zugriffskontrolle [7] realisiert werden.

Mechanismen zum Schutz personenbezogener Daten werden beim Privatkunden voraussichtlich eher im Gateway als zentrale Kommunikationskomponente umgesetzt werden. Auf dem Smart Meter könnten jedoch auch schon erste Mechanismen realisiert werden. So könnten Daten beispielsweise nicht sekundengenau sondern in größeren Abständen an das Gateway und darüber an weitere Rollen gesendet werden, um so Profilbildungen zu erschweren.

Referenzpunkt 3

Referenzpunkt 3 beschreibt die Kommunikation zwischen Smart Meter und Gateway. Hier können unterschiedliche drahtgebundene (z.B. M-Bus [9], Power Line Communication (PLC)[7]) oder drahtlose (z.B. Wireless M-Bus, Bluetooth, IEEE 802.15.4 Zigbee) Kommunikationstechnologien verwendet werden. Entsprechend der identifizierten Sicherheitsanforderungen sind bei dieser Kommunikation die übertragenen Messwerte gegen (Wieder-) Einspielen, Manipulation und Abhören zu schützen. Bei der Übertragung von Steuerdaten sowie Wartungsdaten für Smart

[7] z.B. nach IEEE 1901, HomePlug AV oder ITU-T G.hn

Meter sind Mechanismen zum Schutz gegen (Wieder-) Einspielen und Manipulationen ausreichend. Grundsätzlich sollte auch die Verfügbarkeit der gesamten Kommunikation in angemessenem Maße gegeben sein. Solange die Messwerte der Smart Meter nur zu Abrechnungszwecken genutzt werden, sind zwischenzeitliche Ausfälle jedoch kein größeres Problem. Falls jedoch Steuerungen im Verteilnetz auf Smart Meter Daten basieren, sind hier höhere Ansprüche an die Verfügbarkeit und die Aktualität der Daten zu stellen. Wobei auch hier das Ausbleiben von Daten einzelner Smart Meter keine größeren Auswirkungen haben sollten, da die Beeinflussung der Steuerungen durch einzelne Smart Meter eher gering. bzw. durch Messstellen des Verteilnetzbetreibers leicht kompensiert werden können. Derartige Messstellen könnten beispielsweise in Ortsnetzstationen oder Umspannwerke integriert werden. Die umzusetzenden Sicherheitsmechanismen sind somit:

- Mechanismen zum Schutz der Authentizität, Integrität und Vertraulichkeit der übertragenen Messwerte
- Mechanismen zum Schutz der Authentizität und Integrität der übertragenen Steuerdaten und Wartungsdaten
- Mechanismen zur Sicherstellung einer gewissen Verfügbarkeit der Kommunikation.

Zum Schutz der Authentizität, Integrität und Vertraulichkeit der Kommunikation zwischen Smart Meter und Gateway können beispielsweise die in die die jeweilige Technologie integrierten Sicherheitsmechanismen wie Verschlüsselungsverfahren direkt verwendet werden. So spezifiziert beispielsweise IEEE 802.15.4 Zigbee derartige Mechanismen und viele PLC Geräte haben ebenfalls entsprechende Mechanismen integriert. Aber auch bei einer direkten, kabelgebunden Verbindung zwischen Smart Meter und Gateway sollten die Daten geschützt werden. Eine kabelgebundene Verbindung ist zwar in der Regel etwas weniger bedroht, als eine drahtlose, dennoch sollten auch hier bekannte Techniken, wie digitale Signaturen, Zeitstempel, und Verschlüsselung eingesetzt werden, um Manipulationen und das Einschleusen falscher Messwerte sowie das Abhören durch Dritte zu verhindern.

Die Sicherstellung der Verfügbarkeit, insbesondere bei drahtloser Kommunikation, ist grundsätzlich schwierig zu realisieren. So gibt es gegen gezielte Jamming-Angriffe auf einen drahtlosen Kanal keine Schutzmöglichkeiten. Selbst bei kabelgebundener Kommunikation sind Angriffe auf die Verfügbarkeit nicht ausgeschlossen. So kann der Energienutzer selbst versuchen die Kommunikation zu stören, so dass keine Messwerte versendet werden und er seinen Stromverbrauch nicht bezahlen muss. Da man solche Angriffe nicht a priori verhindern kann, sollten diese zumindest a posteriori erkannt werden, indem, ähnlich zu Keep-alive-Signalen, regelmäßig Daten versendet werden und deren Ausbleiben eine Unterbrechung der Verbindung oder einen Ausfall des Kommunikationspartners anzeigt.

Die Verfügbarkeit der Kommunikation kann zudem durch nicht beabsichtige Störungen beeinträchtigt werden. Beispielsweise funkt IEEE 802.15.4 im Industrial, Scientific and Medical (ISM) Band in dem auch WLAN und Bluetooth senden, wodurch es zu Störungen (Interferenzen) kommen kann. Auch wenn diese Technologien Frequenzspreizverfahren wie Direct Sequence Spread Spectrum (DSSS) zur Erhöhung der Robustheit einsetzen, können Störungen auftreten und Daten verloren gehen. Dies muss auf Seiten des

Gateways erkannt werden und Daten sollten erneut gesendet werden.

Referenzpunkt 4

Die Sicherheitsmechanismen, die zur Absicherung von Gateways verwendet werden, sind die klassischen Verfahren, die auch zur Absicherung von Smart Metern zum Einsatz kommen können. Da jedoch an ein Gateway viele Smart Meter angebunden sein können, werden an Gateways höhere Sicherheitsstandards gestellt (vgl. BSI Schutzprofil für Smart Meter Gateways [2]). Als zentraler Verbindungspunkt des Privatkunden mit dem Energieversorger und aus Kostengründen bietet es sich an, Sicherheitsfunktionalitäten im Gateway zu bündeln. Somit ist insbesondere hier ein guter Schutz gegen Manipulationen des Systems notwendig und es muss sichergestellt werden, dass nur authentifizierte und autorisierte Rollen-Mitglieder auf das Gateway zugreifen können. Auch ist ein Gateway eine geeignete Komponente, um Datenschutz-Regeln durchzusetzen (Policy Enforcement Point). Es muss also Nutzern ermöglicht werden, individuelle oder aber auch standardisierte Regeln festzulegen, wie mit Daten umgegangen werden soll und wie bzw. unter welchen Bedingungen andere Rollen darauf zugreifen dürfen. Beispielsweise könnte ein Nutzer eine Regel spezifizieren, die besagt, dass die erfassten Messwerte zum einen anonymisiert und sekundengenau an den Verteilnetzbetreiber gesendet werden, zum anderen personenbezogen, aber aggregiert dem Energielieferanten zur Verfügung zu stellen sind. Der Verteilnetzbetreiber erhält so einen aktuellen Überblick über den derzeitigen Energiebedarf oder auch -überschuss des Energienutzers, der dafür günstigere Tarife erhält. Für den Energielieferanten sind aggregierten Daten zur Rechnungsstellung ausreichend. Weiterhin bietet es sich an, im Gateway Mechanismen umzusetzen, um geeignet auf Störungen der Kommunikation mit dem Energieversorger (vgl. Referenzpunkt 5) reagieren zu können. Wenn Störungen erkannt werden, können beispielsweise zu sendende Messwerte zwischengespeichert werden und wenn die Kommunikation wieder verfügbar ist gesendet werden.

Im Referenzmodell nicht dargestellt ist die Schnittstelle zu Komponenten der Heimautomatisierung, dem Smart Home, da dies nicht Fokus dieses Artikels ist. Denkbar ist in diesem Zusammenhang, dass aktuelle Verbrauchsdaten vom Gateway ins lokale Heimnetz gesendet werden, um dem Nutzer eine bequeme Verbrauchstransparenz zu ermöglichen. Hierzu wären ebenfalls geeignete Sicherheitsmechanismen zu realisieren.

Die umzusetzenden Sicherheitsmechanismen sind:

- Mechanismen zum Schutz gegen Manipulationen
- Mechanismen zur Authentifizierung und Autorisierung zugreifender Rollen
- Mechanismen zur Umsetzung von Datenschutz-Regeln
- Mechanismen zur Erkennung von Störungen der Kommunikation mit dem Energieversorger und Reaktion.

Die Umsetzung von Sicherheitsmechanismen für Gateways wird detailliert im BSI Schutzprofil [2] beschrieben. Dieses schreibt beispielsweise auch den Einsatz eines HSMs im Gateway vor, um, wie weiter oben bereits ausgeführt, Schutz gegen Manipulationen zu bieten. Für Smart Meter, die nicht in das Ga-

teway integriert sind, ist aber kein HSM vorgeschrieben. Die Authentifizierung und Autorisierung kann wie an Referenzpunkt 2 beschrieben erfolgen. Wie die Umsetzung von Datenschutz-Regeln geschehen kann und welche vertraglichen oder gesetzlichen Vorgaben einzuhalten sind, muss Gegenstand weiterer Forschung sein. Das BSI Schutzprofil beschreibt hierfür derzeit auch nur rudimentäre Anforderungen zum Einsatz von Mechanismen zum Schutz personenbeziehbarer Daten, wie z.B. Pseudonymisierung. Ein Datenschutz-Regelwerk könnte beispielsweise festlegen, dass sekundengenaue Messwerte nur pseudonymisiert gesendet werden dürfen. Die Einhaltung des Datenschutzes wird sich aller Voraussicht nach jedoch nicht ausschließlich am Gateway umsetzen lassen. Somit stehen auch Energieversorger bzw. die dort relevanten Rollen in der Pflicht sich datenschutzkonform zu verhalten. Dieser Aspekt wird an Referenzpunkt 6 diskutiert. Die Erkennung von Störungen kann beispielsweise mittels Keep-alive-Signalen erfolgen und als Reaktion werden, wie bereits oben erwähnt, Daten zwischengespeichert oder weitere organisatorische Maßnahmen getroffen werden.

Referenzpunkt 5

Referenzpunkt 5 beschreibt die Kommunikation zwischen Gateway und dem Energieversorger[8]. Diese Kommunikation erfolgt über einen oder mehrere Kommunikationsnetzbetreiber und kann über verschiedene, schon vorhandene Netze, erfolgen, z.B. Telefonnetz, DSL-Anschluss, Kabelnetz, Mobilfunk aber auch PLC oder Glasfaser (Fiber to the Home).

Vom Gateway werden die vom Smart Meter erfassten Messwerte und auch weitere Daten zur Abrechnung (z.B. die Annahme eines Tarifs) sowie ggf. Statusmeldungen an den Energieversorger gesendet. Zum Schutz der Authentizität, Integrität und Vertraulichkeit dieser Daten, müssen geeignete Mechanismen zur Absicherung der Kommunikation etabliert werden. Ggf. ist auch deren Verfügbarkeit und Aktualität wichtig, wenn diese, wie schon an Referenzpunkt 3 beschrieben, verwendet werden, um Steuerungen im Verteilnetz durchzuführen. Für empfangene Preisinformationen ist die Vertraulichkeit weniger relevant. Die Daten sollten aber verbindlich sein, damit sie im Nachhinein nicht abgestritten werden können. Für Steuerdaten ist neben deren Authentizität und Integrität auch deren Aktualität sicherzustellen, falls der Energieversorger Komponenten, die Energie-Verbraucher sind, entsprechend der verfügbaren Energie fernsteuert. Bei Wartungsdaten sind Mechanismen zum Schutz der Authentizität und Integrität ausreichend.

Die umzusetzenden Sicherheitsmechanismen sind somit:

- Mechanismen zum Schutz der Authentizität, Integrität, Vertraulichkeit und Aktualität der Messwerte, Daten zur Abrechnung und Statusmeldungen
- Mechanismen zum Schutz der Authentizität, Integrität, Verbindlichkeit und Aktualität von Preisinformationen
- Mechanismen zum Schutz der Authentizität, Integrität und Aktualität von Steuerdaten
- Mechanismen zum Schutz der Authentizität und Integrität von Wartungsdaten.

[8] Die relevanten einzelnen Rollen werden an Referenzpunkt 6 diskutiert.

Die Umsetzung von Sicherheitsmechanismen zum Schutz der Authentizität, Integrität und Vertraulichkeit der übertragenen Daten kann durch digitale Signaturen und Verschlüsselung, z.B. durch Verwendung von kryptographischen Protokollen wie IPsec oder über TLS abgesicherte HTTPS-Verbindungen (vgl. auch [4]), erfolgen.

Als Basis für die Sicherstellung der Aktualität der Daten müssen die verwendeten Kommunikationsverbindungen verfügbar sein. Je nach eingesetzter Technologie muss mit unterschiedlichen Qualitätsstufen hinsichtlich der Verfügbarkeit gerechnet werden. Wenn drahtlos, z.B. über Mobilfunk wie GSM oder UMTS kommuniziert wird, und Gateways zusätzlich noch in Kellerräumen mit meist schlechtem Empfang installiert sind, sollten häufige Störungen eingeplant werden. Auch beim Einsatz kabelgebundener Technologien wie Telefonnetz, DSL, PLC oder Glasfaser, die grundsätzlich eine höhere Zuverlässigkeit bieten [11], können Störungen nicht ganz ausgeschlossen werden. Somit muss damit gerechnet werden, dass Messwerte verzögert oder gar nicht beim Energieversorger oder aktuelle Preisinformationen und Verbrauchsdaten nicht beim Energienutzer eintreffen. Ebenso wie an Referenzpunkt 3 sollten Störungen zumindest erkannt werden und geeignete Maßnahmen getroffen werden. Auf Seiten des Privatkunden kann ein Ausbleiben von aktuellen Preisinformationen dazu führen, dass nicht der günstigste Tarif ausgewählt werden kann. Hier ist zu überlegen ob dies einfach in den seltenen Fällen akzeptiert wird oder sich geeignete organisatorische Maßnahmen finden lassen.

Referenzpunkt 6

Auf Seiten des Energieversorgers verarbeiten die Rollen Energielieferant, Verteilnetzbetreiber, Messdienstleister und Messstellenbetreiber Daten, die vom Energienutzer in der Privatkunden Domäne empfangen oder gesendet werden. Entsprechend sind auch auf Seiten des Energieversorgers Sicherheitsmechanismen zur Datensicherheit und zum Datenschutz umzusetzen und es sind entsprechende Vorschriften und Gesetze wie z.B. das Bundesdatenschutzgesetz (BDSG) einzuhalten. Die Daten müssen hierbei sowohl in den datenverarbeitenden Systemen als auch beim Austausch zwischen den Rollen geschützt werden.

Um Datenschutz Anforderungen zu erfüllen, muss sichergestellt werden, dass die Mitglieder der Rollen Messdienstleister und Energielieferant die Daten, wie Abrechnungsdaten, Verbrauchsdaten oder auch andere personenbezogene Daten vertrauenswürdig, korrekt und rechtzeitig verarbeiten, speichern und nur an autorisierte Dritte entsprechend definierter Datenschutz-Regeln weiterleiten. Die Weitergabe von Daten an den Verteilnetzbetreiber sollte nur aggregiert und/oder anonymisiert erfolgen. Grundsätzlich sollten bei der Verarbeitung und Weitergabe personenbezogenen Daten die Prinzipien der Datensparsamkeit, Zweckbindung, Erforderlichkeit, Transparenz, Mitwirkung und Kontrolle beachtet werden [22].

Eine vertrauenswürdige, korrekte und rechtzeitige Verarbeitung sowie deren Weitergabe ist grundsätzlich für alle Daten wichtig. So muss der Messdienstleister die Messwerte korrekt verarbeiten und weiterleiten, um eine korrekte Abrechnung durch den Energielieferanten auf Basis der Preisinformationen zu ermöglichen. Für den Verteilnetzbetreiber ist

die Verarbeitung von korrekten Daten ebenfalls wichtig, um beispielsweise Steuerungen oder Planungen seines Netzes durchzuführen. Auch beim Messstellenbetreiber ist eine vertrauenswürdige und korrekte Datenverarbeitung notwendig, um sicherzustellen, dass keine manipulierten oder fehlerhaften Updates und Patches auf Smart Metern und Gateways installiert, oder auf Basis falscher Steuerdaten inkorrekte Steuerungen durchgeführt werden.

Zur Sicherstellung der Versorgungssicherheit muss der Energieversorger neben den bereits erwähnten Mechanismen der IT-Sicherheit auch weitere, organisatorische Maßnahmen ergreifen. Wenn beispielsweise Daten über den aktuellen Strombedarf ausbleiben, darf das Gesamtsystem nicht zusammen brechen. Hierfür müssen entsprechende Maßnahmen vorgesehen sein.

Grundsätzlich sind die umzusetzenden Sicherheitsmechanismen:

- Mechanismen zur Sicherstellung der vertrauenswürdigen, korrekten und rechtzeitigen Verarbeitung, Speicherung und Weitergabe von Messwerten, Daten zur Abrechnung, aktuellen Verbrauchsdaten und Rechnungsdaten, Preisinformationen, Steuerdaten, Statusdaten, Wartungsdaten
- Weitere organisatorische Maßnahmen zur Sicherstellung der Versorgungssicherheit.

Zur Umsetzung des ersten Punkts müssen zum einen die Systeme und zum anderen die Kommunikation zwischen den einzelnen Systemen abgesichert werden. Zum Schutz der Systeme selbst sind klassische IT-Sicherheitsmechanismen wie z.B. Zugangskontrollen, oder Patchmanagement zu realisieren (vgl. [4]), wie sie auch bei jedem anderen IT-System vorzusehen sind. Bei der Umsetzung kann man sich z.B. an den IT-Grundschutz-Katalogen des BSI [23] orientieren, soweit der Schutzbedarf niedrig ist. Die Absicherung der Kommunikation zwischen den verschiedenen Systemen der beteiligten Rollen kann ähnlich wie zuvor beschrieben erfolgen.

