Technischer Datenschutz an öffentlichen Ladestationen unter Berücksichtigung des Referentenentwurfs der Messsystemverordnung

Eva Weis, Ass. iur.

Karlsruher Institut für Technologie (KIT)
Zentrum für Angewandte Rechtswissenschaft (ZAR)
Forschungsgruppe Energieinformationsrecht und Neue Rechtsinformatik
Postfach 6980
76128 Karlsruhe
eva.weis@kit.edu

Abstract: Der Beitrag beantwortet die drängende Frage, ob das bestehende technische Datenschutzkonzept des Energiewirtschaftsgesetzes (EnWG) für stationäre Anwendungsfälle auch für den Betrieb öffentlicher Ladestationen der Elektromobilität sachgerecht anwendbar ist. Im Ergebnis wird dies auf Basis einer technisch/rechtlichen Detailanalyse verneint. Die insofern vom Verordnungsgeber zwischenzeitlich zutreffend gewünschte Konsequenz der temporären Freistellung von Messsystemen, die in diesem Kontext eingesetzt werden, begegnet, wie nachgewiesen wird, allerdings formell- und materiell-rechtlichen Bedenken.[1]

1 Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Auftrag des Bundesministeriums für Wirtschaft und Technologie Schutzprofile und technische Richtlinien erstellt, welche einen produktbezogenen technischen Datenschutz für intelligente Messsysteme etablieren sollen [BSI13a] [BSI13b]. Diese für stationäre Anwendungsfälle geschaffenen Regelungen gelten nach der weiten Gesetzesterminologie für jegliche Art von Messsystemen im Sinne von § 21d EnWG und insofern auch für solche in öffentlichen Ladestationen für Elektromobile. Insbesondere vor dem Hintergrund, dass die EU anstrebt bis zum Jahr 2020 in Deutschland 150.000 öffentlich zugängliche Ladepunkte zu installieren[2], stellt sich die Frage inwieweit insbesondere die Anforderungen der technischen Richtlinie auch für den Anwendungsfall einer öffentlichen Ladestation umsetzbar sind, bei der ein Kunde unabhängig davon an welcher Ladestation Strom bezogen wird immer von seinem eigenen Lieferanten beliefert[3] und monatlich abgerechnet wird.[4] Dass die Anwendung

[1] Die Autorin dankt Oliver Raabe für Anmerkungen und Anregungen die der Erstellung dieses Beitrages sehr dienlich waren. Der Beitrag ist im Rahmen des vom BMWi geförderten IKT für Elektromobilität II Projektes iZEUS entstanden.
[2] Vgl. COM(2013) 18 final, Richtlinienvorschlag des europäischen Parlaments und des Rates über den Aufbau der Infrastruktur für alternative Kraftstoffe, S. 23.
[3] Die Belieferung durch den eigenen Lieferanten und somit einen Netzzugangsanspruch auch bejahend [Ho09].

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5
 www.informatik2013.de

der technischen Anforderungen aus der technischen Richtlinie hier nicht problemlos möglich ist zeigt sich bereits daran, dass mit § 12 MsysV RefE (im Folgenden nur MsysV) eine Ausnahmeregelung für solche Messsysteme geschaffen werden soll. Die zweite Fragestellung ist allerdings, ob diese Freistellung im Hinblick auf das gewünschte Ergebnis rechtskonform gestaltet ist.

2 Elektromobilität im Datenschutzkonzept des EnWG

Die bereichsspezifischen Datenschutzregelungen des EnWG wurden aufgrund erheblicher Datenschutzrisiken, welche im Zusammenhang mit dem Einbau der damals noch als Smart Meter bezeichneten Systeme auftreten, eingeführt. Zentral im Schutzkonzept des EnWG ist der Begriff des Messsystems, an welchen alle datenschutzrechtlichen Regelungen anknüpfen. Das Messsystem wird von § 21d Abs. 1 EnWG definiert als „*eine in ein Kommunikationsnetz eingebundene Messeinrichtung zur Erfassung elektrischer Energie, das den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegelt*". Die Datenschutzregelungen des EnWG orientieren sich wie alle anderen Regelungen dieses Gesetzes ebenfalls an klassischen stationären Anwendungsfällen und sind somit eigentlich nicht für mobile Sachverhalte konzipiert.

