DB-Spektrum manuscript No.
(will be inserted by the editor)

Die Smart-Metering-Debatte 2010-2016 und ihre Ergebnisse zum Schutz der Privatsphäre

Wird der technische Datenschutz und die Datensicherheit von Energieverbrauchsdaten gesetzlich effektiv gewährleistet?

Ulrich Greveler

22. April 2016

Zusammenfassung Die Energiewende wirkt sich auf den Umbau der Stromversorgung im Hinblick auf Datenhaltung und Datenübertragung in erheblicher Weise aus. Während in der Vergangenheit der Strom nur zum verbrauchenden Haushalt *hin* floss, ist das dezentrale organisierte und informationstechnisch aufgerüstete *Smart Grid* der Zukunft durch bidirektionalen Austausch und Aggregierung von Netzzustandsdaten gekennzeichnet. Eine wesentliche Komponente, die variable Tarife und bedarfsabhängigen Verbrauch im Haushalt ermöglicht, ist der digitale Stromzähler (Smart Meter), der nun gemäß gesetzlicher Vorgaben in alle privaten Haushalten Einzug finden soll.

Seit 2010 häufen sich Berichte über potentielle Angriffsflächen und Sicherheitslücken bei Smart-Metering-Systemen. Auch Datenschützer äußerten deutliche Bedenken, da die Auswertung von Energieverbrauchsdaten erhebliche Einblicke in die Privatsphäre der Kunden zulassen kann. In der dabei entstehenden Debatte, die um Forschungsergebnisse im Hinblick auf die Sensibilität der zu übertragenden Daten und mögliche Sicherheitsarchitekturen bereichert wurde, prallten energiepolitische Ziele, wirtschaftliche Interessen der Infrastrukturhersteller und Sicherheits- und Datenschutzbedenken, die von Verbraucherschützern und Datenschützern vorgebracht wurden, aufeinander.

Der Beitrag gibt einen Überblick über den Verlauf der Debatte seit 2010 und beschreibt das im Gesetzgebungsverfahren entstehende Ergebnis, das umfangreiche Regelungen zur Ausgestaltung der Sicherheitsanforderungen digitaler Messsystem enthält.

Prof. Dr.-Ing. Ulrich Greveler
Hochschule Rhein-Waal
Friedrich-Heinrich-Allee 25
D-47475 Kamp-Lintfort
E-Mail: mail@ulrich-greveler.de

Schlüsselwörter Smart Meter · Security · Privacy

1 Hintergrund

Die Bereitstellung einer nachhaltigen Energieversorgung als Teilaspekt der sogenannten *Energiewende* stellt ein zentrales energiepolitisches Ziel der Bundesregierung dar. Diese Energiewende wirkt sich auf den Umbau der Stromversorgung in Deutschland insbesondere im Hinblick auf die Aspekte Datenhaltung und Datenübertragung in erheblicher Weise aus. Während in der Vergangenheit der Strom nur zum verbrauchenden Haushalt *hin* floss ist das dezentrale organisierte und informationstechnisch aufgerüstete Stromnetz der Zukunft (als *Smart Grid* bezeichnet) durch bidirektionalen Austausch sowohl von Stromflüssen als auch von granularen Datenpunkten – sowie der Aggregierung von Netzzustandsdaten gekennzeichnet.

Das Konzept der Smart Grids ermöglicht eine Vielzahl von intelligenten, energietechnischen Innovationen: Es können beispielsweise virtuelle Kraftwerke realisiert werden, die eine Bündelung mehrerer Stromerzeuger (z. B. Photovoltaik, Windenergie und Biogasanlagen) und steuerbarer Großverbraucher (z. B. Kühlhäuser, die innerhalb von Toleranzen ihren Strombedarf variabel halten können) umfassen, so dass eine hohe Netzstabilität trotz volatiler Produktionsparameter erzielt wird. Mit der Anbindung privater Haushalte an dieses Grid wäre eine Möglichkeit geschaffen, die Abhängigkeit von konventioneller Energieerzeugung weiter zu reduzieren.

Mit dem 2016 beschlossenen[1] Gesetz zur Digitalisierung der Energiewende ist die Diskussion um Sicherheit und Datenschutz bei der Verarbeitung von Energieverbrauchsdaten, die bei einem flächendeckenden Roll-Out von Smart-Metern (digitalen Stromzählern) massenhaft anfallen werden, erneut aufgeflammt. Bisher nutzen private Haushalte fast ausschließlich elektromechanische Stromzähler (Ferraris-Zähler), die händisch abgelesen werden und — abgesehen von Tag-Nacht-Strom-Tarifen im Umfeld von Elektrospeicherheizungen — keine zeit- oder lastabhängige Tarifierung erlauben. Die digitalen Zähler sollen die alten Stromzähler ablösen und damit den Weg für die Digitalisierung des gesamten Stromnetzes ebnen. Smart Meter bezeichnen dabei alle digitalen Zähler, die Strom, Gas oder Wassermengen erheben, den Verbrauch digital anzeigen und in ein Kommunikationsnetz eingebunden sind.

Auf Seiten der Haushalte soll sich dabei viel verändern: Aus passiven Energiekonsumenten werden „Prosumer“, die unter Einbeziehung von Stromerzeugungs- und Stromspeicheranlagen in privater Hand an der Konzeptionierung des Stromversorgungssystems mitwirken und wirtschaftlich teilnehmen. Die Anforderungen an die unterstützenden Mess- und Übertragungstechnologien sowie an die Verarbeitung von Daten in Echtzeit zur Steigerung des Netzes bergen neuen Herausforderungen im Hinblick auf Datenschutz und Datensicherheit.

2 Ereignisse und Meilensteine

2.1 **2010**: Schutzprofile nach drittem Energiepaket

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde im September 2010 vom Bundesministerium für Wirtschaft und Energie (BMWi) beauftragt, Schutzprofile und Technische Richtlinien für die Kommunikationseinheit zukünftiger digitaler Messsysteme zu entwickeln. Ziel war die Erarbeitung eines einheitlichen technischen Sicherheitsstandards für alle Marktakteure. [1] Vorausgegangen war das *dritte Energiepaket*, das das Europäische Parlament im April 2009 verabschiedet hatte. Es enthielt die Empfehlung, dass 80 Prozent der Haushalte bis zum Jahre 2020 Smart Metering nutzen sollen.