Maßnahmen zur Sicherstellung der Versorgungssicherheit betreffen insbesondere den Verteilnetzbetreiber. Diese Domäne wird detailliert in nachfolgendem Kapitel betrachtet. Entsprechende Maßnahmen müssen über die reinen IT-Sicherheitsmaßnahmen hinausgehende Techniken umfassen, wie spezielle organisatorische Maßnahmen, Redundante Auslegungen von Infrastrukturen, um Fehler zu kompensieren, oder auch die Verwendung von Prognosedaten, falls aktuelle Daten nicht ausreichen, um Steuerungen durchzuführen. Wenn beispielsweise aktuelle (aggregierte oder anonymisierte) Messwerte ausbleiben (als Folge eines gezielten Angriffs oder einer Störung), können Prognosedaten verwendet werden, um dies zu kompensieren. Auch können redundante Messstellen z.B. an Ortsnetzstationen oder Umspannwerken installiert werden, die aggregierte Messwerte einzelner Netzabschnitte liefern. Diese Messwerte könnten zum einen verwendet werden, falls Messwerte vieler Smart Meter ausbleiben. Zum anderen könnten diese Daten auch genutzt werden, um Plausibilitätschecks durchzuführen. Dadurch kann verhindert werden, dass eine Vielzahl an manipulierten Smart Metern durch das Senden falscher Verbrauchsdaten den Verteilnetzbetreiber zu Fehlsteuerungen verleiten, welche zu Störungen und Ausfällen führen.

Referenzpunkt 7

Referenzpunkt 7 beschreibt die Kommunikation zwischen Energieversorger und Energienutzer, um diesem Daten, wie die aktuellen Verbrauchsdaten, Preisinformationen und Rechnungsdaten, zu Informationszwecken zur Verfügung zu stellen. Diese Daten werden über das Internet an den Energienutzer gesendet. Da es sich, mit Ausnahme der Preisinformationen, um personenbezogene Daten handelt, müssen bei der Übertragung neben Mechanismen zur Sicherstellung der Authentizität und Integrität auch Mechanismen zur Wahrung der Vertraulichkeit etabliert werden. Da diese Daten rein informativ sind und im Gegensatz zu den Daten am Referenzpunkt 5 keine Reaktionen nach sich ziehen, ist hier die Aktualität der Daten von geringer Relevanz

Die umzusetzenden Sicherheitsmechanismen sind somit:

- Mechanismen zum Schutz der Authentizität, Integrität und Vertraulichkeit von Rechnungsdaten und aktuellen Verbrauchsdaten
- Mechanismen zum Schutz der Authentizität und Integrität von Preisinformationen.

Als Mechanismen zum Schutz der Authentizität, Integrität und Vertraulichkeit bei der Übertragung über das Internet bieten sich auch hier über TLS abgesicherte HTTPS-Verbindungen an. Rechnungsdaten könnten alternativ auch PGP-verschlüsselt per Email an den Energienutzer gesendet werden.

4 Verteilnetz

Ein Verteilnetz wird von einem Verteilnetzbetreiber (engl. Distribution System Operator (DSO)) betrieben und unterhält Stromnetze im Nieder- und Mittelspannungs-Bereich. Da ein großer Teil der Energie verbrauchenden Geräte Niederspannungsgeräte in den privaten Haushalten sind, stellen die Niederspannungsnetze die zentralen Energieverteilnetze für die Domäne Privathaushalt dar. An Niederspannungsnetze werden einphasige Geräte angeschlossen. In Mitteleuropa werden solche Niederspannungsnetze üblicherweise mit Spannungen zwischen 230 V / 400 V (einphasig / dreiphasig) und 1000 V betrieben (siehe auch Tabelle 1). Derartige Netze sind in der Regel räumlich begrenzt und überspannen einen Bereich von einigen 100 m bis zu einigen wenigen Kilometern. Diese räumliche Beschränkung ist notwendig, um Spannungsverluste zu vermeiden. Üblicherweise bestehen Niederspannungsnetze aus mehreren Kabelsträngen, die einzelne Häuser oder Häusergruppen in räumlich naher Umgebung in einer sternförmigen Topologie versorgen. Im Haus erfolgt die Unterverteilung ebenfalls in der Regel sternförmig zu den Steckdosen und sonstigen Verbrauchern. Niederspannungsnetze werden über regionale Transformatorenstationen aus einem Mittelspannungsnetz bzw. von einem Übertragungsnetzbetreiber (engl. Transmission System Operator, (TSO)) versorgt.

Ein Übertragungsnetzbetreiber erhält Strom von großen Erzeugern wie Kohle- oder Atomkraftwerken und überträgt den Strom über große Entfernungen in Hochspannungsnetzen. Ein Verteilnetzbetreiber kann aber auch selbst Strom erzeugen, z.B. durch eigene Windparks oder Blockheizkraftwerke. Üblicherweise gehören Verteilnetzbetreiber zu einem lokalen bzw. kommunalen Energieversorgungsunternehmen wie einem Stadtwerk. In Deutschland werden Verteilnetze von über 720 Stadtwerken, ca. 70 regionalen Netzbetreibern und über 100 privaten Versorgern betrieben [11]. Eine detaillierte Einführung in Verteilnetze findet sich in [12].

Tabelle 1 aus [11] gibt einen Überblick über die wichtigsten Charakteristika der Stromnetze in Deutschland.

In zukünftigen Smart Grids wird erwartet, dass sowohl zwischen den Komponenten und Mitglieder, die sich innerhalb eines Verteilnetzes befinden, als auch mit Mitgliedern weiterer Rollen erheblich mehr als jetzt kommuniziert werden muss, um den Netzbetrieb

Netzbereich	**Abkürzung**	**Spannung**	**Reichweite**	**Gesamtentfernung in Deutschland**
Höchstspannungsnetz	HÖS	220 kV oder 380/400 kV	unbegrenzt	36.000 km
Hochspannungsnetz	HS	max. 110 kV	10 – 100 km	75.000 km
Mittelspannungsnetz	MS	max. 36 kV	1 – 50 km	500.000 km
Niederspannungsnetz	NS	230 V / 400 V	< 2 km	1.000.000 km

Tabelle 1: Netzbereiche in Deutschland [11]

zu optimieren und Steuerungen wie Lastflusssteuerung oder Netzüberwachungen durchzuführen. Derzeit wird im Verteilnetz noch überwiegend manuell gesteuert und in vielen Bereichen kommt man derzeit noch ohne Kommunikation aus. So agieren beispielsweise Ortsnetzstationen meist autonom. Durch die ansteigende Nutzung von erneuerbaren Energien ist aber zu erwarten, dass sich dies in Zukunft ändern wird.

In diesem Kapitel wird zunächst ein kurzer Überblick über die Domäne der Verteilnetze gegeben, indem zunächst die beteiligten Rollen und eine typische Netztopologie vorgestellt werden. Anschließend werden wieder repräsentative Anwendungsfälle, die sich ergebenden Sicherheitsanforderungen der einzelnen Rollen und eine mögliche Sicherheitsarchitektur beschrieben.

4.1 Grundlagen

Im Verteilnetz sind die folgende Rollen relevant (vgl. auch [12]): Verteilnetzbetreiber, Produzent, Kommunikationsnetzbetreiber, Übertragungsnetzbetreiber, Energielieferant, Messdienstleister, Energienutzer und Messstellenbetreiber. Abbildung 5 stellt die Zusammenhänge zwischen den einzelnen Rollen graphisch dar. Der Fokus liegt dabei auf dem Verteilnetzbetreiber. Nicht direkt relevante Beziehungen werden zur besseren Übersicht nicht dargestellt.

Der *Verteilnetzbetreiber* betreibt, wie bereits oben erwähnt, Niederspannungsnetze bzw. Mittelspannungsnetze auf regionaler Ebene und sorgt für die Stromversorgung der Endverbraucher, d.h. er liefert Energie an den Energienutzer. In Zukunft wird es zur Steuerung von Verteilnetzen zu einer vermehrten Kommunikation kommen. So müssen zur

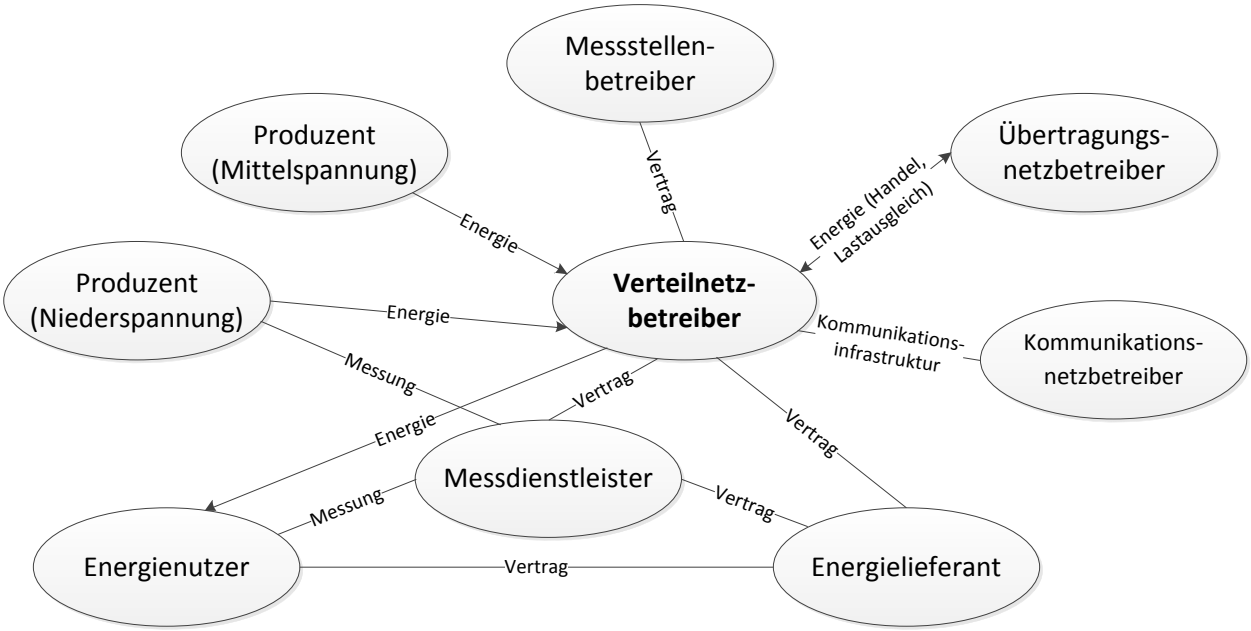


Abbildung 5: Rollen in der Domäne Verteilnetz und deren Beziehungen

Überwachung und Steuerung Messwerte und Statusdaten erfasst und übertragen werden sowie mittels Steuerdaten Steuerungen durchgeführt werden. Dies muss zum einen innerhalb des Verteilnetzes erfolgen, z.B. zur Überwachung und Steuerung von Ortsnetzstationen oder Umspannwerken. Zum anderen werden auch mit anderen Rollen vermehrt Daten ausgetauscht werden müssen, um die Verteilnetze versorgungssicher zu betreiben. Hierzu können z.B. Energieverbraucher ferngesteuert werden, um den Verbrauch an das Angebot anzupassen (vgl. Kapitel 3.1), wofür entsprechende Steuerdaten übertragen werden müssen.

Mit dem *Übertragungsnetzbetreiber* findet sowohl Kommunikation zur Herstellung eines Lastausgleichs als auch zur Abwicklung des Energiehandels statt. Hierzu werden Daten, wie das aktuelle Angebot und die aktuelle Nachfrage nach Energie, sowie Abrechnungsdaten auszutauschen sein. Der Übertragungsnetzbetreiber ist mit Produzenten verbunden, die mittels Großkraftwerken in das Höchstspannungsnetz einspeisen. Eine direkte Verbindung zwischen Verteilnetzbetreiber und Produzenten auf Höchstspannungsebene gibt es somit nicht.

Die *Produzenten,* mit denen der Verteilnetzbetreiber kommuniziert, sind verantwortlich dafür, Energie ins Niederspannungsnetz oder ins Mittelspannungsnetz des Verteilnetzbetreibers einzuspeisen. Dies kann beispielsweise ein Prosumer sein, der mittels einer Photovoltaikanlage ins Niederspannungsnetz einspeist. Falls der Verteilnetzbetreiber ein überregionales Verteilnetz mit eigenen Erzeugungsanlagen betreibt, wird auch mit diesen Produzenten, die ins Hochspannungsnetz einspeisen, kommuniziert. Hier müssen ebenfalls Messwerte über die eingespeiste Energie und ggf. weitere Statusdaten übertragen werden. Auch wird der Verteilnetzbetreiber eigene Energieerzeugungsanlagen überwachen und steuern und hierzu Steuerdaten sowie Statusdaten übertragen. Eventuell werden auch Prognosedaten über die erwartete Energiekapazität übertragen. Dies ist insbesondere für die Erzeugung mittels erneuerbarer Energien relevant.

Der *Energienutzer* wird durch den Verteilnetzbetreiber mit Energie versorgt. Eine direkte Kommunikation findet nur statt, wenn der Energienutzer direkt einen Vertrag mit dem Verteilnetzbetreiber zur Lieferung von Energie hat (vgl. Kapitel 3.1). Üblicherweise findet die Kommunikation aber mit dem Energielieferanten und Messdienstleister statt.

Der *Energielieferant* hat einen Vertrag mit dem Energienutzer über Lieferung von Energie. Hierzu müssen Messwerte, weitere Daten zur Abrechnung und Rechnungsdaten ausgetauscht werden.

Der *Messdienstleister* erfasst den Energieverbrauch des Energienutzers mit Hilfe der Smart Meter. Die (ggf. aggregierten) Messwerte stellt er dem Energielieferanten zur Abrechnung zur Verfügung. Auch wird die erzeugte Energie erfasst, die ein Prosumer ins Niederspannungsnetz einspeist. Diese Messwerte sowie weitere Statusdaten können in Zukunft auch dem Verteilnetzbetreiber zur Verfügung gestellt werden, so dass dieser diese Daten nutzen kann, um sein Netz bestmöglich zu betreiben. Wie bereits in Kapitel 3 diskutiert, sollten die Messwerte aus Datenschutzgründen entweder aggregiert (z.B. auf Netzabschnitte) oder anonymisiert bzw. pseudonymisiert sein.

Der Verteilnetzbetreiber hat einen Vertrag mit dem *Messstellenbetreiber*, der für den Verteilnetzbetreiber Messstellen installiert und

Wartungsarbeiten vornimmt, um beispielsweise Störungen zu beseitigen. Zwischen ihnen müssen Rechnungsdaten für die Installation und Betrieb ausgetauscht werden. Weiterhin ist denkbar, dass weitere Daten über durchgeführte oder durchzuführende Arbeiten wie z.B. ein Zählerwechsel ausgetauscht werden.

Zur Kommunikation mit den anderen Rollen und zur Kommunikation mit den einzelnen Systemen innerhalb des Verteilnetzes werden dem Verteilnetzbetreiber durch einen oder mehrere *Kommunikationsnetzbetreiber* entsprechende Kommunikationsinfrastrukturen bereitgestellt.

Die Rollen *Bilanzkreiskoordinator* und *Bilanzkreisverantwortlicher* sind nötig, um alle tatsächlichen Einspeisungen und Entnahmen innerhalb eines Regelgebiets zu saldieren. Diese Rollen wurden durch die freie Wahlmöglichkeit eines Energielieferanten unabhängig vom Netzbetreiber nötig, um die vom Lieferanten durch ein fremdes Netz geleitete Energie abzurechnen. Hierzu werden virtuelle Energiemengenkonten sogenannte Bilanzkreise gebildet, in denen z.B. ein Energielieferant alle seine Einspeise- und Entnahmestellen innerhalb einer Regelzone sowie Fahrplanlieferungen von und zu anderen Bilanzkreisen zusammenfasst. Dieser agiert dann in der Rolle Bilanzkreisverantwortlicher und ein Übertragungsnetzbetreiber in der Rolle Bilanzkreiskoordinator. Der Verteilnetzbetreiber liefert an den Bilanzkreiskoordinator aggregierte Messdaten über Einspeisung bzw. Entnahme je Bilanzkreis. Mit dem Bilanzkreisverantwortlichen (und anderen Energielieferanten) werden ebenfalls aggregierte Messdaten über Einspeisung bzw. Entnahme je Bilanzkreis sowie Daten zur An-, Ab- oder Ummeldung von Kunden ausgetauscht. Im Folgenden wird auf diese Rollen nicht weiter eingegangen, da der Fokus dieses Artikels auf den Domänen Privatkunde und Verteilnetz liegt.

Ebenfalls nicht betrachtet werden die möglicherweise relevanten Rollen *Gebäudeautomations-Anbieter* und *weitere Energiedienstleister,* da zurzeit noch nicht klar ist, wie diese in Smart Grids eingebunden werden.

Jeder der genannten Rollen sind in Smart Grids bestimmte Aufgaben und Pflichten zugeordnet. Zur Erfüllung dieser Aufgaben benötigen die Rollen Daten und Informationen, auch um zum Beispiel im Zusammenspiel mit anderen Rollen anderer Domänen ihren Verpflichtungen zur Aufrechterhaltung der Versorgungssicherheit gerecht zu werden. Es ist deshalb unumgänglich zu analysieren, welche Daten bzw. Informationen für die verschiedenen Aufgaben bzw. Anwendungsfällen von den beteiligten Rollen benötigt werden, welche Daten zwischen wem ausgetauscht werden müssen, ob dies eine zeitkritische Kommunikation ist, und welche Daten ggf. mittel- bis langfristig archiviert werden müssen. Im Zuge der Analyse sind die Anforderungen an die Informationssicherheit und den Datenschutz der von den Rollen verarbeiteten Daten zu erfassen. Analog zu Kapitel 3 wird deshalb im Folgenden eine solche Analyse anhand einer angenommenen Referenzarchitektur und relevanter Anwendungsfällen durchgeführt.