Das Datenschutzkonzept des EnWG baut auf drei Säulen auf [RLP11, S. 831]. Zum Einen wurden explizite materielle Datenschutzregelungen in das EnWG aufgenommen. Zum Zweiten wurde mit § 21i EnWG eine umfangreiche Rechtsverordnungsermächtigung geschaffen, welche dem Verordnungsgeber weitreichende Handlungs- und Spezifizierungsmöglichkeiten eröffnet, von welchen bislang allerdings bis auf den hier zu untersuchenden Referentenentwurf der MsysV noch kein Gebrauch gemacht wurde. Zum Dritten wurden vom BSI Schutzprofile sowie technische Richtlinien für Smart Meter Gateways (SMGW) entwickelt, welche auch bereits durch § 21e EnWG vorgesehen sind. Deren nähere Ausgestaltung ist dabei aber ebenfalls einer Rechtsverordnung vorbehalten, für welche sich die Ermächtigung aus § 21i Abs. 1 Nr. 3 und 12 EnWG sowie aus § 21i Abs. 2 Nr. 10 EnWG ergibt. Die MsysV soll dies umsetzen und zumindest gemäß der Verordnungsbegründung das bereits entworfene Schutzprofil und die technische Richtlinie für verbindlich erklären [Bu13, S. 2].

Bei der Konzeption des Datenschutzes im EnWG wurde allerdings nicht beachtet, dass die eingeführten Regelungen auch elektromobile Sachverhalte erfassen, also auch in Fällen von Ladevorgängen an öffentlichen Ladestationen anwendbar sind. Auch hier wird nämlich eine kommunikationsfähige messtechnische Einrichtung verwendet werden, welche der Begriffsdefinition in § 21d Abs. 1 EnWG entspricht und somit ein Messsystem im Sinne des EnWG darstellt [WPL13]. Dies führt zu der Problematik, wie sich die für stationäre Fälle entworfenen Vorgaben auf elektromobile Sachverhalte auswirken.

[4] Siehe zur Szenariodefinition auch [WPR11, S. 131ff].

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5
 www.informatik2013.de

Festzustellen ist zunächst, dass schon die Grundkonzeption der Regelungen nicht auf Fälle der Verwendung von Messsystemen in öffentlichen Ladestationen passt. Dies erklärt sich aus historischer Perspektive daraus, dass insbesondere der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) die sogenannte Datenhoheit für besonders wichtig erachtete [BFD11, S. 2], was im Zuge des Gesetzgebungsverfahrens dann auch beachtet wurde. Dieses Prinzip ist im Kontext öffentlicher Ladestationen allerdings faktisch ungeeignet. Sobald ein Kunde an einer öffentlichen Ladestation einen Ladevorgang anstößt, werden die Messdaten durch das in die Ladestation eingebaute Messsystem generiert und müssen zu Abrechnungszwecken auch mit einem personifizierenden Merkmal attribuiert werden.[5] Aber bereits zu diesem Zeitpunkt kann im Unterschied zu stationären Fällen nicht mehr von einer Datenhoheit der Nutzer ausgegangen werden. Vielmehr ist die Datenhoheit bereits im Moment der Entstehung der Daten, der sich mit dem Vorgang der Erhebung deckt, verloren, da sich die Daten schon in diesem Moment außerhalb des Herrschaftsbereichs des Kunden befinden. Da insofern schon das Grundkonzept nicht für mobile Anwendungsfälle taugt, ist es ein leichtes zu erkennen, dass sich auch auf Basis der Anwendung der auf diesem Grundkonzept basierenden Regelungen, Schwierigkeiten ergeben können.