Im Jahre 2010 häuften sich Presseberichte über potentielle Angriffsflächen, Datenschutzrisiken und reale Sicherheitslücken bei bis dahin eingesetzten Smart-Metering-Systemen. So schrieb Joshua Pennell in der ZEIT: „Diese neue Technik birgt gewaltige Gefahren. Sie eröffnet eine neue Front für Cyberangreifer.“[2] Insbesondere die Vorstellung, dass Angreifer via Internet Zugriff auf Smart-Meter nehmen und die Stromabnahme unterbrechen bzw. die Verbrauchsdaten abrufen könnten, bzw. infolge von massenhaften Eingriffen Blackouts (flächendeckende Stromausfälle) verursachen könnten, stellte ein Szenario dar, das in vielen Berichten aufgegriffen wurde. Dieses Szenario ist – in Abhängigkeit von der gewählten Systemarchitektur – keineswegs unrealistisch und wurde bei der Spezifikation von Sicherheitsanforderungen berücksichtigt, nicht zuletzt weil Energieversorgungsnetze eine kritische Infrastruktur darstellen. Smart-Meter-Lösungen, die eine Unterbrechung der Gesamtversorgung erlauben und die Schnittstellen gegenüber dem Internet aufweisen, spielten zwar in den Roll-Out-Pilotprojekten der Energieversorger in Deutschland keine Rolle, waren aber im Markt existent. Im April 2010 schreckte eine Meldung [15] die Branche auf, nach der eine US-Studie gravierende Sicherheitslücken bei intelligenten Stromzählern identifizierte. Schwächen des Datenprotokolls ZigBee ließen ein Ablauschen kryptographischer Schlüssel zu, womit Angreifer die Kontrolle über den Smart Meter erhalten könnten und sogar lokale Stromausfälle provozieren könnten. Der Angriff würde dabei nicht über ein WAN bzw. das Internet ausgeführt sondern erfolgte über einen ZigBee-Sender mit hoher Reichweite.

Molina-Markham et al. [7] stellten 2010 fest, dass Metering-Daten, die viertelstündlich erhoben werden, in einer Weise ausgewertet werden, dass feststellbar ist, wann sich Personen zuhause aufhalten, wann sie dort schlafen und wann sie Mahlzeiten zubereiten. Erhöht man die Granularität in den Minuten- oder Sekundenbereich, sind auch Aussagen möglich, ob das Frühstück warm oder kalt zubereitet wurde, wann Wäsche gewaschen oder der Fernseher eingeschaltet wurde – oder ob die Kinder alleine zu Hause waren.

2.2 **2011**: Energiewirtschaftsgesetz und unsichere Rollouts

Im Energiewirtschaftsgesetz (EnWG) und im so genannten Energiepaket, das vom Deutschen Bundestag im Juni 2011 beschlossen wurde, wurden Schutzprofile und Technische Richtlinien verankert. Zudem wurden Rollen und Akteure definiert: Der *Letztverbraucher* bezieht und verbraucht Energie und kann (soweit es eine natürliche Person ist) ein Recht auf informationelle Selbstbestimmung geltend machen. Der *Gateway-Administrator* administriert das Smart-Meter-Gateway beim Letztverbraucher, z. B. durch Einbau und Konfiguration. Der *Übertragungsnetzbetreiber* verbindet die

[1] Zum Erstellungszeitpunkt dieses Beitrages war noch nicht absehbar, zu welchem Zeitpunkt das Gesetz in Kraft tritt und welche Änderungen des Gesetzestextes im parlamentarischen Verfahren beschlossen werden.

Verteilnetze und transportiert Energie während der *Verteilnetzbetreiber* für die lokale Stromverteilung zum Letztverbraucher hin sorgt. Die letztgenannten Rollen sind daher zu unterscheiden vom *Energielieferanten*, der Strom liefert und abrechnet, dabei ggf. einen *Messstellenbetreiber* nutzt, der Messeinrichtungen betreibt und das Messsystem administriert.

Bei einer Untersuchung einer Arbeitsgruppe, die der Autor dieses Beitrages an der FH Münster leitete, wurde 2011 festgestellt, dass die Daten bei einem getesteten Metering-Anbieter unverschlüsselt und nicht signiert vom privaten Haushalt zu einer zentralen Stelle übertragen wurden. Dies stellte einen Verstoß gegen Grundsätze von Datenschutz und Datensicherheit dar. Diese Tatsache wog umso schwerer, da vom getesteten Anbieter vertraglich dem Endkunden zugesichert wurde, dass die Datenübertragung verschlüsselt erfolge. [4] Die getesteten Systeme entsprachen nicht dem gesetzlich verankerten Schutzprofil. Das Schutzprofil und die technische Richtlinien zur Gewährleistung von Datenschutz und Datensicherheit waren zu diesem Zeitpunkt nicht verbindlich, so dass der Verstoß sich hier auf die nicht erfüllte vertragliche Zusicherung beschränkte. Ein weiteres Detailergebnis der Untersuchung war, dass über die Auswertung der hier feingranular vorliegenden Daten (Abtastrate $0,5$Hz) eine Bestimmung des eingestellten Fernsehsenders auf dem im Haushalt befindlichen LCD-TV möglich war, was zu zahlreichen Presseberichten führte.

Seit 2011 hat das BSI gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, der Physikalisch-Technische Bundesanstalt und der Bundesnetzagentur das Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems entworfen und nach Einarbeitung von Kommentierungen der Verbände und von Verbraucherschutzorganisationen fortgeschrieben. Insgesamt sind nach BSI-Angaben mehr als 1200 Kommentare eingereicht worden, womit das „hohe Interesse, das dem Thema in Fachkreisen und zunehmend auch in der Politik beigemessen wird“[5] belegt werde. Schutzprofile und technische Richtlinie legen verbindliche und einheitliche Mindeststandards sowie Vorgaben zur Funktionalität der Messsysteme und deren Interoperabilität fest.

2.3 **2012**: Starker Widerstand der Datenschützer

Im März 2012 hat die Europäische Kommission Empfehlungen zur Vorbereitung für die Einführung intelligenter Messsysteme amtlich bekanntgemacht, die den Schutz personenbezogener Daten bei Erfassung und Verarbeitung durch intelligente Messsysteme einfordern. In Bezug auf Datensicherheit wird explizit Verschlüsselung als wesentliche Maßnahme benannt. Zudem wird die Bereitstellung einer sicheren Datenkommunikation beschrieben, die sowohl die Angebots- als auch die Nachfrageseite betrifft. Ein hohes Sicherheitsniveau sei gemäß der EU-Empfehlungen für die gesamte Kommunikation zwischen dem Zähler und dem Betreiber unerlässlich. Dies gelte sowohl für die direkte Kommunikation mit dem Zähler als auch für alle Mitteilungen, die über den Zähler zu oder von Geräten oder Steuerungen in den Räumlichkeiten des Kunden erfolgen. [9]