Eine mögliche Referenzarchitektur der Netztopologie der Domäne Verteilnetz und deren Anbindung an das Übertragungsnetz und an Energienutzer wie Privatkunden sind in Abbildung 6 dargestellt. Die Abbildung beschreibt die funktionalen Elemente im Verteilnetz und die Strom bzw. Datenverbindungen darin. Das Verteilnetz ist an das Übertragungsnetz angeschlossen und bezieht von

dort Strom, der von Produzenten in Großkraftwerken erzeugt wird. Betreibt der Verteilnetzbetreiber ein überregionales Verteilnetz, so wird der über Höchstspannungsnetze empfangene Strom zunächst in einem *Umspannwerk* auf Hochspannung transformiert. Zur Transformation zwischen den verschiedenen Spannungsebenen der Höchst-, Hoch- und Mittelspannung betreibt der Verteilnetzbetreiber verschiedene *Umspannwerke* und zur Transformation zwischen der Mittelspannungsebene und der Niederspannungsebene betreibt er *Ortsnetzstationen* (Trafostationen).

In Zukunft werden viel mehr verteilte *Erzeuger* auf den verschiedenen Spannungsebenen an das Verteilnetz angebunden sein. Dies umfasst mittlere Erzeuger wie On-shore Windparks, kleine Erzeuger wie Geothermie oder Biogasanlagen, sowie kleinste Erzeugungsanlagen wie Photovoltaikanlagen beim Privatkunden oder Blockheizkraftwerke. Zum Ausgleich von Schwankungen in der Verfügbarkeit der Energie können *Speicher* auf den verschiedenen Spannungsebenen eingesetzt werden. *Verbraucher* sind auf Mittelspannungsebene meist Industriebetriebe und auf Niederspannungsebene Privatkunden oder kleine Gewerbebetriebe.

Die Kommunikation findet zentral mit einer *Netzleitstelle* statt. Derzeit existieren Kommunikationsbeziehungen vorwiegend zwischen Umspannstationen und der Leitstelle. Dagegen arbeiten die Ortsnetzstationen in der Regel autonom ohne Kommunikation. Hier ist aber im Zuge des Ausbaus von Smart Grids zu erwarten, dass auch Ortsnetzstationen kommunizieren werden. Die Kommunikation umfasst die Überwachung, Steuerung und Wartung der Anlagen wozu Messwerte, Steuerdaten sowie Wartungsdaten ausgetauscht werden können. Die Kommunikation mit den Verbrauchern umfasst den Austausch von Messwerten, aktuellen Verbrauchsdaten, Preisinformationen, Steuerdaten, Wartungsdaten etc. Mit Erzeugern müssen Messwerte zur Abrechnung, Statusdaten, Steuersignale zur Überwachung und Steuerung sowie Wartungsdaten zur Wartung ausgetauscht werden. Mit Energie-Speichern werden ebenfalls Messwerte zur Abrechnung ausgetauscht, sowie Statusdaten z.B. zur Anzeige der verfügbaren Speicherkapazität oder gespeicherten Energie. Speicher können beispielsweise auch angeschlossene Elektrofahrzeuge sein (vgl. Kapitel 5).

Zur besseren Übersichtlichkeit sind in Abbildung 6 einige Kommunikationsbeziehungen vereinfacht dargestellt. So wird aufgrund der gesetzlich vorgeschriebenen Rollentrennung beispielsweise die Leitstelle des Verteilnetzbetreibers keine Messwerte der Smart Meter direkt erhalten, sondern diese über den Messdienstleister, der diese Daten ggf. aggregiert oder anonymisiert (vgl. Kapitel 3), empfangen.

Die in Abbildung 6 dargestellte Architektur mit einer zentralen Leitstelle wird für die nahe Zukunft als am Wahrscheinlichsten angesehen [12]. In Zukunft ist grundsätzlich ebenfalls denkbar, dass es auch eine direkte Kommunikation zwischen Systemen geben wird, z.B. zwischen Smart Metern und Ortsnetzstationen zur direkten (automatisierten) Steuerung von Ortsnetzstationen basierend auf den empfangenen Messwerten der angebundenen Smart Meter. Beim Entwurf von Sicherheitsarchitekturen sollten solche Möglichkeiten von Beginn an berücksichtigt werden.

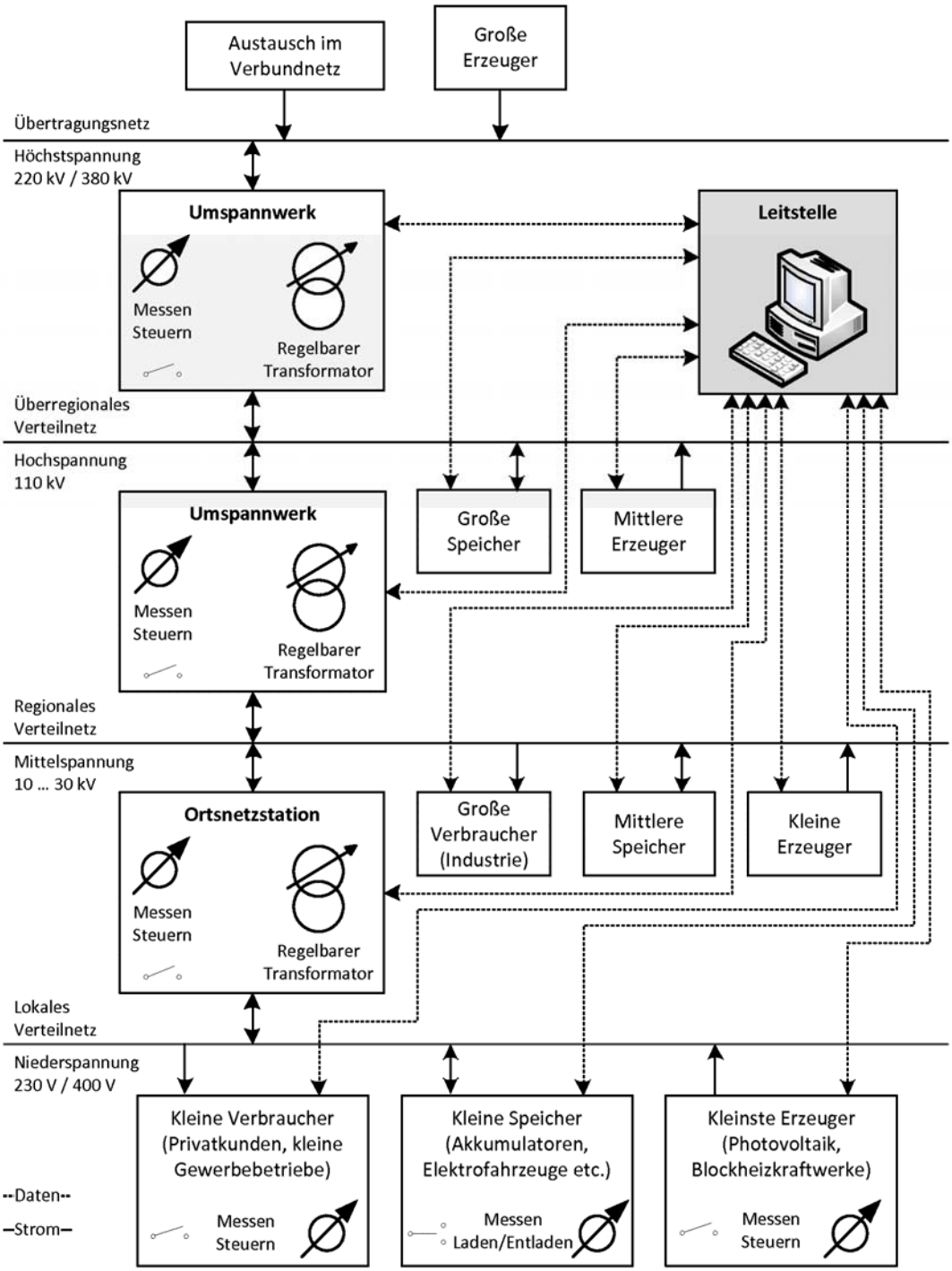


Abbildung 6: Repräsentative Topologie der Domäne Verteilnetz

4.2 Anwendungsfälle

Da die beiden Domänen Privatkunde und Verteilnetz direkt zusammen hängen, sind die in Kapitel 3.2 beschriebenen Anwendungsfälle größtenteils ebenfalls für die Domäne Verteilnetz relevant. So sind die erfassten Messwerte beim Anwendungsfall *Messwerterfassung* für den Verteilnetzbetreiber interessant, um seinen Netzbetrieb zu optimieren. Hier müssen jedoch bei der Entwicklung der Sicherheitsarchitektur die Sicherheitsanforderungen der bislang noch nicht betrachteten Rollen berücksichtigt werden. Hierzu gehören z.B. die Datenschutzanforderungen des Privatkunden.

Der Anwendungsfall *Fernanschaltung / Fernabschaltung* von Smart Metern ist für den Verteilnetzbetreiber insofern interessant, dass er aufgrund der Informationen, die er vom Messstellenbetreiber über die Art und Anzahl der angeschlossenen Kunden erhält, Lastprofile zur Prognose des Energiebedarfs erstellen kann.

Beim Anwendungsfall *Erkennung und Behandlung von Ausfällen* erhält der Verteilnetzbetreiber Informationen über Ausfälle in seinem Netz, um entsprechend reagieren zu können.

Der Anwendungsfall *Wartung* ist nur insofern interessant, dass Smart Meter und Gateways korrekt funktionieren und die erhaltenen (aggregierten oder anonymisierten) Messwerte korrekt sind.

Durch den Anwendungsfall *Echtzeit Tarifierung* soll das Nutzungsverhalten des Kunden durch Preisanreize entsprechend der verfügbaren Energie im Verteilnetz gesteuert werden. Für den Verteilnetzbetreiber ist dieser Anwendungsfall somit besonders wichtig, um die Nachfrage an das Angebot anzupassen und Schwankungen in der Energieversorgung auszugleichen.

Neben diesen Anwendungsfällen werden nachfolgend noch zwei weitere Anwendungsfälle speziell aus Sicht des Verteilnetzes vorgestellt. Im ersten Anwendungsfall *Einspeisen von Energie* werden die Auswirkungen von verteilt eingespeister Energie in das Verteilnetz betrachtet. Der zweite Anwendungsfall *Steuerung und Überwachung* betrachtet die Überwachung und Steuerung von (gewerblichen bzw. industriellen) Energieverbrauchern und Systemen innerhalb des Verteilnetzes. Es werden jeweils wieder die beteiligten Rollen und Daten, die die Rollen zur Erfüllung ihrer Aufgaben benötigen werden, beschrieben.

Basierend auf diesen und den in Kapitel 3.2 beschriebenen Anwendungsfällen werden in Kapitel 4.3 die Sicherheitsanforderungen der einzelnen Rollenabgeleitet.

Use-Case: Einspeisen von Energie

Dieser Anwendungsfall wurde aus Sicht des Privatkunden prinzipiell schon in Kapitel 3.2 im Anwendungsfall *Messwerterfassung* beschrieben. Der Privatkunde kann Energie, die in installierten Erzeugungsanlagen erzeugt wurde, oder die in Speichern, wie den Batterien von Elektrofahrzeugen gespeichert wurde, in das Verteilnetz einspeisen. Die Erfassung der Messwerte über die eingespeiste Energie erfolgt, wie im Anwendungsfall *Messwerterfassung* beschrieben, über Smart Meter. Der Verteilnetzbetreiber kann aber auch selbst mittels eigener Erzeugungsanlagen Energie erzeugen und in sein Verteilnetz einspeisen.

Für das Netzmanagement, die Abrechnung und auch die Wartung ist die Erfassung und

Kommunikation von Informationen zur Energienutzung, -erzeugung und -speicherung notwendig. Diese Informationen sind insbesondere für den Verteilnetzbetreiber für das Netzmanagement wichtig, um die Versorgungssicherheit zu gewährleisten. So müssen beispielsweise für die einzelnen Netzsegmente (aggregierte) Messwerte z.B. durch den Messdienstleister oder eigene Messstellen im Verteilnetz über Energieverbrauch und durch Energieerzeuger und Speicher eingespeiste Energie erfasst werden. Auch müssen (ggf. aggregierte) Statusinformationen zu verfügbaren Erzeugungsressourcen, gespeicherten Energien, verfügbaren Speicherkapazitäten etc. erfasst werden. Basierend auf diesen Daten kann der Verteilnetzbetreiber dann entsprechende Steuerungen in den einzelnen Netzsegmenten seines Verteilnetzes vornehmen, um auf Spitzen in Angebot und Nachfrage zu reagieren.

Use Case: Steuerung und Überwachung

Dieser Anwendungsfall nutzt die im vorherigen Anwendungsfall erfassten Daten zur Steuerung und Überwachung von Komponenten. In Smart Grids werden wesentlich mehr Komponenten als in heutigen Netzen gesteuert werden, um mit der dezentralen Einspeisung umzugehen und entsprechend dem Angebot und der Nachfrage das Verteilnetz und angeschlossene Verbraucher zu steuern. Für die beiden Fälle: (1) Steuerung des Verteilnetzes selbst und (2) Steuerung von Verbrauchern müssen Messwerte, Statusdaten etc. erfasst und übertragen werden und mittels Steuerdaten die Steuerungen oder Regelungen durchgeführt werden. Zum Erfassen von Messwerten könnten sowohl Smart Meter in Privathaushalten als auch Messstellen an Subsystemen des Verteilnetzes wie Ortsnetzstationen, Umspannwerken, Kraftwerken und Speichern, sowie an Übergangsstellen zum Übertragungsnetz verwendet werden.

Im ersten Fall werden vom Verteilnetzbetreiber Steuerdaten an Systeme innerhalb des Verteilnetzes gesendet, um z.B. Steuerungen oder Regelungen des Lastflusses vorzunehmen. Damit kann beispielsweise bei einem Überschuss an Energie diese Überkapazität in lokalen Speichern zwischen gespeichert werden und Ausfälle von Komponenten können kompensiert werden. Um diese Steuerungen durchführen zu können, benötigt der Verteilnetzbetreiber, wie im Anwendungsfall *Einspeisen von Energie* beschrieben, Messwerte und weitere Statusdaten. Auch hier sind meist aggregierte Daten oder Daten, die nur Änderungen beschreiben, ausreichend. In der Sicherheitsarchitektur lässt sich bei diesem Anwendungsfall somit der Datenschutz leicht realisieren. Ein weiterer Vorteil dieser Datensparsamkeit, indem keine detaillierten Daten gesendet werden, ist die geringere Datenmenge, die sich beispielsweise effizient signieren lässt.

Der zweite Fall umfasst die entfernte Steuerung von Verbrauchern und ggf. Speichern und Erzeugern. Wie in den Kapiteln 3.1 und 3.2 beschrieben, kann dies entweder indirekt, z.B. über Preisanreize, oder direkt erfolgen, wobei die direkte Steuerung primär im industriellen oder gewerblichen Umfeld zu erwarten ist.

4.3 Sicherheitsanforderungen

Bei der Betrachtung der Sicherheitsanforderungen der einzelnen Rollen werden wieder die in Kapitel 3.3 beschriebenen Daten *Messwerte*, *Daten zur Abrechnung*, *aktuelle Verbrauchsdaten*, *Preisinformationen*, *Rechnungsdaten*, *Steuerdaten*, *Wartungsdaten*, *Statusdaten* sowie *weitere Daten* berücksichtigt, da diese auch im Verteilnetz relevant sind. Im Verteilnetz werden einige dieser Daten jedoch andere Formen haben, z.B. können Steuerdaten sowie Statusdaten von Ortsnetzstationen oder Umspannwerken Daten aus SCADA-Netzen sein.

Für die Sicherheitsanforderungen der Rollen *Kommunikationsnetzbetreiber*, *Energielieferant*, *Messdienstleister* und *Messstellenbetreiber* ergeben sich keine Änderungen im Vergleich zu Kapitel 3.3. Im Folgenden werden deshalb nur die Sicherheitsanforderungen der 4 Rollen *Verteilnetzbetreiber*, *Energienutzer*, *Produzent* und *Übertragungsnetzbetreiber* beschrieben.

(1) Rolle: Verteilnetzbetreiber

Zusätzlich zu den in Kapitel 3.3 beschriebenen Sicherheitsanforderungen muss die Authentizität, Integrität, Verfügbarkeit und Aktualität sowohl von Statusdaten von Systemen beim Kunden als auch von Systemen im Verteilnetz gewährleistet werden. Damit wird sichergestellt, dass die Daten von der besagten Stelle stammen, während der Übertragung nicht verändert wurden und rechtzeitig eintreffen. Um zu gewährleisten, dass die empfangenen Daten auch von einem vertrauenswürdigen System stammen, welches nicht manipuliert wurde, ist weiterhin die Integrität der Systeme, also von IKT-Komponenten von Energie-Speichern, -Erzeugern, Ortsnetzstationen, Umspannwerken etc. sicherzustellen. Bei der Umsetzung dieser Anforderungen ist zu beachten, dass die Schutzanforderungen für die Systeme im Verteilnetz wesentlich höher sind als in der Domäne Privatkunde, da deren Ausfall wesentlich schwerwiegendere Folgen hätte als die Störung der Versorgung eines einzelnen Kunden.

Zusammengefasst umfassen die Sicherheitsanforderungen für den Verteilnetzbetreiber:

- Versorgungssicherheit im vertraglich zugesicherten Umfang
- Authentizität, Integrität, Verfügbarkeit und Aktualität von Preisinformationen, Steuerdaten, Statusdaten
- Authentizität und Integrität von aggregierten oder anonymisierten Messwerten und Daten zur Abrechnung
- Integrität der Systeme von Smart Metern, Gateways, Speichern, Erzeugern, Ortsnetzstationen, Umspannwerken etc.
- Authentizität und Integrität von Wartungsdaten.