So ist aus materiell rechtlicher Sicht beispielsweise die Problematik zu nennen, dass der Kunde seine Auskunftsrechte aus § 21h EnWG nur gegenüber dem Messstellenbetreiber (MSB) geltend machen kann [WPL13]. Bei der Nutzung verschiedener Ladestationen, welche unter Umständen alle von unterschiedlichen MSBs betreut werden, dürfte sich dieses Nutzerrecht als in der Praxis kaum umsetzbar erweisen und würde insofern auch nicht mehr dem dieser Regelung eigentlich angedachten Schutzzweck genügen [WPL13].

Neben den materiell rechtlichen Problemstellungen[6] ergeben sich aber auch Fragestellungen hinsichtlich der an Messsysteme gestellten technischen Anforderungen. Fraglich ist nämlich wie sich die für stationäre Sachverhalte entworfenen technischen Vorgaben auf Messsysteme in öffentlichen Ladestationen auswirken. Der Verordnungsgeber hat zwar erkannt, dass Messsysteme für elektromobile Anwendungsfälle in vielerlei Hinsicht einen Sonderfall darstellen würden [Bu13, S. 30] und deswegen die Übergangsregelung in § 12 MsysV geschaffen, wonach „*Messsysteme, die ausschließlich der Erfassung der zur Beladung von Elektromobilen entnommenen oder durch diese zurück gespeisten Energie dienen, […] bis zum 31. Dezember 2020 von den Regelungen dieser Verordnung ausgenommen [sind]*“. Diese Vorgehensweise, erweist sich aufgrund der durch das Schutzprofil und der technischen Richtlinie aufgestellten technischen Vorgaben auch als richtig, was nachfolgend gezeigt werden soll. Allerdings stellt sich sodann die Frage, inwieweit die Regelung des § 12 MsysV überhaupt mit dem höherrangigen Recht des EnWG vereinbar ist.

[5] Siehe zur Notwendigkeit einer ID-Attribuierung [PRW10, S. 407f].
[6] Siehe hierzu ausführlich [WPL13].

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5
 www.informatik2013.de

3 Die technische Perspektive

Zunächst soll untersucht werden, wie sich die derzeitigen technischen Anforderungen, die durch das Schutzprofil und die technischen Richtlinie an Messsysteme gestellt werden, auf solche in öffentlichen Ladestationen auswirken. Hierzu bedarf es zunächst einer Betrachtung der Architektur, wie sie das BSI zur Ausgestaltung des Schutzprofils und der technischen Richtlinie zugrundegelegt hat. Wie in Abbildung 1 dargestellt wird von Seiten des Schutzprofils und der technischen Richtlinie zwischen drei verschiedenen Netzwerken unterschieden [BSI13a, S. 15] [BSI13b, S. 14]. Zum Einen wird die Verbindung zum Wide Area Network (WAN) spezifiziert, über die alle externen Kommunikationsvorgänge vorgenommen werden. Als Schnittstellen in das WAN wird zwischen einer Schnittstelle für die sogenannten externen Marktteilnehmer (EMT) und einer Schnittstelle hin zum Gateway-Administrator (GWA) differenziert. Zum Anderen wird auch die Verbindung ins Local Metrological Network (LMN) spezifiziert, in welchem die Elektrizitätszähler eingebunden sind. Das Dritte betrachtete Netzwerk ist das Home Area Network (HAN). Hier werden drei Schnittstellen beschrieben, die für unterschiedliche Anwendungsfälle vorgesehen sind. Zwei dieser Schnittstellen sind dafür gedacht Daten für den Letztverbraucher oder den Servicetechniker bereitzustellen. Die dritte Schnittstelle, betrifft die Kommunikation mit sogenannten Controllable Local Systems (CLS).[7]