Im Mai 2012 meldete sich der EU-Datenschutzbeauftragte Peter Hustinx zu Wort und warnt in seiner Stellungnahme [14] vor der Einführung intelligenter Messsysteme in Europa. Mit den neuen Geräten könnten Mitglieder eines Haushalts in ihren eigenen vier Wänden ausgeforscht werden, man könne feststellen, ob sie im Urlaub oder auf der Arbeit sind oder ob sie medizinische Geräte benutzen und welches Freizeitverhalten sie auszeichne. In Verbindung mit Daten aus weiteren Quellen ergäbe sich Auswertemöglichkeiten über Data Mining, was Gefahren wie tiefe Einblicke in die Privatsphäre oder Preisdiskriminierung durch Anbieter berge. (Vgl. dazu auch Tabelle 1.)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und Düsseldorfer Kreis hat im Juni 2012 eine *Orientierungshilfe datenschutzgerechtes Smart Metering* [10] herausgegeben. Das Dokument betrachtet die gesamte Prozesskette der Verarbeitung personenbezogener Daten: Das Messen von Strommengen mittels digitaler Zähler, die Verarbeitung im Smart Meter / lokalen Messsystem und die weitere Nutzung durch sämtliche Stellen, die an der Stromlieferung, -verteilung und -mengenabrechnung beteiligt sind. Besonderes Augenmerk wird in der Orientierungshilfe auf den Punkt *Privacy by Design* gelegt: Die Gewährleistung des Datenschutzes müsse bereits bei der Konzeption und Gestaltung der Messsysteme erfolgen. Der Ansatz *Privacy by Design* verfolgt dabei, Datenschutz von Beginn an in die Gesamtkonzeption einzubeziehen anstatt Schwachstellen nach der Implementierungsphase mit hohen Aufwänden zu beheben. Darüber hinaus müsse der Letztverbraucher über die bei ihm installierte Technik „alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen.“ Die Orientierungshilfe bewegt sich dabei im Rahmen der zuvor genannten EU-Empfehlungen und präzisiert diese durch die Spezifikation von Use Cases, die mit einer dreiteiligen Bewertungsskala (normal, hoch und sehr hoch) den Datenschutzbedarf für jeden Use Case festlegt. So wird beispielsweise der Use Case „Datenbereit-

Tabelle 1 Datenschutzverletzungen beim Einsatz von Smart Metern. Quelle: McKenna et al., 2012 [16]; zitiert nach Dietrich, 2015 [17]

Interessengruppe	Beispiele
Illegale Nutzung	Einbrecher können Einbruchsziele ausmachen.
	Stalker können ihre Opfer beobachten
Kommerzielle Nutzung	Gezielte Werbung, basierend auf den Smart Meter Daten eines Haushalts oder Individuums.
	Versicherungen könnten z. B. überprüfen, ob ihre Kunden die elektronischen Geräte tatsächlich ausschalten, wenn sie das Haus verlassen
Staatliche Exekutivorgane	Aufdeckung von illegalen Aktivitäten, wie z. B. Drogenanbau.
	Überprüfung von Alibis: z. B. war der Tatverdächtige tatsächlich den ganzen Abend Zuhause?
Andere Parteien in Rechtsstreitigkeiten	Im Sorgerechtsstreit: Wird das Kind alleine Zuhause gelassen?
	Bei Streitigkeiten mit dem Vermieter: Leben mehr Menschen im Wohnobjekt als erlaubt?
Familienmitglieder oder Mitbewohner	Haushaltsmitglieder spionieren einander aus, z. B.: Eltern können überprüfen, ob die Kinder schlafen oder lange wach bleiben und Videospiele spielen.
	Partner können sich gegenseitig überwachen.

stellung für Zu- und Abschalten von Lasten“ mit *hoch* bewertet, da eine Profilbildung durch Verbrauchsdaten von unterbrechbaren Verbrauchseinrichtungen (Weiße Ware[2]) nicht ermöglicht werden darf.

[2] Zur *Weißen Ware* werden Waschmaschinen, Geschirrspülmaschinen, Gefriertruhen und weitere elektrische Kleingeräte gezählt. Diese Geräte bieten neben den zu ladenden Akkumulatoren von Elektrofahrzeugen ein besonderes Potential, vom intelligenten Netz gesteuert (z. B. zeitweise von der Stromabnahme gehindert) zu werden, um eine Netzstabilisierung und optimale Auslastung zu erzielen.

2.4 **2013/14**: Skepsis bei Energiewirtschaft, weitere Sicherheitspannen

Eine Studie von Ernst & Young im Auftrag des BMWi [13] empfiehlt 2013, dass bis 2022 zwei Drittel aller deutschen Haushalte mit neuen Zählern ausgestattet werden. Dabei wird ein behutsamer Roll-Out angestrebt: 20 Millionen Haushalte sollten Smart Meter ohne Kommunikationsmöglichkeiten erhalten; bei 12 Millionen kommt ein Meter mit verbundenem Gateway zur Datenübertragung zum Einsatz. Dieses Roll-Out-Szenario soll nach Ergebnissen der Studie einen volkswirtschaftlichen Nutzen von bis zu 13 Milliarden Euro bringen, der sich über die kommenden 20 Jahre verteilt.

Die Studie von Ernst & Young wird vom BMWi genutzt, die Debatte um das Argument der positiven volkswirtschaftlichen Effekte zu bereichern, sie liefert aber auch den Kritikern Munition, da sie für den Löwenanteil der Stromkunden keine Ersparnis prognostiziert: Die EU-Vorgabe führe „für den Großteil der Endkunden zu unverhältnismäßig hohen Kostenbelastungen“ [13]. Da die Autoren der Studie ganz unverblümt auch eine „weitergehende Nutzung der Daten durch Dritte“ als Geschäftsmodell ins Spiel bringen, wird die Studie auch in Presseberichten sehr kontrovers rezipiert. So schreibt Kai Biermann in der ZEIT [3] unter der Überschrift „Stromkunden sollen sich überwachen lassen – und dafür zahlen“: „Die Stromkunden sollen also nicht nur für die teuren Zähler zahlen, sie sollen später auch noch ihre persönlichen Daten vermarkten lassen.“ und er zitiert Patrick Breyer, aktiv im Arbeitskreis Vorratsdatenspeicherung, mit den Worten: „Eine zwangsweise Fernübertragung unseres Stromverbrauchs in Echtzeit wäre ein Alptraum für unsere Privatsphäre in den eigenen vier Wänden.“