(2) Rolle: Energienutzer

Für den Energienutzer ergeben sich zusätzlich zu den in Kapitel 3.3 beschriebenen Sicherheitsanforderungen noch die Anforderungen nach Authentizität, Integrität und Vertraulichkeit von Statusdaten von Systemen beim Kunden, um eine korrekte Abrechnung und den Datenschutz sicherzustellen. Zum Schutz gegen Manipulationen muss ebenfalls die Integrität der IKT-Systeme von Energie-Speichern und -Erzeugern gewährleistet sein.

Zusammengefasst sind die Sicherheitsanforderungen für den Energienutzer:

- Vertraulichkeit und Datenschutz (bzw. nutzerkontrollierbare Weitergabe) von Messwerten, Daten zur Abrechnung, aktuellen Verbrauchsdaten, Rechnungsdaten, Statusdaten
- Authentizität und Integrität von Messwerten, Daten zur Abrechnung und Statusinformationen von Systemen beim Kunden
- Authentizität, Integrität, Aktualität und Verbindlichkeit von Preisinformationen
- Integrität der Systeme von Smart Metern, Gateways, Speichern, Erzeugern etc.
- Authentizität und Integrität von Steuerdaten, Wartungsdaten
- Versorgungssicherheit.

(3) Rolle: Produzent

Energie-Produzenten, die auf unterschiedlichen Spannungsebenen angesiedelt sind, möchten ihren produzierten Strom korrekt abgerechnet haben und dabei einen möglichst hohen Gewinn erzielen.

Für die Abrechnung müssen Messwerte über den verbrauchten Strom sowie ggf. weitere Daten zur Abrechnung korrekt erfasst, weitergeleitet und verarbeitet werden. Somit muss die Authentizität und Integrität von Messwerten und Daten zur Abrechnung über alle datenverarbeitenden Systeme gewährleistet sein.

Durch wechselnde Preise kann ein Produzent versuchen, seinen erzeugten Strom zu einem möglichst hohen Preis zu verkaufen. Dies ist beispielsweise für einen Prosumer auf Niederspannungsebene interessant, der Strom in Hochpreiszeiten verkauft und in Niederpreiszeiten selbst nutzt oder in Speichern wie z.B. seinem Elektroauto zwischenspeichert. Hierzu benötigt der Produzent Prognosedaten zur Abschätzung von Angebot, Nachfrage, der Preisentwicklung und seiner erwarteten, erzeugten Energiemenge. Hierzu könnten Daten wie der Wetterbericht, um eine Prognose über die potentiell erzeugbare erneuerbare Energie zu erstellen, oder typische Lastprofile herangezogen werden. Auch wenn solche Prognosedaten mit einem hohen Unsicherheitsfaktor behaftet sind, sollten sie grundsätzlich von einer vertrauenswürdigen Stelle stammen, die sich korrekt authentifiziert hat und die Daten müssen vor Manipulationen geschützt sein. Weiterhin müssen die erhaltenen Preisinformationen authentisch, integer, verfügbar und aktuell sein.

Falls sich aus übertragenen Messwerten und Daten zur Abrechnung Rückschlüsse auf Personen und deren Verhalten (z.B. eines Prosumers) ergeben, sind die Vertraulichkeit und der Datenschutz dieser Daten sicherzustellen.

Zusammengefasst sind die Sicherheitsanforderungen für Produzenten die folgenden:

- Authentizität und Integrität von Messwerten, Daten zur Abrechnung, Prognosedaten
- Authentizität, Integrität, Verfügbarkeit und Aktualität von Preisinformationen
- Vertraulichkeit und Datenschutz von Messwerten, Daten zur Abrechnung.

(4) Rolle: Übertragungsnetzbetreiber

Der Übertragungsnetzbetreiber hat genauso wie der Verteilnetzbetreiber die Hauptanforderung, dass sein Netz verfügbar ist. Hierzu muss die Leittechnik zur Steuerung des Netzes korrekt funktionieren und die übertragenen Steuernachrichten müssen authentifi-

ziert, gegen Manipulation geschützt, verfügbar und aktuell sein. Gleiches gilt für Statusdaten sowie Steuerdaten, die mit angeschlossenen Verteilnetzbetreibern ausgetauscht werden. Diese werden zum korrekten Betrieb des Übertragungsnetzes benötigt, z.B. zur Lastflussoptimierung oder für Schutzfunktionen wie der Sicherstellung der Frequenzstabilität.

Auf weitere Anforderungen des Übertragungsnetzbetreibers, wie beispielsweise nach korrekter Abrechnung der Netznutzung, soll hier nicht weiter eingegangen werden, da der Fokus dieses Artikels der Privatkunde und das Verteilnetz ist.

Zusammengefasst sind die Sicherheitsanforderungen für den Übertragungsnetzbetreiber die folgenden:

- Verfügbarkeit des Übertragungsnetzes
- Authentizität, Integrität, Verfügbarkeit und Aktualität von Statusdaten sowie Steuerdaten.

4.4 Sicherheitsarchitektur

Analog zu Kapitel 3.4 wird im Folgenden eine generische Sicherheitsarchitektur für die Domäne Verteilnetz vorgestellt, welche die in Kapitel 4.3 beschriebenen Sicherheitsanforderungen erfüllt.

Referenzmodell

Abbildung 7 zeigt ein Referenzmodell der Domäne Verteilnetz basierend auf der Architektur aus Abbildung 6 mit einer Leitstelle. Da

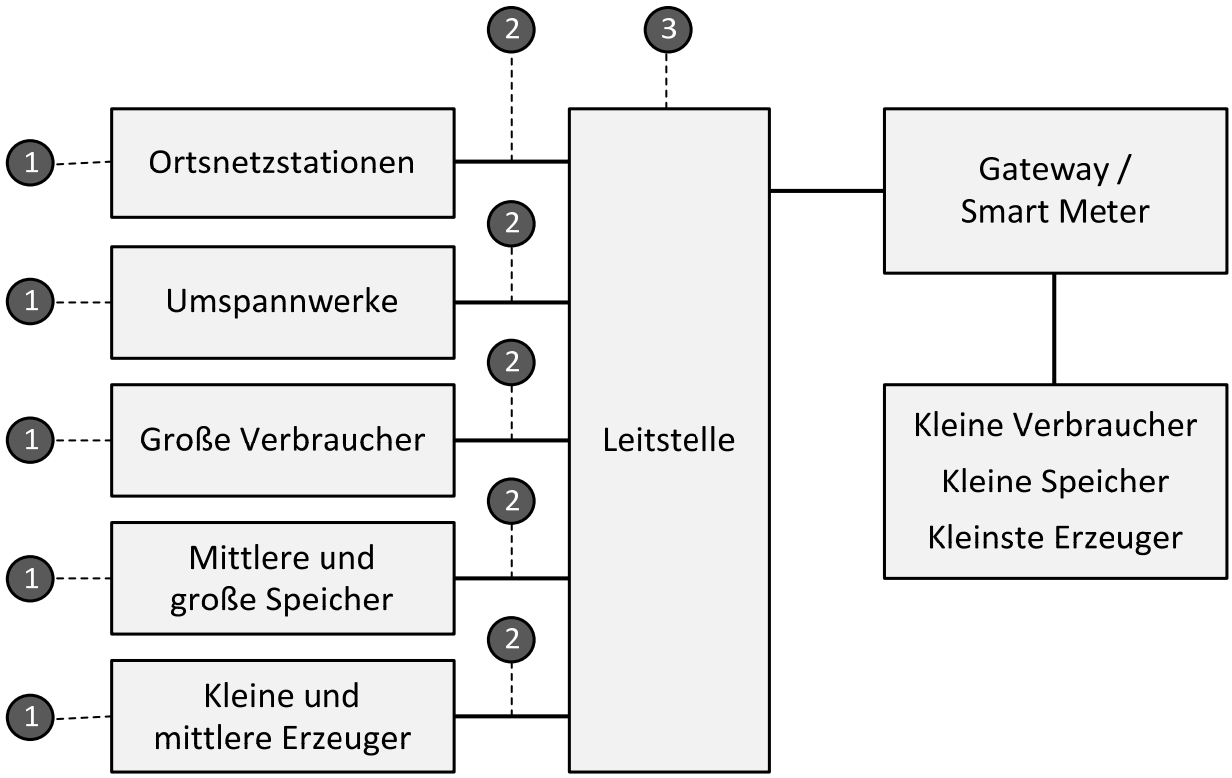


Abbildung 7: Referenzmodell der Domäne Verteilnetz mit Referenzpunkten

die Sicherheitsarchitektur hier nur auf einem relativ hohem Abstraktionsniveau beschrieben wird, sind einige Komponenten und Schnittstellen zur besseren Übersichtlichkeit zusammengefasst. Auch wird der Privatkunde in diesem Kapitel nicht erneut diskutiert. Nachfolgend werden anhand der Referenzpunkte 1 bis 3 die Sicherheitsmechanismen der Sicherheitsarchitektur beschrieben.

Falls sich in Zukunft auch andere Architekturen etablieren, in denen z.B. Smart Meter Gateways direkt mit Ortsnetzstationen kommunizieren, lassen sich die in diesem und in Kapitel 3.4 beschrieben Sicherheitsmechanismen leicht auf diese erweiterten Architekturen übertragen.

Referenzpunkt 1

Der Referenzpunkt 1 beschreibt die Sicherheitsmechanismen zur Absicherung der IKT-Systeme von Ortsnetzstationen, Umspannwerken, großen Verbrauchern wie Industrieunternehmen sowie den verschiedenen Speichern und Erzeugern. Durch das relativ hohe Abstraktionsniveau werden ähnliche Sicherheitsmechanismen einzusetzen sein, auch wenn ihre Umsetzung und insbesondere Einbindung in die Architekturen unterschiedlich erfolgen wird. Dies ist insbesondere darin begründet, dass Ausfälle von Ortsnetzstationen oder Umspannwerken wesentlich größere Auswirkungen haben, als Ausfälle einzelner Speicher oder Erzeuger, da direkt viele angeschlossenen Haushalte oder Firmen betroffen sind.

Es müssen Mechanismen zum Schutz gegen Manipulationen etabliert werden, um eine korrekte Funktionsweise der IKT-Systeme zu gewährleisten. Dies geht einher mit geeigneten Mechanismen zur Authentifizierung und Autorisierung von Mitgliedern der verschiedenen Rollen zum Schutz gegen unberechtigte Zugriffe.

Für den Verteilnetzbetreiber ist besonders die Verfügbarkeit der IKT-Systeme wichtig. Dies gilt in besonderem Maße für Ortsnetzstationen und Umspannwerke, da ein Ausfall der IKT-Systeme eine entfernte Überwachung und Steuerung verhindert. Diese Systeme müssen auch garantieren, dass bestimmte Daten innerhalb gewisser Zeiten verarbeitet werden, z.B. Statusmeldungen über Ausfälle. Aber auch Ausfälle der IKT-Systeme von Energie-Speichern, -Erzeugern und -Verbrauchern können Auswirkungen auf das Verteilnetz und die Verteilnetzautomatisierung haben, da die Netzsteuerung auf aktuelle Daten zum Energieverbrauch oder zu Einspeisekapazitäten zurückgreifen wird.

Neben Verbrauchern, Speichern und Erzeugern auf Mittel- und Hochspannungsebene gilt dies natürlich auch für die IKT-Systeme der beim Privatkunden installierten Verbraucher, Speicher und Erzeuger auf Niederspannungsebene, oder aber auch für das Gateway (vgl. Kapitel 3.4). Wobei hier der Ausfall einzelner Systeme keine größeren Auswirkungen haben wird und sich Probleme erst bei Ausfällen vieler Systeme ergeben.

Für Ortsnetzstationen sind, je nach tatsächlicher Architektur des Netzes, ggf. noch zusätzliche Sicherheitsmechanismen nötig. So ist beispielsweise denkbar, dass Privatkunden nicht direkt mit der Leitstelle kommunizieren, sondern mittels Schmalband-Powerline (PLC) an eine Ortsnetzstation angebunden sind, welche die Daten in die jeweiligen Richtungen vermittelt. Falls dies der Fall ist, sind auch an die Ortsnetzstation selbst Anforderungen ähnlich wie in Kapitel 3.4 beschrieben zu stellen. So müssten Mechanis-

men zur Sicherstellung der vertrauenswürdigen, korrekten und rechtzeitigen Verarbeitung, (Zwischen-)Speicherung und Weitergabe von Messwerten, Daten zur Abrechnung, Preisinformationen, Steuerdaten, Statusdaten und Wartungsdaten etabliert werden.

Falls jedoch Privatkunden nicht an Ortsnetzstationen angebunden sind, sind die umzusetzenden Sicherheitsmechanismen:

- Mechanismen zum Schutz gegen Manipulationen
- Mechanismen zur Authentifizierung und Autorisierung zugreifender Rollen
- Mechanismen zum Schutz der Verfügbarkeit der Systeme.

Die Umsetzung der Sicherheitsmechanismen zum Schutz gegen Manipulationen wird insbesondere bei Ortsnetzstationen und Umspannwerken voraussichtlich wie bisher durch physische Sicherheit, wie z.B. abgeschlossene Gebäude sichergestellt. Für Verbraucher, Speicher und Erzeuger ist zu untersuchen, ob hier ggf. auch spezielle Hardware Sicherheitsmodule, analog zum Gateway beim Privatkunden (vgl. Kapitel 3.4), eingesetzt werden können oder müssen, um Manipulationsversuche an IKT-Komponenten abzuwehren bzw. zu erkennen. Da es schwierig ist, Angriffe gänzlich zu verhindern, ist zu überlegen, ob weitere Maßnahmen wie Einbruchserkennungsverfahren, die die gefährdeten IKT-Komponenten überwachen, also Host-basierte Intrusion Detection Systeme (IDS), sinnvolle Ergänzungen sind. Derartige Überwachungssysteme könnten Alarmmeldungen an die Leitstelle senden, sobald ein möglicher Angriff erkannt wird. Erforderlich sind hierfür aber sehr gute Erkennungsraten, da häufige Fehlalarme mit entsprechenden Reaktionsmaßnahmen im operativen Betrieb nicht tolerabel sind.

Authentifizieren müssen sich sowohl Personen wie Administratoren der Systeme als auch IKT-Systeme. Die Authentifizierung kann wie bereits beschrieben mit Hilfe von kryptographischen Protokollen umgesetzt werden; die Autorisierung kann mittels Zugriffskontrolllisten zusammen mit Rollen-basierter Zugriffskontrolle realisiert werden.

Zur Sicherstellung der Verfügbarkeit und zur Einhaltung gewisser Zeitschranken sind zum einen derzeit schon eingesetzte klassische Safety-Mechanismen wie die redundante Auslegung von IKT-Systemen, um Fehlertoleranz zu erzielen, nötig. Damit ließen sich Ausfälle einzelner IKT-Komponenten kompensieren. Eine weitere Möglichkeit besteht in der Priorisierung von Aktivitäten, so dass bei partiellen Ausfällen nur noch die Kernfunktionen aufrecht erhalten werden. Damit Angreifer derartige Situationen nicht gezielt herbeiführen können, und damit einen Denial-of-Service-Angriff provozieren, werden auch hier Erkennungsverfahren benötigt, um übliches und unübliches Kommunikationsverhalten unterscheiden zu können.

Zum anderen wird durch die zunehmende IKT-Durchdringung bei der Steuerung von Verteilnetzen die Abhängigkeit der Funktions- und Betriebssicherheit (Safety) von der IT-Sicherheit (Security) immer größer. In der Vergangenheit wurden Safety-kritische Systeme meist nur in abgeschotteten Bereichen eingesetzt. Durch die starke Vernetzung und Einsatz in offenen Bereichen ergeben sich nun aber vielfältige Angriffsmöglichkeiten. Somit sind Maßnahmen zur Gewährleistung der Betriebssicherheit alleine nicht mehr ausreichend, sondern müssen durch IT-Sicherheits-Maßnahmen ergänzt werden.

Beispielsweise können vorgeschaltete Firewall-Systeme den Zugriff auf IKT-Komponenten des Verteilnetzes kontrollieren, so dass diese nicht durch zu viele Zugriffe überlastet werden. Betriebssicherheit und IT-Sicherheit können aber auch zwei gegenläufige Ziele sein. Beispielsweise benötigt der Einsatz von Kryptographie zusätzliche Ressourcen, wie z.B. Rechenleistung und Speicher, die in eingebetteten Sensoren wie SCADA Komponenten jedoch äußerst knapp sind. Als Folge einer zu hohen Ressourcenbelastung oder auch einer zu großen zeitlichen Verzögerung, die durch zusätzliche IT-sicherheitsbedingte Kontrollen auftreten, könnten es zu verzögerter Bearbeitung kommen, so dass definierte Echtzeitanforderungen nicht mehr eingehalten werden. Diese Wechselwirkungen zwischen Betriebssicherheit und IT-Sicherheit sind bei der Entwicklung und Umsetzung geeigneter Sicherheitsmechanismen (im Sinne von Safety und Security) zu beachten. Beispielsweise sollten abgestufte Sicherheitszonen eingeführt werden, so dass Kontrollen nur an Zonenübergängen durch ressourcenstarke Komponenten erfolgen.

Referenzpunkt 2

Referenzpunkt 2 beschreibt die Kommunikation zwischen den IKT-Systemen mit der Leitstelle. Die IKT-Systeme gehören zu Ortsnetzstationen, Umspannwerken, großen Verbrauchern sowie den verschiedenen Speichern und Erzeugern Die Kommunikation von kleinen Verbrauchern, kleinen Speichern, kleinsten Erzeugern und Smart Metern auf Niederspannungsebene mit der Leitstelle erfolgt über das Gateway. Wie bereits erwähnt, sind in diese Kommunikationsbeziehung auch noch weitere Rollen wie der Messdienstleister eingebunden. Die umzusetzenden Sicherheitsmechanismen wurden schon weiter oben beschrieben.

Grundsätzlich sind diese Sicherheitsmechanismen und Umsetzungen für die anderen Spannungsebenen ähnlich, da ähnliche Kommunikationsbeziehungen bestehen. So werden auch Ortsnetzstationen und Umspannwerken mit lokalen Messstellen ausgestattet sein und Messwerte an die Leitstelle senden. Auch werden sie Statusmeldungen senden und Steuerdaten sowie Wartungsdaten empfangen. Diese Daten werden auch mit Verbrauchern, Speichern und Erzeugern ausgetauscht werden. Bei diesen ist zusätzlich denkbar, dass auch Daten zur Abrechnung, aktuelle Verbrauchsdaten und ggf. auch Preisinformationen ausgetauscht werden. Die umzusetzenden Mechanismen entsprechen den weiter oben bereits diskutierten Sicherheitsmaßnahmen. Dies gilt jedoch nicht für den Fall, wenn die Kommunikation der Privatkunden über die Ortsnetzstation erfolgt (vgl. Kapitel 3). Für die weitergeleiteten, teilweise personenbezogenen Daten müssen Mechanismen wie in Kapitel 3.4 beschrieben umgesetzt werden.

Kommuniziert der Privatkunde nicht über Ortsnetzstationen, sind folgende Sicherheitsmechanismen umzusetzen:

- Mechanismen zum Schutz der Authentizität, Integrität und Aktualität der Messwerte, Daten zur Abrechnung, Statusmeldungen, Preisinformationen sowie Steuerdaten
- Mechanismen zum Schutz der Authentizität und Integrität von Wartungsdaten.

Bereits heute sind Umspannwerke mit einer Leitstelle verbunden. Zur Kommunikation werden entweder eigene Leitungen oder die Infrastruktur eines fremden Kommunikationsnetzbetreibers verwendet [12]. Eigene Lei-

tungen sind entweder die Stromleitungen selbst (Powerline oder Trägerfrequenztechnik) oder parallel laufende Leitungen meist in Form von Glasfasern. Bei Nutzung der Dienste eines Kommunikationsnetzbetreibers kann auf verschiedene Angebote, wie spezielle Mietleitungen aus Kupfer oder Glasfaser, Telefonnetz bzw. DSL-Anschluss, Mobilfunk, Richtfunk etc. zurückgegriffen werden. Beide Varianten, also die Nutzung eigener Leitungen oder aber von fremden Kommunikationsnetzanbietern, bieten sich auch für die Anbindung von Ortsnetzstationen, Verbrauchern, Speichern und Erzeugern an.

Wie die Absicherung der Kommunikation umgesetzt wird, hängt somit stark von den konkret eingesetzten Technologien und der Art des Netzausbaus ab. Die Nutzung eigener Leitungen hätte aus Sicherheitsgründen sicherlich Vorteile im Gegensatz zur Nutzung offener Netze wie dem Internet. Doch selbst bei der Nutzung eigener Netze können Angriffe nie ganz ausgeschlossen werden. Grundsätzlich könnten zur Sicherstellung der Authentizität, Integrität und falls zusätzlich benötigt auch der Vertraulichkeit beispielsweise Virtual Private Networks (VPN) mittels IPsec (vgl. [4]) aufgebaut werden.

Die Sicherstellung der Aktualität der übertragenen Daten ist ebenfalls stark von den eingesetzten Technologien und Netzstrukturen abhängig. So sollten Technologien eingesetzt werden die hoch verfügbar sind und die benötigten Datenraten bereitstellen. Auch sollten geeignete Redundanz-Konzepte umgesetzt werden.

Referenzpunkt 3

Dieser Referenzpunkt beschreibt die Sicherheitsmechanismen zur Absicherung der Leitstelle. Diese stellt als zentrale Komponente im Verteilnetz einen Single-Point-of-Failure dar und dementsprechend muss deren Verfügbarkeit und korrekte Funktionsweise besonders geschützt werden.

In Kapitel 3.4 wurden die Sicherheitsmechanismen für die Rolle Energieversorger bereits diskutiert. Diese lassen sich auch auf die Leitstelle übertragen. So muss sichergestellt werden, dass alle Daten, d.h. erhaltene Messwerte, Daten zur Abrechnung, aktuelle Verbrauchsdaten, Rechnungsdaten, Preisinformationen, Steuerdaten, Statusdaten und Wartungsdaten vertrauenswürdig, korrekt und rechtzeitig verarbeitet, gespeichert und übertragen werden.

Konkret müssen somit die Leitstellen gegen unberechtigte Manipulationen geschützt werden. Zugriff auf die Komponenten der Leitstellen darf nur durch authentifizierte und autorisierte Rollen-Mitglieder erfolgen. Weiterhin müssen Mechanismen zum Schutz vertraulicher Daten etabliert werden. Falls in der Leitstelle personenbezogene Daten, z.B. Messwerte individueller Privatkunden, die nicht anonymisiert oder aggregiert wurden, verarbeitet werden, müssen hierzu ebenfalls angemessene Schutz-Mechanismen etabliert werden. Insbesondere müssen Mechanismen zum Schutz der Verfügbarkeit der Komponenten der Leitstellen etabliert werden, da ein Ausfall große Auswirkungen hätte.

Die umzusetzenden Sicherheitsmechanismen sind somit:

- Mechanismen zum Schutz gegen Manipulationen der Komponenten der Leitstelle
- Mechanismen zur Authentifizierung und Autorisierung zugreifender Rollen-Mitglieder, inklusive der Protokollierung der Zugriffe für spätere Nachweisführungen
- Mechanismen zum Schutz vertraulicher und personenbezogener Daten
- Mechanismen zum Schutz der Verfügbarkeit der Leitstellen- Systeme.

Die Umsetzung der Sicherheitsmechanismen kann grundsätzlich analog zu den zuvor beschriebenen Vorgehensweisen erfolgen. Wie zudem in Kapitel 3.4 bereits ausgeführt, kann man sich bei der konkreten Umsetzung an den IT-Grundschutz-Katalogen des BSI orientieren.

5 Elektromobilität

Es ist ein erklärtes Ziel der Bundesregierung [24] die Zahl der Elektrofahrzeuge auf Deutschlands Straßen bis zum Jahr 2020 auf mindestens eine Million zu steigern. Bis zum Jahr 2030 soll diese Zahl sogar auf mindestens sechs Millionen Elektrofahrzeuge erhöht werden. Durch die steigende Anzahl an Elektrofahrzeugen wird die Elektromobilität in Zukunft ebenfalls eine wesentliche Komponente der Smart Grids werden. Ein Hauptaugenmerk aktueller Forschungsarbeiten liegt auf der Batterie von Elektrofahrzeugen. Deren Kapazität, die erforderlichen Ladevorgänge und -zeiten, aber auch deren Rolle als mobiler Energie-Speicher sind dabei wichtige Punkte. Für die Diskussion im vorliegendem Artikel sind insbesondere Ladevorgänge als auch die mobilen Speicher von Interesse, die es erlauben, Energie ins Smart Grid zurückzuspeisen. Der Anschluss ans Smart Grid kann zu Hause, an halböffentlichen Ladesäulen (z.B. am Arbeitsplatz) oder an öffentlichen Ladesäulen erfolgen. Aus Sicherheitssicht sind hier insbesondere Fragen der korrekten Abrechnung sowie der Datenschutz relevant. Im Folgenden werden, analog zu den vorherigen Kapiteln, zunächst Grundlagen und Anwendungsfälle beschrieben. Anschließend werden dann Sicherheitsanforderungen und eine mögliche Sicherheitsarchitektur diskutiert.

5.1 Grundlagen

Bei der Elektromobilität sind die folgenden Rollen, analog zur Domäne Privatkunde wie sie in Abbildung 2 dargestellt sind, relevant: Energienutzer, Energielieferant, Verteilnetzbetreiber, Messstellenbetreiber, Messdienstleister, Kommunikationsnetzbetreiber und Hersteller. Im Mittelpunkt des Interesses steht der Fahrzeug-Eigentümer bzw. -Halter, der in der Rolle eines *Energienutzers* auftritt. Die Energieübertragung in die Fahrzeugbatterie kann dabei auf unterschiedlichen Ladeverfahren beruhen. Diese können ähnlich wie andere Übertragungstechniken in kabelgebundene und kabellose Ladeverfahren unterteilt werden [25].

Kabelloses Laden, welches zum Beispiel mit Hilfe von Induktion realisiert werden kann, bietet dabei den Vorteil, dass ein Elektrofahrzeug überall, theoretisch auch während der Fahrt, geladen werden kann, sofern die benötigte Ladeinfrastruktur vorhanden ist. Nachteilig ist allerdings, dass heute existierende, kabellose Technologien im Vergleich zu kabelgebundenen Lösungen eine deutlich höhere Verlustrate beim Ladevorgang aufweisen [26], keine Rückspeisung von Energie erlauben und darüber hinaus eine genaue Positionierung des Elektrofahrzeugs benötigen, wodurch kabellose Lösungen oftmals komplexer in der Umsetzung sind als kabelgebundene. Schwerer wiegt jedoch, dass der Einsatz von kabellosen Techniken mit deutlich höheren Kosten verbunden ist, da eine geeignete Ladeinfrastruktur erst aufgebaut werden muss, während diese im Fall von kabelgebundenem Laden in Form von normalen Steckdosen in vielen Bereichen bereits vorhanden ist. Daher erscheint es aus heutiger Sicht, vor allem aufgrund der existierenden Gegebenheit, sehr unwahrscheinlich, dass sich kabellose Technologien gegenüber kabelgebundenen Technologien im Bereich der Elektromobilität schnell durchsetzen werden. Deshalb beschränken wir unsere Diskussion im Folgenden auf kabelgebundene Technologien.

Das Laden bzw. Rückspeisen von Strom erfolgt zu Hause oder an (halb-) öffentlichen Ladesäulen. Eine Ladesäule kann somit je

nach Ausprägung ein Teil der Domäne *Privatkunde* oder der Domäne *Verteilnetz* sein. Der Strom wird von einem *Energielieferanten* oder direkt von einem *Verteilnetzbetreiber*, der ggf. eigene Ladesäulen betreibt, bezogen. Der *Messdienstleister* erfasst den genutzten Strom beim Laden oder den rückgespeisten Strom mit Hilfe von entsprechenden Zählern. Diese Informationen werden an den Energielieferanten geleitet, um eine Abrechnung zu ermöglichen. Denkbar sind aber auch direkte Abrechnungen wie z.B. Barzahlung nach der Nutzung einer öffentlichen Ladesäule.

Die Installation und Wartung der Zähler erfolgt wieder durch den *Messstellenbetreiber* und die Kommunikation aller Rollen untereinander wird durch einen oder mehrere *Kommunikationsnetzbetreiber* realisiert. Mitglieder der Rolle *Hersteller* sind beispielsweise Hersteller von Elektrofahrzeugen oder von Ladesäulen.

Für den Anwendungsfall des Ladens des Elektrofahrzeugs zu Hause kann man zwei grundsätzliche Varianten [27] unterscheiden:

- Laden über eine herkömmliche Steckdose oder
- Laden über eine spezielle Ladeeinrichtung.

Bei der ersten Variante entstehen in der Regel keine zusätzlichen Kosten für die Ladeinfrastruktur, da Steckdosen in vielen privaten Bereichen bereits in ausreichendem Maße vorhanden sind. Im verwendeten Ladekabel ist hierzu meist bereits eine geeignete Steuereinrichtung integriert.

Die zweite Variante ist im Gegensatz zu herkömmlichen Steckdosen mit zusätzlichen Anschaffungskosten verbunden, bietet aber auch mehr Funktionalität. So können Ladeeinrichtungen beispielsweise aufgrund des dreiphasigen Anschlusses schnellere Ladezeiten ermöglichen oder erlauben das Rückspeisen von Strom in das Smart Grid, was mit herkömmlichen Steckdosen derzeit nicht möglich ist.

Die Verbrauchserfassung kann in beiden Fällen durch den im Haushalt installierten Smart Meter erfolgen.

Darüber hinaus wird derzeit auch die Möglichkeit diskutiert, den Ladevorgang in privaten und (halb-)öffentlichen Bereichen gezielt durch Tarife oder gar direkt durch den Netzbetreiber zu steuern [28]. Dadurch könnte der Ladevorgang beispielsweise nach Möglichkeit gezielt auf Niederstromzeitphasen verschoben werden, wodurch die Last des Smart Grids zu Hochstromzeitphasen reduziert werden kann.

In Abbildung 8 (vgl. hierzu auch [12]) sind vereinfacht mögliche Topologien für das Laden mittels Steckdose, mittels Ladeeinrichtung und mittels einer steuerbaren Ladeeinrichtung, die beispielsweise anhand von empfangenen Preissignalen das Laden in einem möglichst günstigen Zeitraum durchführt, dargestellt.

Ein Elektrofahrzeug kann auch an Ladesäulen in (halb-)öffentlichen Bereichen geladen werden. In halböffentlichen Bereichen, wie auf dem Parkplatz des Arbeitgebers oder eines Geschäfts, ist die Abrechnung stark vom jeweiligen Betreiber der Ladevorrichtung abhängig. So könnte eine Abrechnung gerade bei kleinen Strombeträgen gänzlich entfallen, mit dem Einkauf, dem Parken oder dem Lohn verrechnet werden oder aber direkt an der Ladevorrichtung bezahlt werden [25].

In öffentlichen Bereichen erfolgt das Laden an öffentlichen Ladeeinrichtungen [25]. Die Abrechnung kann hierbei unterschiedlich

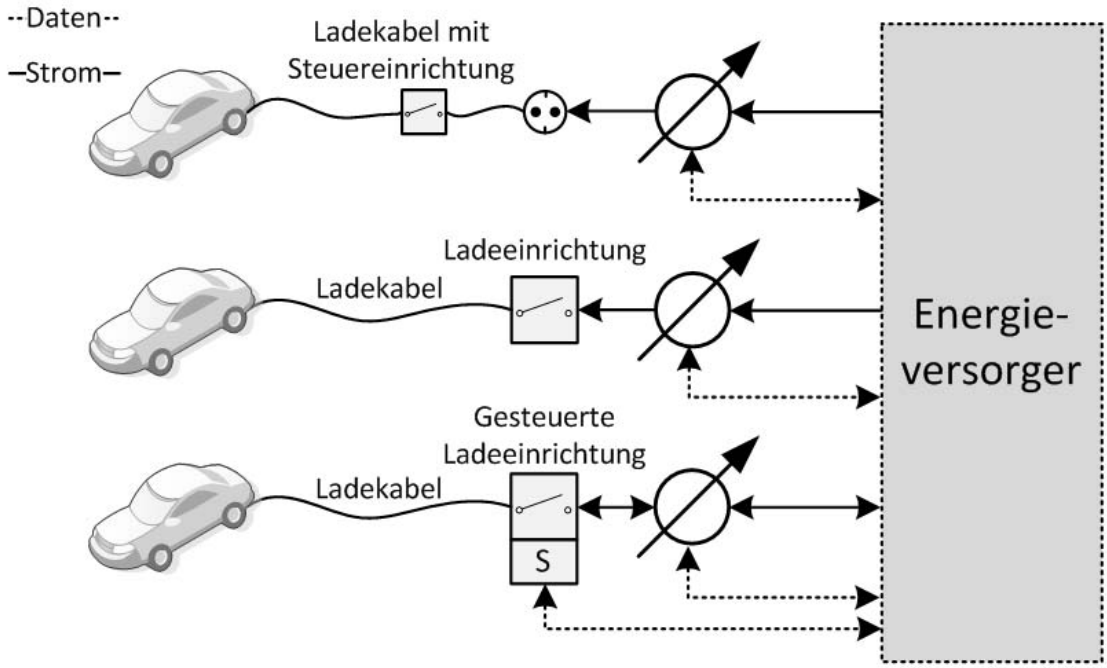


Abbildung 8: Netztopologien für den Anschluss beim Kunden

umgesetzt werden. Zum einen besteht die Möglichkeit, klassische Bezahlsysteme wie Bargeld, EC- oder Kreditkarten zu verwenden. In diesem Fall würde sich das Laden an öffentlichen Ladesäulen aus abrechnungstechnischer Sicht nicht vom Tanken an Benzintankstellen unterscheiden. Zum anderen könnten auch neue Abrechnungssysteme eingesetzt werden. Dabei wird im Rahmen der Elektromobilität derzeit vor allem über Fahrstromverträge diskutiert [29]. In diesem Fall schließt ein Fahrer einen Vertrag mit einem Stromlieferanten ab, der ihm nach vorherigen Authentifikation (z.B. über Smartcards) das Laden an Ladesäulen ermöglicht. Die Abrechnung erfolgt dann beispielsweise monatlich oder jährlich über den Fahrstromvertrag. Dabei kann der Anbieter des Fahrstromvertrags auch gleichzeitig der private Stromlieferant sein, wodurch die Abrechnung auch über den normalen Stromvertrag erfolgen kann.

Neben Fahrstromverträgen für Fahrer sind auch Fahrstromverträge für Fahrzeuge im Gespräch [29]. In diesem Fall würde ein Fahrzeughalter einen Fahrstromvertrag für ein bestimmtes Fahrzeug abschließen. Die für das Laden erforderliche Authentifikation könnte dann beispielweise direkt vom Fahrzeug über das Ladekabel durchgeführt werden und ohne Interaktion des Fahrers erfolgen. Dadurch könnte ein Elektrofahrzeug auch von verschiedenen Fahrern über ein und denselben Fahrstromvertrag abgerechnet werden.