Aber auch aus dem Bereich der Energiewirtschaft und dem Elektroingenieurwesen wird der umfassende Nutzen des Smart Metering angezweifelt, hier auch im Hinblick auf die beabsichtigte netzstabilisierende Wirkung. Als Echtzeit-Sensor für die Messung der Energieabnahme sind die Geräte aufgrund der Übertragungslatenzen und geringen Abtastraten aus Sicht vieler Stromtechnikexperten eher ungeeignet. So schreibt Achim Leitner im elektronikJOURNAL, Editorial des Chefredakteurs (Juni 2013): „Brancheninsider gehen davon aus, dass man die Metering-Daten besser nicht zur Grid-Automatisierung heranzieht, sondern sie bei ihrer ursprünglichen Aufgabe belässt: Stromverbauch messen, die Daten zur Abrechnung bereitstellen und dem Verbraucher jederzeit eine detaillierte Aufstellung geben.“ [18] Die für für das Gateway vorgesehenen Sicherheitsanforderungen stoßen ebenfalls auf wenig Gegenliebe bei den Technikexperten. Der Vorwurf,

dass bei der Anforderungserstellung fachlich nur eingeschränkt ausgebildete Informatiker zuwerke gegangen seien, die zu wenig Kenntnisse der Stromtechnik aufweisen, wird kaum verklausuliert in einem Beitrag des Siemens-Wissenschaftlers David von Oheimb im gleichen Magazin [19] deutlich: „IKT-Security-Experten sind in der Regel nicht mit der Anwendungsdomäne der Energienetzwerke vertraut und neigen daher dazu, Randbedingungen zu übersehen, die durch ihre physikalischen, organisatorischen und wirtschaftlichen Charakteristiken gegeben sind."; im Teasertext wird zusammengefasst: „Das Ergebnis ist viel Aufwand mit so gut wie keinem Nutzen."

Auf der Sicherheitskonferenz *Black Hat Europe* 2014 beschrieben Alberto Garcia Illera und Javier Vazquez Vidal [20] wie sie in Spanien weit verbreitete intelligente Stromzähler manipulieren konnten, nachdem sie feststellten, dass diese zwar eine kryptographische Absicherung aufwiesen, der verwendete symmetrische 128-Bit-AES-Schlüssel jedoch in vielen Zählern verwendet wurde und aus der Firmware extrahiert werden konnte. Da der Verbindungsaufbau zum Zähler über das Stromnetz erfolge, könnten sie die Geräte massenhaft manipulieren und einen Stromausfall in einem Stadtviertel auslösen.

Kurzzeitig deutet die Bundesregierung einen Kurswechsel an und stellt den Smart-Meter-Rollout in Frage. Wirtschaftsstaatssekretär Rainer Baake distanziert sich öffentlich beim Berliner Energiekongress von der verpflichtenden Einführung. Das Handelblatt schrieb dazu: „Der Einbau sogenannter intelligenter Stromzähler in Wohnungen wird von der Bundesregierung nicht mehr forciert. Für Haushalte sei dies [nach Aussage von Baake] zu teuer und lohne sich nicht"[22]. Dieser vermeintliche Kurswechsel war aber nur von kurzer Dauer, denn wenige Monate später ist in einer Pressemitteilung des BMWi zu lesen: Es ist „das Ziel des Bundeswirtschaftsministeriums, auf Basis der nun veröffentlichten Eckpunkte [für das Verordnungspaket *Intelligente Netze*] verlässliche rechtliche Rahmenbedingungen für den sicheren Einsatz von Intelligenten Messsystemen auf den Weg zu bringen." [21]

2.5 **2015**: Gesetzesentwurf zur verpflichtenden Metering-Einführung

Die angekündigten rechtlichen Rahmenbedingungen wurden im September 2015 konkretisiert als das BMWi auf Basis der Konsultationsergebnisse zum Verordnungspaket einen Referentenentwurf für ein Gesetz zur Einführung des Smart-Metering vorlegte. Das Tempo wurde nun merklich erhöht: Länder und Verbände hatten zwar Gelegenheit sich zum Entwurf äußern, jedoch nur noch bis zum Oktober 2015, da das Kabinett und der Bundesrat sich noch im gleichen Jahr mit dem Gesetz befassen sollten.

Der finale Gesetzesentwurf zum *Gesetz zur Digitalisierung der Energiewende* wurde vom Bundeskabinett im November 2015 beschlossen. Der Text berücksichtigt dabei Hinweise und publizierte Forschungsergebnisse, die aus Fachdiskussionen und wissenschaftlichen Untersuchungen stammen und die Schwachstellen bei vorhandenen Smart-Meter-Infrastrukturen aufzeigten. Es wird insbesondere deutlich, dass die Sensibilität von granularen Stromverbrauchsdaten von den Gesetzesautoren berücksichtigt wurde. Eine Duldungspflicht seitens der Letztverbraucher wurde im Entwurf zwar verankert, sie erstreckt sich jedoch allein auf Daten, die viertelstündlich erhoben und innerhalb der häuslichen Infrastruktur gespeichert werden. Diese Daten sind zwar granulare Energieverbrauchsdaten und lassen Rückschlüsse auf Lebensgewohnheiten und Anwesenheitszeiten zu, sie sind jedoch nicht *fein*granular und verwischen daher Informationen, die bis in die Intimsphäre reichen können. Im Einzelnen lassen sich folgende zentralen Punkte im Gesetzesentwurf feststellen.

- Schutzprofile und technische Richtlinien zur Gewährleistung von Datenschutz und Datensicherheit werden nun verbindlich. Damit dürfen unsichere Gateways nicht mehr eingesetzt werden, und ein drohender Wildwuchs bei technischen Realisierungen von Datenschutzanforderungen wird frühzeitig beendet.
- Zu sendende Daten werden vom Smart-Meter-Gateway verschlüsselt und signiert. Damit werden elementare Standards bei der Durchsetzung von Datensicherheit gesetzlich festgeschrieben.
- Gesetzlich vorgegeben wird gemäß Entwurf, dass standardmäßig 15-Minutenwerte im Messsystem vorhanden sind. Diese werden aber nicht notwendigerweise übertragen. Die gespeicherten Werte könnten beispielsweise für die Visualisierung des Stromverbrauchs genutzt werden, um dem Letztverbraucher hausintern Energiekosteneinsparpotentiale aufzuzeigen. Unklar bleibt, wie zukünftig ein behördlicher Zugriff auf diese im Messsystem gespeicherten Daten erfolgen könnte, beispielsweise im Zuge von Ermittlungsverfahren oder bei strafprozessualer Durchsuchung. Eine behauptete häusliche Anwesenheit seitens eines Tatverdächtigen könnte durch Auswertung der Daten widerlegt oder mindestens begründet angezweifelt werden.
- Ob Daten übertragen werden, regeln die Vorschriften des dritten und vierten Teils des Gesetzesentwurfs. Es darf, soweit der Letztverbraucher keinen variablen Tarif vereinbart hat und keine steuerba-

ren Geräte betrieben werden, standardmäßig nur ein Wert pro Abrechnungsjahr nach außen übertragen werden. Für die meisten Haushalte wird die Infrastruktur daher keine Änderung im Hinblick auf die zu Abrechnungszwecken übermittelte Information bewirken.
– Technische Richtlinien des BSI, die Sicherheitsanforderungen an das Smart-Meter-Gateway, das Sicherheitsmodul und die Administration des Gateways vorsehen, werden erneut gesetzlich verankert. Zudem werden kryptographische Vorgaben formuliert und eine Schlüsselinfrastruktur wird vorgezeichnet. Die Richtlinien und Vorgaben sind dabei umfassend, vergleichsweise streng und gehen insbesondere hinsichtlich der Komplexität über die aus Datenschützersicht formulierten Erwartungen hinaus. Dies geschah offenbar vor dem Hintergrund, dass intelligente Stromnetze als zukünftige, kritische Infrastruktur gesehen werden, deren Schutz besondere Priorität seitens der Bundesregierung genießt.
– Die Einbaupflicht beginnt zwar bereits im Jahre 2017 (ab 10.000 Kilowattstunden pro Jahr) aber erst 2020 für private Haushalte, die typischerweise 10.000 Kilowattstunden deutlich unterschreiten.