In der bisherigen Betrachtung wurde davon ausgegangen, dass alle öffentlichen Ladesäulen einem Energieversorger unterstellt sind. Es wird jedoch, sowohl innerhalb Deutschlands als auch im Ausland, viele un-

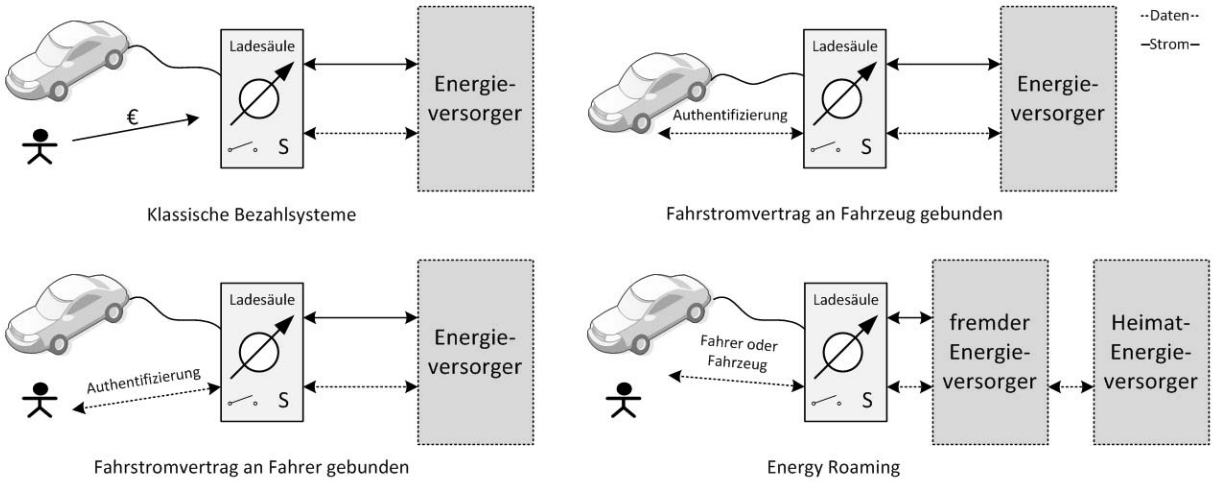


Abbildung 9: Netztopologien beim Anschluss an Ladesäulen

terschiedliche Energieversorger mit Ladesäulen geben. Grundsätzlich sollte eine einheitliche Lösung entwickelt werden, so dass im Falle von Fahrstromverträgen für Fahrer bzw. Fahrzeuge alle Ladesäulen nutzbar sind. Hierzu ist ein einheitliches, länderübergreifendes *Energy Roaming* Konzept nötig [29]. Die Authentifizierung von Fahrern bzw. Fahrzeug könnte hierbei ähnlich wie beim Roaming im Mobilfunk umgesetzt werden. Fahrer bzw. Fahrzeughalter haben einen Fahrstromvertrag mit ihrem Heimat-Energieversorger. Bei Nutzung einer Ladesäule eines fremden Energieversorgers kontaktiert dieser den Heimat-Energieversorger mit dessen Hilfe die Authentifizierung durchgeführt wird und die beiden Energieversorger rechnen den Verbrauch untereinander ab.

Abbildung 9 stellt die derzeit diskutierten Netztopologien noch einmal graphisch dar.

Eine weitere Möglichkeit, wie Elektrofahrzeuge „geladen“ werden können, ist das Auswechseln der Batterien [27]. Dies ist insbesondere dann von Interesse, wenn Fahrzeuge wie z.B. Taxen während des Tages nicht für längere Zeit abgestellt und aufgeladen werden können. Da sich dieser Austausch im Wesentlichen nicht vom Tanken von Benzin unterscheidet, wird dies im Folgenden nicht weiter betrachtet.

5.2 Anwendungsfälle

Im Folgenden werden repräsentative Anwendungsfälle und relevante Schutzziele für die Elektromobilität beschrieben, um daraus anschließend die Sicherheitsanforderungen der einzelnen Rollen abzuleiten. Wie in den Kapiteln 3.2 und 4.2 wurden die Anwendungsfälle größtenteils aus den in [10] beschriebenen sicherheitsrelevanten Anwendungsfällen abgeleitet.

Use-Case: Laden eines Elektrofahrzeugs zu Hause ohne Energierückspeisung oder gesteuertem Laden

Dieser Anwendungsfall beschreibt das Laden eines Elektrofahrzeugs beim Kunden zu Hause wie zuvor beschrieben und in Abbildung 8 dargestellt. Aus Sicherheitssicht muss

hierbei vor allem der physische Zugang zur Ladevorrichtung geschützt werden, damit Unbefugte nicht Strom stehlen oder die Vorrichtung manipulieren können.

Use-Case: Laden an Ladesäulen ohne Energierückspeisung oder gesteuertem Laden

Dieser Anwendungsfall beschreibt das Laden eines Elektrofahrzeugs an öffentlichen Ladesäulen wie bereits beschrieben und in Abbildung 9 dargestellt. An den Ladesäulen (oder über andere Wege) müssen dem Fahrer aktuelle Preisinformationen angezeigt werden. Für die Abrechnung werden derzeit sowohl klassische Bezahlsysteme als auch Fahrstromverträge diskutiert. Je nach Bezahlsystem erfolgt vor dem Laden ggf. eine Authentifikation, die beispielsweise mit Smartcard und PIN-Eingabe realisiert werden kann.

Im Falle von Fahrstromverträgen existieren vornehmlich Datenschutzprobleme, da die Ladesäule aus eichrechtlichen Gründen sowohl die Kunden-ID als auch die Messwerte beim Laden kennen muss [29]. Ferner müssen diese Daten auch dem Energieversorger des Kunden bekannt sein, damit eine Abrechnung für den Kunden erstellt werden kann. Dadurch ergibt sich für den Energieversorger die Möglichkeit, Bewegungsprofile der Kunden anzufertigen. Diese Möglichkeit könnte neben dem Energieversorger auch für andere an der Abrechnung beteiligte Anbieter existieren, sofern diese die Kunden-ID während des Ladens erhalten. Da die genaue Kommunikation und Datenübertragung zwischen den einzelnen Rollen aber noch nicht genau festgelegt ist, kann an dieser Stelle keine Aussage darüber getroffen werden, welche Rollen dafür in Frage kämen. Darüber hinaus hätte im Fall eines Fahrstromvertrages für ein Fahrzeug auch der Fahrzeughalter die Möglichkeit, Bewegungsprofile von anderen Fahrern zu erstellen, da die letztendliche Abrechnung ihm zukommt.

Neben Abrechnungsdaten wird auch erwogen Statusdaten über die Ladeleitung zu übertragen, wie z.B. aktuelle Informationen über Routenplanung oder die Ladeleistung, [30] die die Batterie unterstützt. Diese Informationen könnten sensitiv sein und sollten im Allgemeinen verschlüsselt und integritätsgeschützt übertragen werden. Andernfalls könnte ein Angreifer beispielsweise die Überlastung der Batterie durch falsche Informationen hervorrufen.

Ferner ist noch die physische Sicherheit der Ladesäule selbst sicherzustellen. Diese müssen stabil gebaut sein, um gegen Vandalismus gewappnet zu sein. Zusätzlich besteht die Möglichkeit von Skimmingangriffen, falls mit der EC-Karte oder Kreditkarte bezahlt wird.

Schließlich muss neben den IKT-Anforderungen insbesondere auch die Verfügbarkeit der Energie gewährleistet werden, um eine gewisse Versorgungssicherheit für Fahrzeuge zu erreichen.

Use-Case: Gesteuertes Laden

Sowohl beim Laden zu Hause als auch an Ladesäulen soll zukünftig die Möglichkeit bestehen, das Laden von Elektrofahrzeugen gezielt zu steuern. Dies soll zu einer Entlastung des Stromnetzes in Hochstromzeitphasen beitragen, aber auch die Möglichkeit bieten von günstigen Tarifen in Niederstromzeitphasen zu profitieren. Die Steuerung könnte dabei direkt durch den (Netz-)Betreiber oder aber indirekt durch Tarifänderungen des Lieferanten erfolgen [28]. Beide Szenarien wer-

den im Folgenden getrennt voneinander betrachtet.

Die zusätzliche Belastung durch Elektroautos für das Stromnetz wird zwar als verhältnismäßig gering eingeschätzt [25], kann aber dennoch zu Ladespitzen führen, falls viele Fahrzeuge gleichzeitig zum Laden an das Stromnetz angeschlossen werden [30]. Ein solcher Fall könnte beispielsweise am Abend, wenn viele Leute nach Hause kommen, eintreten, oder wenn sich viele Elektrofahrzeuge an einer Stelle befinden, wie im Falle von Flughäfen oder Stadien.

Um der Gefahr einer Netzüberlastung entgegenwirken zu können, besteht daher die Überlegung, die Ladevorgänge vom Netzbetreiber steuern zu lassen [28]. Dadurch könnte die Ladung von Elektrofahrzeugen vom Netzbetreiber überwacht und koordiniert werden, wodurch Netzüberlastungen von vornherein verhindert werden könnten. Allerdings setzt eine Steuerung durch den Netzbetreiber voraus, dass detaillierte Informationen über die am Netz angeschlossenen Elektrofahrzeuge vorliegen. So müsste der Netzbetreiber beispielsweise Informationen über die Kapazität einer Batterie und deren aktuellen Ladezustand abrufen können. Zusätzlich müssten auch die Mobilitätsbedürfnisse der einzelnen Fahrer berücksichtigt werden. Daher erscheint ein derartiges Szenario aus heutiger Sicht aufgrund der Einschränkungen, die für die Fahrer damit verbunden sein könnten, und der Fülle an Informationen, die verarbeitet werden müssten, als eher unwahrscheinlich.

Wahrscheinlicher ist dagegen, dass ein solches Szenario im kleinen Rahmen umgesetzt wird. So wäre beispielsweise eine Koordinierung der Ladevorgänge im halböffentlichen Bereich denkbar [27].

Neben der Regelung des Ladens durch den (Netz-)Betreiber, könnte das Laden auch gezielt durch Tarifänderungen gesteuert werden [28]. Hierbei könnten zum Beispiel Lieferanten Informationen über den derzeitigen Tarif an Ladeeinrichtungen zu Hause oder öffentliche Ladesäulen übertragen. Abhängig von den Mobilitätsbedürfnissen des Fahrers würde unter Berücksichtigung des aktuellen Tarifs das Laden dann entweder sofort erfolgen, falls der Tarif günstig ist oder aber das Fahrzeug bald wieder benötigt wird, oder auf einen späteren Zeitpunkt verschoben werden. Da Fahrzeuge in der Regel etwa 96% [25] des Tages stehen, ist es wahrscheinlich, dass sich dadurch in vielen Bereichen Einsparungen erzielen ließen, vor allem falls ein Fahrzeug für einen längeren Zeitraum beim Arbeitgeber oder über Nacht abgestellt wird. Um diesen Ansatz verfolgen zu können, muss jedoch der Fahrer seine Mobilitätsbedürfnisse vor dem Laden mitteilen. Noch ist unklar wie genau dieser Vorgang erfolgen soll. Im privaten Bereich wäre zum Beispiel denkbar, dass eine Ladeeinrichtung auf einen bestimmten Zeitplan programmiert wird, der den Bedürfnissen der Fahrer entspricht. Vorstellbar wäre auch, dass das Laden der Batterie in unterschiedliche Bereiche eingeteilt wird. So könnte zum Beispiel ein kritischer Bereich definiert werden, der eine Mindestmenge an Energie für eine Elektrofahrzeugbatterie festlegt, so dass unerwartete kürzere Fahrten auf jedem Fall durchgeführt werden können. Das Laden kritischer Bereiche würde dann sobald wie möglich erfolgen, während andere unkritische Bereiche abhängig vom Tarif geladen werden.

Die Überlegungen zur Sicherheit sind analog zu den beiden obigen Anwendungsfällen. Zusätzlich muss jedoch noch sichergestellt werden, dass die Kontroll-Software für Ladevor-

gänge korrekt und entsprechend der Wünsche des Fahrers arbeitet, und dass die Preisinformationen integer und aktuell sind.

Use-Case: Energierückspeisung

Dieser fortgeschrittene Anwendungsfall erweitert die vorherigen Anwendungsfälle um die Möglichkeit, das Elektrofahrzeug als Speicher in Smart Grids zu nutzen und Energie zurückzuspeisen. Die Überlegung ist dabei, dass Fahrzeuge, wie bereits erwähnt, in der Regel über weite Zeiträume des Tages stehen und die verfügbaren Speicherreserven der Elektrofahrzeugbatterie daher über das Fahren hinaus genutzt werden könnte. Dabei sind zwei grundsätzliche Möglichkeiten gegeben. Zum einen könnten Besitzer bzw. Fahrer eines Elektrofahrzeugs die Energie, die in der Fahrzeugbatterie gespeichert ist, benutzen, um andere Elektrogeräte im Haus zu Spitzenlastzeiten mit Strom zu versorgen. Damit könnte man die vorhandene Energie nutzen und diese später in Niedertarifzeiten, oder wenn erneuerbare Energiequellen (z.B. Photovoltaikanlagen) im Haushalt selber zur Verfügung stehen, wieder auffüllen.

Zum anderen könnten die Elektrofahrzeugbatterien von Energieerzeugern ähnlich einem Pumpspeicherkraftwerk als Zwischenspeicher für Energie benutzt werden. Dieses Konzept wird auch als „Vehicle to Grid“ (V2G) bezeichnet. Zwar enthält jede Fahrzeugbatterie nur eine vergleichsweise geringe Menge an Energie, doch wird diese mit anderen Elektrofahrzeugbatterien kombiniert, so kann kurzfristig eine hohe Energieleistung erzielt werden [26]. Somit könnte die vorhandene Energie in Hochstromzeitphasen benutzt werden, um Lastspitzen auszugleichen. Zusätzlich würde V2G ermöglichen, überschüssige Energie, die z.B. aus erneuerbaren Energiequellen erzeugt wird, ohne den Bau von zusätzlichen Pumpspeicherkraftwerken, kostengünstig zwischenzuspeichern. Damit könnten Elektrofahrzeugbatterien als mobiler Energiespeicher zur Regelung des Stromnetzes eingesetzt werden, da bei Energieüberschuss Energie aufgenommen und bei Energieknappheit Energie abgegeben werden kann. Allerdings ist die technische Realisierung von V2G aus heutiger Sicht schwierig. So kann es durch das häufige zu- und abschalten von Batterien zum Stromnetz, wie es bei Elektromobilität erwartet werden kann, beispielsweise zu Oberschwingungen kommen, die zum Ausfall des ganzen Stromnetzes führen könnten [30].

Um V2G nutzen zu können, müssen Fahrzeughalter ihre Elektrofahrzeugbatterie als mobile Energiespeicher zur Verfügung stellen. Die dafür nötigen Anreize könnten beispielsweise über vergünstigte Stromtarife oder Entgelte geschaffen werden. Denkbar wäre auch, dass Elektrofahrzeugbesitzer die gespeicherte Energie zu einem möglichst hohen Preis an den Energieversorger oder über den Energiemarktplatz „verkaufen“. Da derzeitige Batterien allerdings nur eine bestimme Anzahl von Ladezyklen überdauern, ist es aus heutiger Sicht fraglich, ob Fahrzeugbesitzer von Rückspeisung Gebrauch machen werden. Dies wird von den Anschaffungskosten der Batterie und dem Sparpotential der Rückspeisung abhängig sein.

Aus Sicherheitssicht ist im Falle von Rückspeisung darauf zu achten, dass die Verfügbarkeit des Systems zur Steuerung der Rückspeisung sowie die Integrität der Steuernachrichten gewährleistet werden. Zusätzlich besteht im Falle von V2G aus Fahrzeughaltersicht das Risiko, dass Bewegungsprofile erstellt werden können, da der zurückgespeiste Strom dem betreffenden Fahrzeug-

halter gutgeschrieben werden muss, wodurch eine eindeutige Identifikation möglich sein kann.

5.3 Sicherheitsanforderungen

Die zentralen Bereiche, aus denen Sicherheitsanforderungen resultieren sind die Authentifikation (und Autorisation) von Fahrern bzw. Fahrzeugen zur Abrechnung sowie die Datenschutzanforderungen.

Da die Elektromobilität sehr eng mit der Domäne Privatkunde und der Domäne Verteilnetz zusammenhängt, sind die Sicherheitsanforderungen sehr ähnlich oder teilweise sogar identisch mit den Anforderungen, wie sie schon in den vorherigen Kapiteln beschrieben wurden. Für die Rollen Verteilnetzbetreiber, Kommunikationsnetzbetreiber, Messstellenbetreiber (MSB), Messdienstleister (MDL) und Hersteller sei deshalb auf diese Kapitel verwiesen. Nachfolgend werden die Sicherheitsanforderungen für die Rollen Energienutzer und Energielieferant unter den Gesichtspunkten der Abrechnung und des Datenschutzes noch etwas detaillierter betrachtet.

(1) Rolle: Energienutzer

Wie schon in Kapitel 3.3 beschrieben, hat der Energienutzer in der Regel hohe Anforderungen an den Datenschutz. Da Elektrofahrzeuge an unterschiedlichen Orten geladen werden und hierfür Daten zur Abrechnung erfasst werden müssen, können Angreifer potentiell Bewegungsprofile erstellen. Somit müssen neben den eigentlichen Messwerten auch die Daten zur Abrechnung, die beispielsweise die ID des Fahrers bzw. dessen Smartcard oder des Fahrzeugs enthalten, Statusdaten und ggf. noch weitere Daten wie Position der Ladesäule entsprechend geschützt werden. Dadurch soll beispielsweise eine automatisierte Auswertung der Nutzung von Ladsäulen nicht möglich sein, um die besuchten Orte des Energienutzers mit seinem Elektrofahrzeug zu bestimmen (z.B. Arbeit, Supermarkt, Bowlingcenter).