Der Gesetzesentwurf wurde noch vor seiner Verabschiedung durch das Bundeskabinett von Verbraucherschützern scharf kritisiert. Der Verbraucherzentrale Bundesverband veröffentlichte im Oktober 2015 eine Erklärung, die einen erheblichen Eingriff in die Grundrechte seitens des Gesetzgebers feststellt und die Energiewende dabei als bloß vorgeschobenen Zweck ausmacht. Experten seien sich nach dieser Erklärung einig, „dass für ein sicheres und effizienteres Stromnetz aggregierte Daten eines Straßenzugs oder eines Viertels vollkommen ausreichten.“ Aus Sicht des Verbraucherzentrale Bundesverband gehe der Trend vielmehr zu autonomen Lösungen innerhalb eines Haushalts, was intelligente Messsysteme und moderne Zähler überflüssig machen würde. [11] Trotz der Schärfe der Kritik (der Vorwurf der „Zwangsdigitalisierung“ wird erhoben) wird deutlich, dass Bedenken zu Datenschutz und insbesondere zur Datensicherheit nicht im Vordergrund stehen. Die Kritik fokussiert sich vielmehr auf den Kostenaspekt und die erzwungene Duldung des Einbaus von Messsystemen. Anerkannt wird hingegen, dass „mit dem Gesetzesentwurf und den Schutzprofilen eine Vielzahl von Regelungen getroffen, die zu mehr Standards und damit auch zu mehr Sicherheit führen werden“. Kritisch wiederum wird gemäß der Stellungnahme gesehen, dass „dem Grundprinzip *privacy by default* nicht ausreichend Rechnung getragen“ werde, weil Nutzer datensparsamere Einstellungen des Gateways in eigener Initiative verlangen müssten. Das Prinzip *privacy by default* sieht datenschutzfreundliche Voreinstellungen vor und ist ein Kernbestandteil der für das Jahr 2016 vorgesehenen EU-Datenschutzreform.

In einer Sitzung des Bundesrates im Dezember 2015 wurde eine umfangreiche Stellungnahme [8] zum Gesetzentwurf zur Digitalisierung der Energiewende verabschiedet. Darin wird angemerkt, die im Entwurf vorgesehene Speicherfrist für Energieverbrauchswerte im Sinne des Verbraucherdatenschutzes von 24 auf zwölf Monate verkürzen. Letztverbraucher mit einem Jahresverbrauchsvolumen von bis zu 6000 Kilowattstunden sollten gemäß der Stellungnahme die Anbindung ihres Messsystems an ein Kommunikationsnetz ablehnen können. Bei Privathaushalten solle jede Ausstattung mit intelligenten Messsystemen allein auf freiwilliger Basis (Opt-Out-Möglichkeit) geschehen.

2.6 Berücksichtigung der Sicherheitspannen und Debattenbeiträge

Der Gesetzesentwurf zeigt, dass die jahrelange Debatte um Nutzen und Gefahren der Metering-Infrastruktur von den Ministerien registriert wurde und dass Sicherheitsmindestanforderungen an die technischen Komponenten gestellt werden, um Gefahren in Bezug auf Sicherheit einer kritischen Infrastruktur und Schutz personenbezogener Daten zu reduzieren. Das Schutzprofil wurde während der Debatte weiterentwickelt und nach zahlreichen Kommentaren mehrfach ergänzt. Das Ergebnis dieses Entwicklungsprozess wird im folgenden Abschnitt betrachtet.

3 Gateway: Sicherheitsanforderungen des BSI

3.1 Schutzprofil und Technische Richtlinie

Ein Schutzprofil gemäß Common Criteria [12] beschreibt mögliche Bedrohungen eines zu evaluierenden Gegenstandes und legt u. a. Mindestanforderungen für Sicherheitsfunktionen fest, fasst die Sicherheitsziele abstrakt zusammen und gibt Annahmen über die Einsatzumgebung vor. Anhand des Schutzprofils kann eine Evaluierung des Gegenstandes durch eine unabhängige Prüfstelle erfolgen, die bei positivem Verlauf in ein Zertifikat mündet, das den Nachweis der Einhaltung des Schutzprofils bestätigt.

Das vom BSI herausgegebene Schutzprofil [5] für Smart-Meter-Gateways definiert die Schnittstellen und sicherheitstechnische Anforderungen für diese Schnittstellen. Zudem werden die potentiellen Bedrohungen

des Gateways nach Angreifertypen unterschieden: lokale Angriffe, netzbasierte Angriffe, Angriffe auf die Systemuhr, etc. Diesen Bedrohungen werden die Sicherheitsziele gegenübergestellt. Die Sicherheitsanforderungen im fast einhundert Seiten umfassenden Schutzprofil sind generischer Natur und wurden technologieunabhängig spezifiziert. Die vorgesehene Stufe der Vertrauenswürdigkeit Common-Criteria-EAL4+ für das Gateway stellt für die Hersteller eine gewisse Herausforderung dar, da sie sich auf demselben Level bewegt, das beispielsweise regelmäßig für die Zertifizierung von Banking-Smartcards, Sicherheitsmodulen, Signaturkomponenten, Patientenkarten oder Generatoren kryptographischer Schlüssel vorgeschrieben ist.

Um eine Interoperabilität der in den Messsystemen eingesetzten Komponenten zu erzielen und um die im Schutzprofil abstrakt definierten Sicherheitsanforderungen zu konkretisieren, wurde eine Technischen Richtlinie des BSI (TR-03109) [6] erstellt und gepflegt. Diese Technische Richtlinie macht in Bezug auf die Sicherheitsfunktionen beispielsweise konkrete kryptographische Vorgaben und definiert eine Public-Key-Infrastruktur. Es werden auch betriebliche Anforderungen an den Gateway-Administrator zur Durchsetzung der Informationssicherheit gestellt; so muss dieser eine Zertifizierung gemäß ISO/IEC 27001 oder eine gleichwertige Qualifizierung erbringen, damit er tätig werden kann. Es wird eine weitere Überarbeitung der Technischen Richtlinie mit Fertigstellung im Laufe des Jahres 2016 erwartet, so dass (nach Einschätzung von Branchenvertretern) mit einer Fertigstellung und dem Roll-Out erster konformer und zertifizierter Gateways nicht vor 2017 gerechnet wird.

3.2 Smart-Meter-Gateway

Das lokale Messsystem enthält als Kernkomponente eine Einheit zur Übertragung von Daten, dem *Smart-Meter-Gateway*, welches die im Haushalt (oder in einer anderen lokal begrenzten Struktur) verbauten Messeinrichtungen mit anderen Akteuren (z. B. Betreiber des Verteilnetzes, Stromlieferant oder Gateway-Administrator, der im Auftrag des Messstellenbetreibers handelt) verbindet. Messeinrichtungen werden in einem Lokalen Metrologischen Netz (LMN) zusammengefasst. Steuerbare Verbraucher (Controllable Local Systems, CLS) kommunizieren direkt mit dem Gateway (vergl. Abb. 1).

Sämtliche Kommunikationsverbindungen gehen in der vom BSI vorgezeichneten Systemarchitektur vom Smart-Meter-Gateway selbst aus. Es gibt keine eingehenden Kommunikationsverbindungen, wodurch die Angriffsfläche gegenüber netzbasierten Angriffstechniken deutlich gemindert wird. Ausgehende Verbindungen können ereignisbasiert oder regelmäßig (z. B. viertelstündlich) durch das Gateway aufgebaut werden. Vorgesehen ist jedoch ein WakeUp-Dienst, der es dem Gateway-Administrator erlaubt, den Verbindungsaufbau über ein signiertes Datenpaket zu einer vordefinierten Adresse anzustoßen und anschließend administrative Aufgaben auszuführen. Eine Beschränkung der zeitlichen Gültigkeit des Pakets erschwert dabei Replay-Angriffe. Grundlage aller bereitgestellten Schnittstellen ist Transport Layer Security (TLS), um Vertraulichkeit, Authentizität und Integrität bei der Datenübertragung umzusetzen. Das Gateway kommuniziert dabei intern mit einem Sicherheitsmodul, das als gesondert zertifizierte Einzelkomponente die kryptographischen Funktionen bereitstellt und als persistenter Speicher für Schlüssel und Zertifikate dient.

Für den Letztverbraucher existiert eine Schnittstelle (Home Area Network, HAN), die es ihm ermöglicht, Verbrauchsdaten oder (sofern er auch Strom produziert) Einspeisemessungen abzufragen. Dazu kann er einen PC, ein Tablet oder ähnliche Geräte mit der Schnittstelle verbinden; der Zugriff erfolgt dann ausschließlich lesend und erfordert eine sichere Authentifizierung. Beschrieben wird zudem ein dediziertes, „kryptographisch gesichertes Display“ welches den abgesicherten Datenstrom empfängt und Verbrauchsdaten (u. a.) visualisiert.

Der Verbraucher wird über diese Schnittstelle in die Lage versetzt, eine (fein-)granulare Übersicht über seinen Verbrauch zu erhalten, ohne dass hoch aufgelöste Verbrauchsdaten an Betreiber übertragen werden müssen. Gateway-Transaktionen wie die Übertragung von Abnahmemengen werden in einem Letztverbraucher-Log vermerkt. Nur ein authentifizierter und autorisierter Letztverbraucher kann die ihn betreffenden Daten über die HAN-Schnittstelle abrufen und Übertragungsvorgänge nachverfolgen. Zudem kann er Änderungen von benutzerbezogenen Daten verifizieren. Auch Servicetechniker, die lokal eingesetzt sind, greifen nach Authentifizierung über die HAN-Schnittstelle auf das Messsystem zu. Das Gateway schottet das lokale Netz gegenüber anderen verbundenen Netzen über Filterfunktionen ab; es dient daher als Firewall für die zu schützenden Messeinrichtungen innerhalb des Heimnetzes.

Über Tarif- und Berechtigungsprofile werden dem Gateway die verbrauchervertraglichen Konditionen (Tarif, Ableseintervalle, Datenempfänger) bekannt gemacht. Die Technische Richtlinie sieht daher ein Datenmodell für Tarifprofile vor, das im Gateway implementiert wird. In den Tarifprofilen werden die vertraglichen