Um eine korrekte Abrechnung zu gewährleisten, ist aus Sicht des Energienutzers sicherzustellen, dass die Authentizität und Integrität von Messwerten und Daten zur Abrechnung sowie die Authentizität, Integrität, Aktualität und Verbindlichkeit von Preisinformationen umgesetzt wird.

Weiterhin müssen Steuerdaten, die z.B. Kommandos wie „Lade jetzt!“ oder „Speise Energie jetzt ein!“ enthalten, authentisch, integer und aktuell sein.

Neben den übertragenen Daten müssen auch die Systeme der Ladeeinrichtungen und Ladesäulen gegen Manipulationen (z.B. der Systemsoftware) geschützt werden, um deren Integrität sicherzustellen. Auch muss sichergestellt werden, dass die angezeigten Preisinformationen aktuell und korrekt sind und auch korrekt zur Abrechnung verwendet werden. In diesem Zusammenhang ist auch die Authentizität und Integrität von Wartungsdaten sicherzustellen, so dass ein Angreifer nicht durch Einspielen falscher Updates Manipulationen vornehmen kann.

Auch muss der Zugriff aus Ladeeinrichtungen und Ladesäulen kontrolliert werden, da diese oft leicht durch Dritte zugänglich sind. Beispielsweise sind Ladeeinrichtungen nicht immer in einer geschlossenen Garage installiert.

Um sicherzustellen, dass die Elektrofahrzeuge entsprechend ihres Bedarfs mit ausrei-

chend Strom versorgt werden, ist wiederum die Versorgungssicherheit sicherzustellen.

Die Sicherheitsanforderungen für den Energienutzer aus Sicht der Elektromobilität sind zusammengefasst die folgenden:

- Vertraulichkeit und Datenschutz der Messwerte, der Daten zur Abrechnung, Statusdaten und weiterer Daten
- Authentizität und Integrität von Messwerten, der Daten zur Abrechnung, Wartungsdaten
- Authentizität, Integrität und Aktualität von Steuerdaten
- Authentizität, Integrität, Aktualität und Verbindlichkeit von Preisinformationen
- Integrität der Systeme von Smart Meter, Gateway, Ladeeinrichtungen, Ladesäulen etc.
- Zugriffskontrolle für Ladeeinrichtungen und Ladesäulen
- Versorgungssicherheit.

(2) Rolle: Energielieferant

Der Energielieferant versorgt den Energienutzer bzw. dessen Elektrofahrzeug mit Strom. Beim Laden bzw. Rückspeisen zu Hause ist dies immer der Heim-Energieversorger, an (halb-) öffentlichen Ladesäulen entweder der Heim-Energieversorger oder beim Energy-Roaming ein fremder Energieversorger.

Für den Energielieferanten ist zum einen die Versorgungssicherheit, zum anderen eine korrekte Abrechnung wichtig. Die Sicherstellung der Versorgungssicherheit muss durch den Verteilnetzbetreiber erfolgen. Die Abrechnung mit Verteilnetzbetreiber, Energienutzer (Fahrer bzw. Fahrzeug) und anderen Energielieferanten führt der Energielieferant entweder selbst durch, oder nutzt hierzu einen gesonderten Dienstleister.

Für eine korrekte Abrechnung muss eine Zugriffskontrolle für Ladeeinrichtungen und Ladesäulen etabliert werden, so dass sich beispielsweise Fahrer bzw. Fahrzeug authentifizieren müssen (außer bei klassischen Bezahlsystemen wie Barzahlung). Auch müssen wieder Ladeeinrichtungen, Ladesäulen etc. vor Manipulationen geschützt werden, sowie, wie zuvor schon beschrieben, die verschiedenen Daten geschützt werden.

Zusammengefasst sind die Sicherheitsanforderungen für den Energielieferanten die folgenden:

- Versorgungssicherheit im vertraglich zugesicherten Umfang
- Authentizität und Integrität von Messwerten, Daten zur Abrechnung, Steuerdaten, Wartungsdaten
- Authentizität, Integrität und Aktualität von Steuerdaten
- Authentizität, Integrität, Aktualität und Verbindlichkeit von Preisinformationen
- Integrität der Systeme von Smart Meter, Gateway, Ladeeinrichtungen, Ladesäulen etc.
- Zugriffskontrolle für Ladeeinrichtungen und Ladesäulen.

5.4 Sicherheitsarchitektur

Im Folgenden wird eine generische Sicherheitsarchitektur für die Elektromobilität vorgestellt, welche die in Kapitel 5.3 beschriebenen Sicherheitsanforderungen erfüllt.

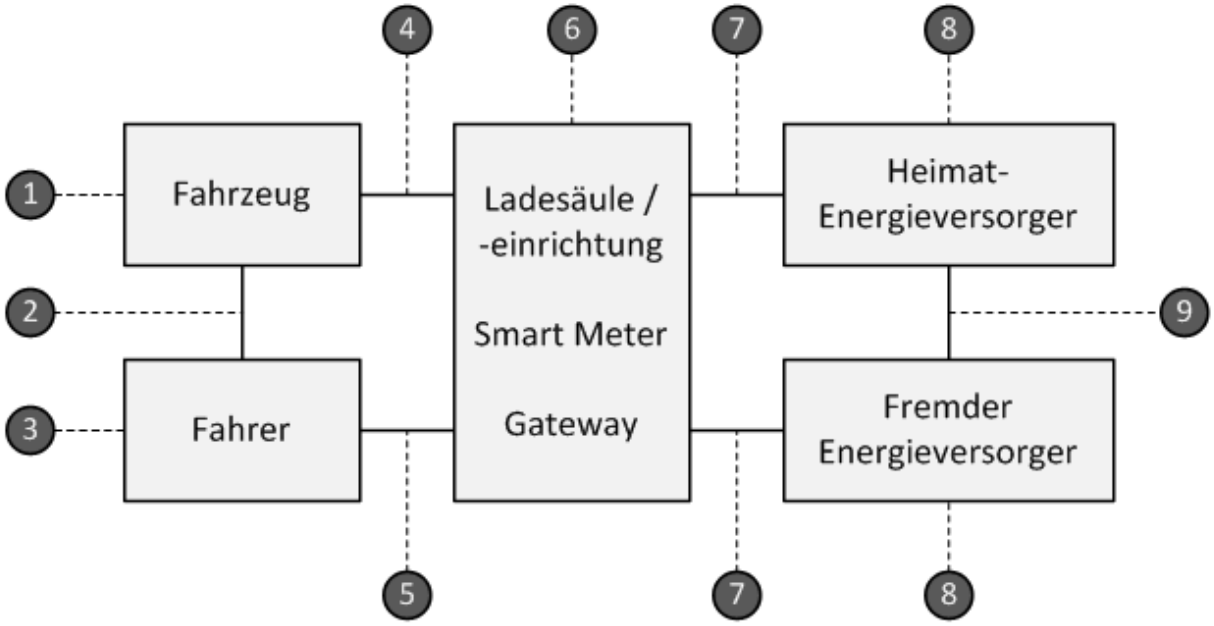


Abbildung 10: Referenzmodell der Elektromobilität mit Referenzpunkten

Referenzmodell

Abbildung 10 zeigt ein Referenzmodell für die Elektromobilität. Die Komponenten Fahrzeug (als Verbraucher bzw. ggf. auch als Speicher) und Fahrer sind mit einer Komponente Ladesäule / -einrichtung inklusive Smart Meter und Gateway verbunden. Diese Zusammenfassung kann bei der hier noch sehr abstrakten Betrachtung durchgeführt werden, da ähnliche Sicherheitsmechanismen zum Einsatz kommen werden. Ladesäulen/-einrichtungen können entweder mit dem Heimat-Energieversorger des Fahrers / Fahrzeugs oder einem fremden Energieversorger verbunden sein. Im Falle des weiter oben beschriebenen Energy Roamings sind diese Energieversorger zu Abrechnungszwecken miteinander verbunden. Anhand der Referenzpunkte 1 bis 9 werden nachfolgend die Sicherheitsmechanismen der Sicherheitsarchitektur für die Komponenten und Schnittstellen beschrieben.

Referenzpunkt 1

Referenzpunkt 1 beschreibt die Sicherheitsmechanismen, die im Fahrzeug selbst etabliert werden müssen, um die Kommunikation mit Ladesäule / -einrichtung und ggf. auch mit dem Fahrer abzusichern.

Für den Fall, dass ein Fahrstromvertrag an das Fahrzeug gebunden ist, (vgl. Kapitel 5.1) muss sich beispielsweise das Fahrzeug gegenüber der Ladesäule authentifizieren. Die hierzu benötigten Authentifizierungsdaten (z.B. kryptographische Schlüssel) müssen somit sicher im Fahrzeug gespeichert werden, so dass ein Angreifer diese nicht auslesen oder manipulieren kann, um beispielsweise auf Kosten eines anderen zu laden. Die entsprechenden Systeme im Fahrzeug sollten deshalb Schutz vor unberechtigtem Zugriff und Manipulationen bieten.

Weiterhin müssen Mechanismen zum Schutz personenbezogener Daten etabliert werden,

die ggf. im Fahrzeug gespeichert werden (müssen). Beispielsweise könnten Daten, wie die genutzten Ladesäulen, gespeichert werden, aus denen sich Bewegungsprofile ableiten ließen. Falls solche Daten gespeichert werden, muss der Zugriff darauf entsprechend kontrolliert werden.

Die umzusetzenden Sicherheitsmechanismen sind somit:

- Mechanismen zum Schutz der Vertraulichkeit und Integrität von Authentifizierungsdaten
- Mechanismen zum Schutz gegen Manipulationen
- Mechanismen zum Schutz personenbezogener Daten

Die beiden ersten Punkte könnten durch den Einsatz von Hardware Sicherheits-Modulen und entsprechender Verfahren realisiert werden. Zum Schutz personenbezogener Daten, die im Fahrzeug gespeichert sind, können Zugriffskontrollmechanismen eingesetzt werden, so dass nur Berechtigte zugreifen dürfen.

Referenzpunkt 2

Referenzpunkt 2 beschreibt die Kommunikation zwischen Fahrer und Fahrzeug. Neben der verbreiteten drahtlosen Kommunikation zwischen Fahrzeugschlüssel und Fahrzeug zum Öffnen der Tür sind hier noch weitere Szenarien denkbar.

Beispielsweise können Flottenfahrzeuge oder Car Sharing Fahrzeuge mit einem Fahrstromvertrag verknüpft sein und das Laden wird darüber abgerechnet. Der tatsächliche Fahrer soll jedoch für den genutzten Strom bezahlen. Für eine Abrechnung muss sich hierzu der Fahrer für die Abrechnungsperiode entsprechend authentifizieren. Somit kann folgende Sicherheitskomponente nötig sein:

- Mechanismus zur Authentifizierung des Fahrers.

Eine mögliche Umsetzung könnte mit Hilfe des neuen Personalausweises (nPA) realisiert werden, wenn das Fahrzeug mit einem entsprechenden Leser ausgestattet ist.

Referenzpunkt 3

Dieser Referenzpunkt beschreibt die Sicherheitsmechanismen für den „Fahrer“. Wie im Kapitel zuvor erwähnt, muss dieser sich ggf. gegenüber dem Fahrzeug authentifizieren. Je nach Realisierung der Abrechnung kann aber ebenfalls eine Authentifizierung der Kommunikation mit der Ladesäule bzw. Ladeeinrichtung nötig sein. Um diese Authentifikation auf eine sichere Basis zu stellen, muss die Vertraulichkeit und Integrität der Authentifizierungsdaten gewährleistet werden. Die umzusetzenden Sicherheitsmechanismen sind somit:

- Mechanismen zum Schutz der Vertraulichkeit und Integrität von Authentifizierungsdaten.

Die Authentifikation des Fahrers kann über den Nachweis des Besitzes eines Authentifizierungstokens wie einer Smartcard realisiert werden. Dort sind die benötigten Authentifizierungsdaten wie kryptographische Schlüssel sicher abgelegt. Zum Zugriff ist noch die Eingabe der korrekten PIN oder der Nachweis anderer Authentisierungsmerkmale, wie beispielsweise biometrische Daten, nötig.

Referenzpunkt 4

Dieser Referenzpunkt beschreibt die Kommunikation zwischen Fahrzeug und Ladesäule bzw. Ladeeinrichtung.

Diese Kommunikation ist nötig, wenn an das Fahrzeug ein Fahrstromvertrag gekoppelt ist, um Abrechnungen zu ermöglichen. Hier müssen zumindest Daten zur Abrechnung wie die ID des Fahrzeugs an die Ladesäule übermittelt werden. Denkbar ist auch, dass eine ID der Ladesäule, Messwerte, Rechnungsdaten und Preisinformationen an das Fahrzeug gesendet werden, die auf einem Display im Fahrzeug angezeigt werden. Empfangene Preisinformationen könnten vom Fahrzeug auch genutzt werden, um selbständig Entscheidungen über den Ladezeitraum zu treffen.

Sowohl beim Laden zu Hause als auch an öffentlichen Ladesäulen wird voraussichtlich für die Anwendungsfälle „Gesteuertes Laden“ und „Energierückspeisung“ eine Kommunikation nötig sein, um Steuerdaten und Statusdaten auszutauschen.

Zur Absicherung der Kommunikation ist es meist notwendig, dass sich das Fahrzeug gegenüber der Ladesäule bzw. Ladeeinrichtung authentifiziert. Ebenfalls sollte sich beim Laden an einer öffentlichen Ladesäule diese sicher gegenüber dem Fahrzeug authentifizieren und es sollte sichergestellt sein, dass diese nicht manipuliert. Es kann jedoch auch sein, dass die Ladesäule selbst nur minimale Fähigkeiten besitzt und Daten nur an den Energieversorger zur Abrechnung weiterreicht. In diesem Fall muss sich der entsprechende Kommunikationsendpunkt beim Energieversorger authentifizieren.

Weiterhin müssen Mechanismen zum Schutz der Authentizität, Integrität, Vertraulichkeit und Datenschutz von Messwerten, Daten zur Abrechnung und Rechnungsdaten etabliert werden.

Für Steuerdaten und Statusdaten sind Mechanismen zum Schutz der Authentizität, Integrität und Aktualität umzusetzen. Dies gilt auch für Preisinformationen, wobei diese verbindlich sein sollten.

Die umzusetzenden Sicherheitsmechanismen sind somit:

- Mechanismen zur (wechselseitigen) Authentifizierung
- Mechanismen zum Schutz der Authentizität, Integrität, Vertraulichkeit und Datenschutz von Messwerten, Daten zur Abrechnung und Rechnungsdaten
- Mechanismen zum Schutz der Authentizität, Integrität und Aktualität von Steuerdaten und Statusdaten
- Mechanismen zum Schutz der Authentizität, Integrität, Aktualität und Verbindlichkeit von Preisinformationen.

Die Umsetzung von Mechanismen zum Schutz der Authentizität, Integrität und Vertraulichkeit könnte wieder mit klassischen Verfahren zur Kommunikationssicherheit wie TLS oder IPsec erfolgen. Zur Sicherstellung der Aktualität sollten Kommunikationstechnologien mit einer hohen Verfügbarkeit eingesetzt werden. So sollten eher auf drahtlose Kommunikationstechnologien verzichtet werden, da Störungen des Funkkanals schnell zu Ausfällen führen können. Auch sind hierbei für einen Angreifer leicht DoS-Angriffe wie Jamming möglich. Auch aus Sicht des Datenschutzes ist eine kabelgebundene Lösung, z.B. die Nutzung von PLC über das Stromkabel, vorzuziehen. So muss zur Authentifizierung die ID des Fahrzeugs übertragen werden. Bei drahtloser Kommunikation

könnten diese IDs leicht (automatisiert) aufgezeichnet werden.

Referenzpunkt 5

Referenzpunkt 5 beschreibt die Kommunikation zwischen Fahrer und Ladesäule bzw. Ladeeinrichtung wenn ein Fahrstromvertrag an den Fahrer gebunden ist. In diesem Fall muss sich zumindest der Fahrer authentifizieren:

- Mechanismen zur Authentifizierung des Fahrers.

Wie bereits beschrieben, erfolgt die Authentifikation des Fahrers voraussichtlich mittels eines Authentifizierungstokens wie einer Smartcard. Hierzu kann in die Ladesäule ein Lesegerät für Authentifizierungstoken und ein PIN-Eingabefeld integriert sein. Alternativ kann die Kommunikation drahtlos z.B. mittels NFC erfolgen. Zur Absicherung dieser Kommunikation können wiederum kryptographische Protokolle wie TLS implementiert werden.

Referenzpunkt 6

Referenzpunkt 6 beschreibt die Sicherheitsmechanismen für die Ladesäule bzw. Ladeeinrichtung, wobei im Folgenden nur (halb-) öffentliche Ladesäulen betrachtet werden. Diese stehen in zugänglichen Bereichen und sind somit der Gefahr von Manipulationen, Vandalismus etc. ausgesetzt. Somit sind Mechanismen zum Schutz gegen Manipulationen an Hard- und Software der Ladesäulen umzusetzen. Auch ist zu überlegen, ob Ladestationen mit möglichst wenigen Funktionalitäten ausgestattet werden, so dass die Daten, die zwischen Fahrer bzw. Fahrzeug und der Abrechnungsstelle des Energieversorgers ausgetauscht werden, lediglich über die Ladestation weitergereicht werden, ohne dass die Station Einsicht in die Daten erhält. Zu dem minimalen Funktionsumfang einer Ladestation gehört, dass der verbrauchte Strom zum Laden korrekt durch ein Smart Meter erfasst und zur Abrechnung an den Energieversorger gesendet wird. Auch müssen die vom Energieversorger erhaltenen Preisinformationen korrekt dargestellt werden (z.B. durch ein Display an der Ladesäule) und aktuell sein.