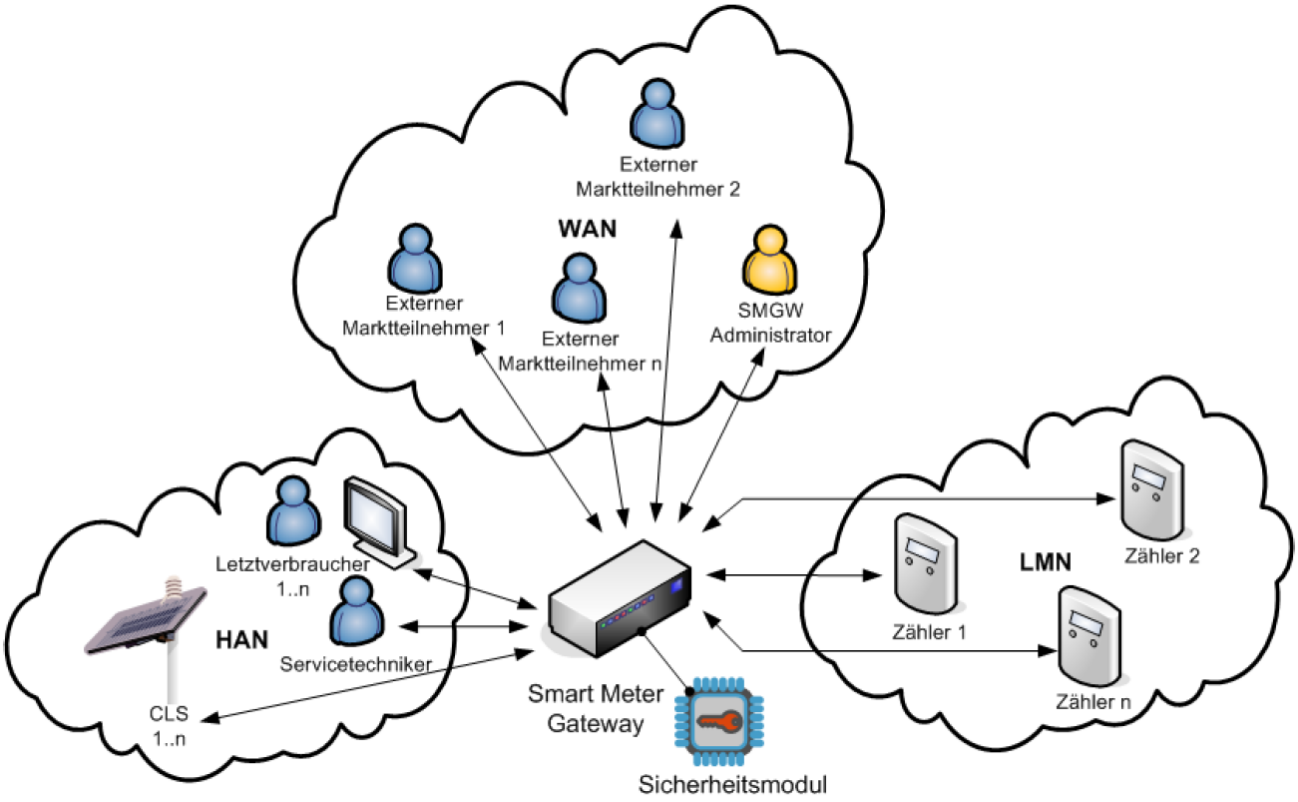

Abb. 1 Einbettung des Gateways in seine Einsatzumgebung, Bildquelle: TR-03109 [6], Seite 14

Nutzungsbedingungen zwischen dem Letztverbraucher und weiteren Akteuren in Form von Rollen und darauf bezogenen Zugriffsrechten abgebildet.

Die in der Einbaupraxis in privaten Haushalten als übliche Konfiguration auftretende Lösung, dass ein als Smart Meter bezeichnetes Gerät das Gateway neben der Messeinrichtung innerhalb seines Gehäuse integriert, wird im Schutzprofil als *One Box Solution* bezeichnet und explizit als bevorzugte Implementierung des Messsystems für Einfamilienhäuser u. a. benannt. Aber auch bei diesen Lösungen wird das Gateway als eigenständige Einheit betrachtet, die die Anforderungen gemäß Schutzprofil und Technischer Richtlinie erfüllen muss.

3.3 Public Key Infrastruktur

Die sichere Kommunikation über Weitverkehrsnetze wird für die Gateways über die Nutzung einer Public Key Infrastruktur (PKI) realisiert. Das BSI nimmt dabei die Rolle der Smart-Metering-Wurzelzertifizierungsinstanz (SM-Root-CA) ein, die das Ende der Zertifikatskette bildet. Für Akteure der Smart-Metering-Infrastruktur werden Zertifikate eingesetzt, die von kommerziellen Anbietern (Sub-CAs) unterhalb der SM-Root-CA, d. h. nicht vom BSI bzw. seinem mit der technischen Realisierung beauftragten Zertifizierungsdiensteanbieter selbst, ausgestellt werden. Der private Schlüssel zum Wurzelzertifikat wird in besonderer Weise geschützt und nur dazu eingesetzt, die Sub-CA-Zertifikate zu signieren.

Mithilfe dieser Zertifikate können sich die Akteure gegenseitig authentisieren und für den Datenaustausch einen verschlüsselten und integritätsgesicherten Kanal eröffnen. Da zu sendende Daten (z. B. die Stromabnahmemenge) vom Gateway zusätzlich auf Datenebene verschlüsselt und signiert wird, ist regelmäßig von einer Mehrfachverschlüsselung der Daten auf dem Übertragungsweg auszugehen.

Allein für die Definition der PKI wurde ein gesonderter Teil 4 der Technischen Richtlinie TR-03109 [6] erstellt, der auf ca. 60 Seiten Zertifikatslaufzeiten, Verzeichnisdienste, Strukturen der Datenfelder, Zertifikats-Extensions für Endnutzer-Zertifikate, unterstützte elliptische Kurven und Attribute der Verzeichniseinträge normativ feinspezifiert.

3.4 Keine Unterbrechung der Stromversorgung des Haushaltes

Abseits der steuerbaren Verbraucher sieht das Schutzprofil für das Gateway keine Funktion vor, dass der Haushalt vom Stromnetz getrennt wird. Eine solche Maßnahme könnte beispielsweise für Kunden mit Zahlungsrückstand eingesetzt werden. Neben dem umstrittenen verbraucherpolitischen Aspekt, ob solche Mechanismen von der Regierung überhaupt gewollt sind, birgt eine solche Funktion ein besonderes Risiko, da bei einem erfolgreichen Angriff auf das Gateway die Auswirkung auf den einzelnen Verbraucher (Funktionsverlust fast sämtlicher elektrischen Geräte) als auch auf das Stromnetz (potentielles kaskadierendes Versagen der Netze bei plötzlichem Trennen vieler Haushalte) erheblich wäre. Zudem könnte auch bei einer Fehlfunktion des Gateways die Trennung des Netzes ausgelöst werden, was gegen eine technische Implementierung der Trennungsvorrichtung insgesamt spricht. Im Schutzprofil wird dazu in einer Fußnote ausgeführt: „Even an intentional stop of the delivery of a certain commodity is not within the scope of this Protection Profile“. Es wird jedoch nicht vorgegeben, dass eine solche Unterbrechungsfunktion nicht durch weitere verbaute Komponenten realisiert wird.

4 Fazit

Der Gesetzgeber hat bei der Ausgestaltung des Gesetzes zur Digitalisierung der Energiewende den Bedenken von Datenschützern und Verbraucherschützern in Bezug auf Datenschutz und Datensicherheit in umfassender Weise Rechnung getragen. Offenbar wurden auch Forschungsergebnisse, die die Sensibilität von Energieverbrauchsdaten nachgewiesen hatten, in die Betrachtungen einbezogen, da auf die Granularität der zu speichernden bzw. zu übertragenden Daten ein deutliches Augenmerk gelegt wurde. Der entwickelte Rechtsrahmen hat hier klare und verlässliche Vorgaben getroffen.

Die technischen Vorgaben eines *privacy-by-design*-Ansatzes über Schutzprofil und Technischen Richtlinie setzen um, dass der zulässige Datenverkehr, der durch den Einsatz von Smart Metern deutlich zunimmt, über die gesetzliche Verankerung abschließend rechtlich geregelt ist. Dies war geboten, da die Digitalisierung der Messeinrichtungen bereits europarechtlich durch das Dritte Binnenmarktpaket vorgegeben war und einer Ausgestaltung im nationalen Recht bedurfte.