Falls an der Ladesäule klassische Bezahlsysteme wie Bargeld, EC-Karte oder Kreditkarte vorgesehen sind, müssen geeignete Schutzmaßnahmen gegen Manipulationen wie Skimming-Angriffe, die mittlerweile auch an Tankstellen durchgeführt werden [31], und gegen Vandalismus getroffen werden. Mechanismen zum sicheren Bezahlen sind auch bei einer Abrechnung über Fahrstromverträge, die an den Fahrer gebunden sind, nötig. Dafür sind geeignete Schnittstellen wie z.B. Smartcard-Leser erforderlich.

Auch muss ein Datenschutz-konformer Umgang mit personenbezogenen Daten (Identität von Fahrer bzw. Fahrzeug, Ort und Zeitpunkt von Ladevorgängen etc.) sichergestellt werden.

Falls auf Ladesäulen zugegriffen wird, z.B. vom Messstellenbetreiber zur Wartung, müssen noch Mechanismen zur Authentifizierung und Autorisierung zugreifender Personen bzw. Komponenten umgesetzt werden.

Die umzusetzenden Sicherheitsmechanismen sind somit:

- Mechanismen zum korrekten Weiterleiten von Daten an den Energieversorger
- Mechanismen zum Schutz gegen Manipulationen

- Mechanismen zur sicheren Bezahlung
- Mechanismen zum Schutz personenbezogener Daten
- Mechanismen zur Authentifizierung und Autorisierung zugreifender Rollen.

Zur Umsetzung könnten wiederum hardwarebasierte Sicherheitsmodule wie HSMs genutzt werden. Diese müssen durch weitere Komponenten wie ein sicheres Display, sichere PIN-Eingabe etc. ergänzt werden. Der Schutz personenbezogener Daten kann am Einfachsten dadurch erfolgen, dass diese Daten lediglich verschlüsselt an den Energieversorger übertragen, aber nicht in der Ladesäule gespeichert werden.

Referenzpunkt 7

Dieser Referenzpunkt beschreibt die Kommunikation zwischen (halb- öffentlicher) Ladesäule bzw. Ladeeinrichtung zu Hause und dem Energieversorger. Die Sicherheitsmechanismen sind auf der hier durchgeführten noch recht abstrakten Ebene für die Kommunikation mit dem Heimat-Energieversorger und fremden Energieversorgern identisch.

Die zuvor beschriebenen Sicherheitsmechanismen sind auch zur Absicherung einer Ladeeinrichtung zu Hause, die mit Smart Meter und Gateway verbunden ist, sowie Ladesäulen umzusetzen. Bei öffentlichen Ladesäulen könnte einem Kunden ggf. direkt eine Rechnung an der Ladesäule ausgestellt werden. In diesem Falle müssten die übertragenen Rechnungsdaten noch abgesichert werden.

Die umzusetzenden Sicherheitsmechanismen sind somit:

- Mechanismen zum Schutz der Authentizität, Integrität, Vertraulichkeit und Aktualität der Messwerte, der Daten zur Abrechnung, Rechnungsdaten und Statusmeldungen
- Mechanismen zum Schutz der Authentizität, Integrität und Aktualität von Preisinformationen sowie von Steuerdaten
- Mechanismen zum Schutz der Authentizität und Integrität von Wartungsdaten.

Die Umsetzung dieser Sicherheitsmechanismen kann wie bereits beschrieben erfolgen.

Referenzpunkt 8

Referenzpunkt 8 beschreibt die Sicherheitsmechanismen für Heimat-Energieversorger und fremde Energieversorger.

Die Energieversorger empfangen Messwerte, Daten zur Abrechnung und Statusdaten und senden Rechnungsdaten, Preisinformationen, Steuerdaten und Wartungsdaten. Diese Daten müssen vertrauenswürdig, korrekt und rechtzeitig verarbeitet, gespeichert und weitergegeben werden.

Beispielsweise empfängt der Heimat-Energieversorger Messwerte und Daten zur Abrechnung wie z. B. die ID des Fahrzeugs, die genutzte Ladesäule und den Zeitraum des Ladens. Diese personenbezogenen Daten müssen dann zur Rechnungsstellung sicher gespeichert und verarbeitet werden, um anschließend die Rechnung zu versenden.

Wie bereits erwähnt, müssen die Energieversorger geeignete Maßnahmen ergreifen, um die Versorgungssicherheit zu gewährleisten.

Die umzusetzenden Sicherheitsmechanismen sind somit:

- Mechanismen zur Sicherstellung der vertrauenswürdigen, korrekten und rechtzeitigen Verarbeitung, Speicherung und Weitergabe von Messwerten, sowie der Daten

- zur Abrechnung, der aktuellen Verbrauchsdaten und Rechnungsdaten, Preisinformationen, Steuerdaten, Statusdaten, Wartungsdaten
- Weitere organisatorische Maßnahmen zur Sicherstellung der Versorgungssicherheit.

Eine mögliche Umsetzung wurde bereits in Kapitel 3.4 diskutiert.

Referenzpunkt 9

Dieser Referenzpunkt beschreibt die Sicherheitsmechanismen zur Absicherung der Kommunikation zwischen Heimat-Energieversorger und fremden Energieversorgern beim Energy-Roaming. Der Kunde lädt sein Fahrzeug bei einem fremden Energieversorger und die Abrechnung erfolgt über seinen Heimat-Energieversorger. Zur Abrechnung können (ggf. aggregierte) Messwerte, Daten zur Abrechnung, Preisinformationen und Rechnungsdaten ausgetauscht werden. Hier sind geeignete Mechanismen zum Schutz von Authentizität, Integrität und Vertraulichkeit sowie zum Datenschutz umzusetzen. Die umzusetzenden Sicherheitsmechanismen sind somit:

- Mechanismen zum Schutz der Authentizität, Integrität und Vertraulichkeit sowie zum Datenschutz von Messwerten, Daten zur Abrechnung, Preisinformationen und Rechnungsdaten.

Die Umsetzung kann wieder mit klassischen Verfahren zur Kommunikationssicherheit wie TLS oder IPsec erfolgen. Zum Datenschutz sind neben der verschlüsselten Übertragung noch weitere geeignete Konzepte zu untersuchen. Beispielsweise könnte darauf verzichtet werden, den Ort der Ladesäule und den Zeitraum der Ladung an den Heimat-Energieversorger zu schicken, so dass dieser keine Bewegungsprofile seiner Kunden erstellen kann.

6 Zusammenfassung

In diesem Artikel wurden mögliche Sicherheitsarchitekturen für die Domänen Privatkunde und Verteilnetz unter Berücksichtigung der Elektromobilität diskutiert. Hierzu wurden für jeweils relevante Anwendungsfälle vorgestellt und die wichtigsten Rollen beschrieben. Ausgehend von den Rechten und Pflichten der Rollen und den identifizierten Anwendungsfällen wurden Sicherheitsanforderungen abgeleitet. Für jede Domäne wurde eine Referenzarchitektur entwickelt, um anhand dieser darzustellen, wie diese Anforderungen in konkreten Architekturen umgesetzt werden könnten, d.h. an welchen Stellen, welche Verfahren und Kontrollen notwendig sind und welche konkreten Techniken hierfür in Betracht kommen.

Sobald konkret abzusehen ist wie die zukünftigen Smart Grids konkret realisiert werden, können die vorgestellten Sicherheits-Referenzarchitekturen entsprechend angepasst und die umzusetzenden Sicherheitsmechanismen weiter konkretisiert werden. Die vorgestellten Domänen-bezogenen Referenzarchitekturen, Rollenmodellierungen und abgeleiteten Sicherheitsanforderungen sowie Umsetzungshinweise verstehen wir als einen ersten Schritt in Richtung auf die Erstellung eines umfassenden Sicherheitskonzepts für Smart Grids. Dies wird in weiteren Schritt noch erheblich auszuweiten und zu vertiefen sein. So sind noch weit tiefergehende Bedrohungs- und auch Risikoanalysen notwendig und auch die Anwendungsfälle sowie Rollen sind sicherlich weiter zu verfeinern. Der Ansatz muss auf alle relevanten Domänen des Smart Grids ausgedehnt werden. Ein besonderes Augenmerk wird dann auf die Schnittstellen zwischen den Domänen und die Domänenübergänge zu legen sein, damit hier keine Sicherheits-Bruchstellen auftreten.

In den weiteren Schritten wird auch die enge Verflechtung von IT-Sicherheit und Betriebssicherheit noch weiter zu untersuchen sein, um zu Lösungen zu gelangen, die nachhaltig sowohl Funktions- und Betriebssicherheit als auch Daten- und Informationssicherheit gewährleisten.

Danksagung

Besonderer Dank gilt Herrn Harald Orlamünder, Ingenieurbüro für Informations- und Kommunikationstechnik in Ditzingen, sowie Frau Krista Grothoff und Herrn Sebastian Vogel vom Lehrstuhl Sicherheit in der Informatik an der TU München.

Literatur

[1] M. Brunner, H. Hofinger, C. Krauß, C. Roblee, P. Schoo, S. Todt. Infiltrating critical infrastructures with next-generation attacks: W32.Stuxnet as a showcase threat. Technical report, Fraunhofer SIT Munich, December 2010.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI). Protection Profile for the Gateway of a Smart Metering System, 2011.

[3] Deutsche Kommission Elektrotechnik Informationstechnik im DIN und VDE. Die deutsche Normungsroadmap E-Energy / Smart Grid, Version 1.0. Technical report, DKE, März 2010.

[4] C. Eckert. *IT-Sicherheit: Konzepte, Verfahren, Protokolle*. Oldenbourg-Verlag, 2011.

[5] C. Eckert, C. Krauß. Sicherheit im Smart Grid - Herausforderungen und Handlungsempfehlungen. *Datenschutz und Datensicherheit*, 8:535–541, 2011.

[6] C. Eckert, C. Krauß, P. Schoo. Sicherheit im Smart Grid - Eckpunkte für ein Energieinformationsnetz. Stiftung-Verbundkolleg / Projekt Newise Nr. 90, 2011.

[7] D. Ferraiolo, D. Kuhn. Role-based access control. In *15th National Computer Security Conference*, 1992.

[8] Heise Online. Meldung vom 19.11.2009. Intelligente Stromnetze: Ich weiß, ob du gestern geduscht hast. http://www.heise.de/security/meldung/Intelligente-Stromnetze-Ich-weiss-ob-du-gestern-geduscht-hast-864221.html.

[9] M-Bus standard. EN 13757. http://www.m-bus.com.

[10] NIST. Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References. NISTIR 7628, August 2010.

[11] H. Orlamünder. Der Einsatz von Informations- und Kommunikationstechnik in Stromnetzen - ein nachaltiges Energieinformationsnetz. Stiftung-Verbundkolleg / Projekt Newise Nr. 85, 2009.

[12] H. Orlamünder. Der Einsatz von Informations- und Kommunikationstechnik in Stromnetzen - ein nachhaltiges Energieinformationsnetz: Aspekte der technischen Kommunikation mit Schwerpunkt Verteilnetzautomatisierung und Elektromobilität. Stiftung-Verbundkolleg / Projekt Newise Nr. 93, 2011.

[13] D. L. U. Greveler, B. Justus. Hintergrund und experimentelle Ergebnisse zum Thema “Smart Meter und Datenschutz”. Technical report, FH Münster, September 2011.

[14] J. Schleich, M. Klobasa, M. Brunner, S. Gölz, K. Götz, G. Sunderer. Smart metering in Germany and Austria – results of providing feedback information in a field trial. Working Paper Sustainability and Innovation, No. S6/2011.

[15] eTelligence Projekt. http://www.etelligence.

[16] Telekommunikationsgesetz. http://www.gesetze-im-internet.de/tkg_2004/index.html

[17] Information and Privacy Commissioner, Ontario, Canada. SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation. November, 2009. http://www.futureofprivacy.org/wp-content/uploads/2009/11/smartprivacy-for-the-smart-grid.pdf

[18] P. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO), 1996.

[19] P. Kocher, J. Jaffe, B. Jun: Differential Power Analysis, Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO), 1999.

[20] Miele Pressemitteilung Nr. 095/2010. http://www.miele-presse.de/media/presse/media/2010-095_Miele_praesentiert_die_ersten_Smart-Grid-faehigen_Hausgeraete.pdf

[21] Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG) http://www.gesetze-im-internet.de/-bundesrecht/enwg_2005/gesamt.pdf

[22] A. Roßnagel, S. Jandt. Datenschutzfragen eines Energieinformationsnetzes. Stiftung-Verbundkolleg / Projekt Newise Nr. 88, 2010.

[23] Bundesamt für Sicherheit in der Informationstechnik (BSI). IT-Grundschutz-Kataloge https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/kataloge.html

[24] Bundesregierung. Regierungsprogramm Elektromobilität, 2011.

[25] Fraunhofer-Institut für System- und Innovationsforschung. Gesellschaftspolitische Fragestellungen der Elektromobilität, 2011.

[26] O. Kaiser, S. Meyer, J. Schippl. Elektromobilität - ITA-Kurzstudie. Düsseldorf : Zukünftige Technologien Consulting der VDI Technologiezentrum GmbH, 2011

[27] K. Mattes, C. Lerch, M. Schröter, K. Phan. Anwendungsfelder mobiler Energiespeicher – Eine Bestandsaufnahme und Perspektiven für die Konzeption aussichtsreicher Geschäftsmodelle für Elektrofahrzeuge. Fraunhofer-Institut für System- und Innovationsforschung, 2011.

[28] Bundesnetzagentur. „Smart Grid“ und „Smart Meter, 2011.

[29] O. Raabe, L. Mieke, F.Pallas, E. Weis. Datenschutz im Smart Grid und der Elektromobilität. Karlsruher Institut für Technologie, 2011.

[30] R. Sterbak. Pictures of the Future - Elektromobilität. Siemens. 2010.

[31] Heise Online. Meldung vom 23.02.2010. Skimming-Angriffe an Tankstellensäulen. http://www.heise.de/security/meldung/Skimming-Angriffe-an-Tankstellensaeulen-937855.html

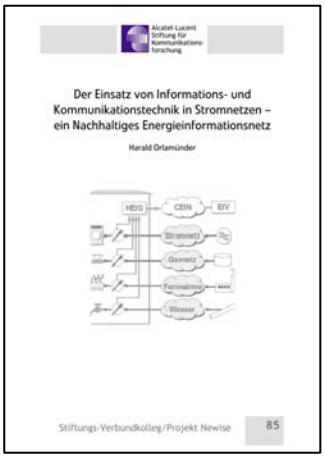
Autorin und Autor

Prof. Dr. Claudia Eckert ist Leiterin der Fraunhofer-Einrichtung für Angewandte und Integrierte Sicherheit (AISEC) in Garching bei München sowie Leiterin des Fachgebiets Sicherheit in der Informationstechnik des Fachbereichs Informatik an der Technischen Universität in München.

Dr. Christoph Krauß leitet den Bereich Innovation und Strategie am Fraunhofer AISEC in München. In enger Abstimmung mit der Institutsleitung ist er verantwortlich für die strategische Ausrichtung des Instituts und die Identifikation von innovativen Forschungsthemen. Weiterhin koordiniert er das Kompetenzfeld Smart Grid Security.

Publikationen

Die Publikationen können kostenfrei über das Stiftungsbüro der Alcatel-Lucent Stiftung bezogen werden.



Harald Orlamünder
Der Einsatz von Informations- und Kommunikationstechnik in Stromnetzen – ein Nachhaltiges Energieinformationsnetz

Stiftungsreihe Nr. 85

Alexander Roßnagel, Silke Jandt
Datenschutzfragen eines Energieinformationsnetzes

Stiftungsreihe Nr. 88

Claudia Eckert
Sicherheit im Smart Grid. Eckpunke für ein Energieinformationsnetz

Stiftungsreihe Nr. 90

Stefan Tenbohlen, Harald Orlamünder, Christian Müller-Elschner
Verteilen und Speichern von Energie im Smart Grid

Stiftungsreihe Nr. 93

Dirk Fox, Katharina Fuchs, Gerrit Hornung, Dieter Klumpp, Johann Kranz, Christoph Krauß, Klaus J. Müller, Alexander Roßnagel

Gestaltungslinien für Sicherheit und Datenschutz im Energieinformationsnetz

Stiftungsreihe Nr. 94

Alcatel-Lucent Stiftung

Die Alcatel-Lucent Stiftung für Kommunikationsforschung ist eine gemeinnützige Förderstiftung für Wissenschaft insbesondere auf allen Themengebieten einer „Informationsgesellschaft“, neben allen Aspekten der neuen breitbandigen Medien speziell der Mensch-Technik-Interaktion, des E-Government, dem Medien- und Informationsrecht, dem Datenschutz, der Datensicherheit, der Sicherheits-kommunikation sowie der Mobilitätskommunikation. Alle mitwirkenden Disziplinen sind angesprochen, von Naturwissenschaft und Technik über die Ökonomie bis hin zur Technikphilosophie.

Die Stiftung vergibt jährlich den interdisziplinären „Forschungspreis Technische Kommunikation“, Dissertationsauszeichnungen für WirtschaftswissenschaftlerInnen sowie Sonderauszeichnungen für herausragende wissenschaftliche Leistungen.

Die 1979 eingerichtete gemeinnützige Stiftung unterstützt mit Veranstaltungen, Publikationen und Expertisen ein eng mit der Praxis verbundenes pluridisziplinäres wissenschaftliches Netzwerk, in dem wichtige Fragestellungen der Informations- und Wissensgesellschaft frühzeitig aufgenommen und behandelt werden.

www.stiftungaktuell.de

Kontakt

Alcatel-Lucent Stiftung
Lorenzstraße 10, 70435 Stuttgart
Telefon 0711-821-45002
Telefax 0711-821-42253
E-Mail office@stiftungaktuell.de
URL: http://www.stiftungaktuell.de