Die technischen Vorgaben sind in ihrem vorgeschriebenen Funktionsumfang, dem Detaillierungsgrad der vorgezeichneten Systemarchitektur und auch in ihrer Mechanismenstärke richtungsweisend und dem Stand der Technik verpflichtet, jedoch lässt sich kritisch anmerken, dass aufgrund der normativen Vorgabe einer komplexen Mindestfunktionalität in Verbindung mit dem aufwändigen Evaluations- und Zertifizierungsprozess nach Common Criteria eine Situation entstanden ist, die es den Infrastrukturmarktteilnehmern (insbesondere den Herstellern von Smart-Metern mit integrierten Gateways, die als Austauschkomponenten für Ferraris-Zähler ohne weitere Anbindung von Systemkomponenten vorgesehen sind) sehr schwer machen wird, zertifizierte Produkte auf den Markt zu bringen. Obwohl die ersten Versionen von Schutzprofil und Technischer Richtlinie bereits mehrere Jahre vor Veröffentlichung des Gesetzesentwurf zur Digitalisierung der Energiewende Ende 2015 vorgelegen haben, haben weitere Detaillierungen und Änderungen neben der hohen Grundkomplexität dazu geführt, dass zum Zeitpunkt des erwarteten Inkrafttretens des Gesetzes im Jahre 2016 keine zertifizierten Smart-Meter-Gateways verfügbar sein werden; Gespräche mit Herstellervertretern legen nahe, dass nach optimistischen Einschätzungen erst Mitte des Jahres 2017 die Marktverfügbarkeit erreicht wird.

Ob die umfangreichen technischen Schutzmaßnahmen und komplexen Vorgaben hinsichtlich der Gateway-Architektur, der PKI, der Kommunikationsbeziehungen und der besonderen Anforderungen an den Gateway-Administrator vorrangig den lauten Warnungen der Datenschützer, der Sorge um eine kritische Infrastruktur oder schlicht beeindruckendem behördlichen Fleiß geschuldet war, kann letztlich dahingestellt bleiben. Es bleibt im Ergebnis eine technisch aufwändig ausdefinierte und in der Maßnahmenfülle auch im globalen Vergleich seinesgleichen suchende Gesamtheit an Anforderungen, die die Hersteller der Systeme in besonderer Weise fordert und den berechtigten Schutzinteressen der Verbraucher entgegen kommt.

Datenschutzrisiken verbleiben hierbei auf Seiten der datenverarbeitenden Stellen, die granulare Verbrauchsdaten speichern (beispielsweise um für Kunden variable Tarife abzurechnen). Sollte es hier zu einem Entweichen von Stromverbrauchsdaten aufgrund unzureichender Schutzmaßnahmen, erfolgreicher Hackerangriffe oder einer missbräuchlichen Nutzung innerhalb der berechtigten Stelle kommen, wäre der Eingriff in die Privatsphäre der Stromkunden kaum zu unterschätzen. Dieses Risiko liegt aber außerhalb der Regelungsmöglichkeiten für die Datenübertragungseinheit im Haushalt; es wird wohl in kommenden Gesetzesvorhaben eine Berücksichtigung finden müssen, wenn es – spätestens nach ersten veröffentlichten Vorfällen – vom Gesetzgeber wahrgenommen wird.

Literatur

1. BSI, Das Smart-Meter-Gateway Sicherheit für intelligente Netze, S. 9. Bundesamt für Sicherheit in der Informationstechnik, Bonn (2016)
2. Joshua Pennell, Dann schalten Hacker die Lichter aus, ZEIT online, 29. April 2010, 10:39h (2010).
3. Kai Biermann, Stromkunden sollen sich überwachen lassen – und dafür zahlen, ZEIT online, 19. November 2013, 16:37h (2013).
4. U. Greveler und B. Justus und D. Löhr, Hintergrund und experimentelle Ergebnisse zum Thema Smart Meter und Datenschutz, Arbeitspapier, Version 0.6 - 20. Sep. 2011 (2011)
5. BSI, Schutzprofil für ein Smart Meter Gateway (BSI-CC-PP-0073). Online: www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Smart-Meter/Schutzprofil_Gateway, abgerufen 1. Feb. 2016
6. BSI, Technische Richtlinie BSI TR-03109, Version 1.0.1, Datum 11.11.2015
7. Andres Molina-Markham et al., Private Memoirs of a Smart Meter, Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for EnergyEfficiency in Building, 2010
8. Bundesrat, Stellungnahme des Bundesrates zum Entwurf eines Gesetzes zur Digitalisierung der Energiewende, Drucksache 543/15 (Beschluss), 18.12.2015
9. EU-Kommission, Empfehlung der Kommission vom 9. März 2012 zu Vorbereitungen für die Einführung intelligenter Messsysteme, (2012/148/EU), Amtsblatt der Europäischen Union (2012)
10. Datenschutzkonferenz und Düsseldorfer Kreis, Orientierungshilfe datenschutzgerechtes Smart Metering, Onlinepublikation Datenschutz Bayern: https://www.datenschutz-bayern.de/technik/orient/oh_smartmeter.pdf, 2012
11. Verbraucherzentrale Bundesverband, Stellungnahme des Verbraucherzentrale Bundesverbandes zum Entwurf eines Gesetzes zur Digitalisierung der Energiewende, 9. Oktober 2015
12. ISO/IEC, Common Criteria for Information Technology Security Evaluation, CC v3.1. Release 4, September 2012
13. Ernst & Young, Kosten-Nutzen-Analyse für einen flächendeckenden Einsatz intelligenter Zähler, Endbericht zur Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie, 2013
14. European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Commission Recommendation on preparations for the roll-out of smart metering systems, Brussels, 8 June 2012
15. Robert Lemos, Angriff der Killerbiene, Technology Review (Heise), online: http://www.heise.de/tr/artikel/Angriff-der-Killerbiene-974224.html, abgerufen 1. Feb. 2013, 2012
16. McKenna and Richardson and Thomson, Smart meter data: Balancing consumer privacy concerns with legitimate applications. Energy Policy, 41, Februar 2012
17. Aljoscha Dietrich, Rechtliche und technische Aspekte des Datenschutzes bei intelligenten Messsystemen (Smart Metern), Internet-Zeitschrift für Rechtsinformatik und Informationsrecht, http://www.jurpc.de/jurpcpdf/20150181.pdf, abgerufen 1. Feb. 2016, September 2014
18. Achim Leitner, Intelligent vernetzt, elektronikJOURNAL, Juni 2013, ISSN: 0013-5674, 2013
19. David von Oheimb, Stellenweise sicher – Kritische Betrachtung der IT-Security-Anforderungen fürs Smart Metering, elektronikJOURNAL, Juni 2013, ISSN: 0013-5674, 2013
20. Alberto Garcia Illera and Javier Vazquez Vidal, lights off the darkness of the smart meters (Konferenzvortrag), Black Hat Europe 2014, Amsterdam, Oktober 2014
21. Bundesministerium für Wirtschaft und Energie, Pressemitteilung – Staatssekretär Baake: Smart Meter wesentlicher Baustein für Energiewende und Energieeffizienz, 9.2.2015
22. Reuters, Bund sagt intelligenten Stromzählern ade, Handelsblatt online: 01.10.2014 10:19 Uhr, 2014.