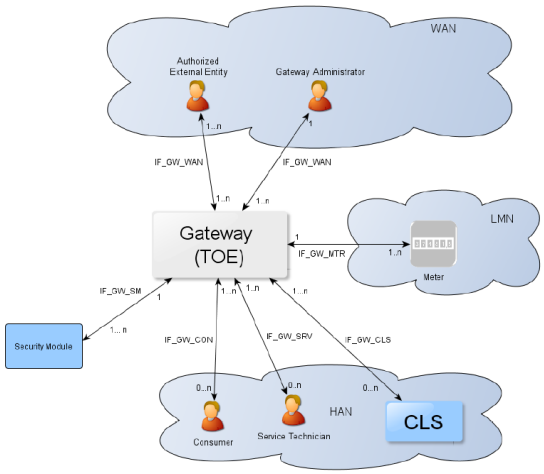

Abbildung 1: Architektur des BSI-Schutzprofils und der technischen Richtlinie[8]

Ausgehend von diesem Grundmodell soll nun dargestellt werden wie sich die durch das Schutzprofil und die technische Richtlinie aufgestellten Vorgaben auswirken, wenn ein BSI-konformes SMGW in öffentlichen Ladestationen zum Einsatz kommt. Dabei soll der Fokus auf die detaillierteren Regelungen der technischen Richtlinie gelegt werden und entsprechend dem Aufbau der technischen Richtlinie hinsichtlich der

[7] Als Beispiele für CLS werden intelligente Haushaltsgeräte, Kraft-Wärme-Kopplungs- oder Photovoltaikanlagen genannt, vgl. [BSI13a, S. 8] und [BSI13b, S. 14].
[8] Entnommen aus [BSI13a, S. 12].

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5

Anforderungen an die Kommunikationsverbindungen und Protokolle zwischen den drei Netzwerken [BSI13b, S. 20ff] unterschieden werden.[9]

3.1 Anforderungen an Verbindungen in das WAN

Das SMGW stellt die zentrale Kommunikationsverbindung in das WAN dar. Bei der Kommunikation in das WAN wird, wie auch aus Abbildung 1 ersichtlich ist, differenziert, ob die Kommunikation mit dem GWA oder mit einem EMT erfolgt. Sowohl das Schutzprofil als auch die technische Richtlinie verstehen unter dem Begriff des EMT alle Teilnehmer im WAN, mit denen das SMGW eine Kommunikationsverbindung aufnehmen kann [BSI13a, S. 10] [BSI13b, S. 13]. Aus energiewirtschaftlicher Sicht sind hierunter insbesondere die klassischen Energiemarktrollen, wie der Lieferant, der Netzbetreiber (VNB) und der MSB zu fassen.[10] Der GWA soll jedoch gerade kein EMT in diesem Sinne sein, sondern wird definiert als eine vertrauenswürdige Instanz, die das SMGW konfiguriert, überwacht und steuert [BSI13a, S. 9]; [BSI13b, S. 13].

3.1.1 Kommunikationsmodell der WAN-Kommunikation

Auffällig an der Grundkonzeption des Schutzprofils und der technischen Richtlinie ist, dass diese, wie in Abbildung 1 ersichtlich und in Bezug auf Ladevorgänge an öffentlichen Ladestationen nochmals in Abbildung 2 dargestellt, von einer sternförmigen Kommunikation in das WAN ausgehen [BSI13b, S. 14f]. Zwar wird mittlerweile formuliert, dass auch eine indirekte Verteilung der Messwerte nicht ausgeschlossen sei [BSI13b, S. 14f], mit Blick auf die Entstehungsgeschichte und auf die Gesamtkonzeption zeigt sich allerdings, dass die sternförmige Verteilung der Konzeption sowohl des Schutzprofils als auch der technischen Richtlinie zugrunde lag [RLP11]. Bei diesem sternförmigen Kommunikationsparadigma wird davon ausgegangen, dass jeder Marktakteur die von ihm benötigten Daten direkt aus dem SMGW erhält. Problematisch an diesem Ausgangspunkt ist allerdings, dass die heute von Seiten der Bundesnetzagentur (BNetzA) verbindlich festgelegte Marktkommunikation einem Kettenparadigma wie in Abbildung 2 für Ladevorgänge an öffentlichen Ladestationen dargestellt folgt. In diesem Kommunikationsmodell werden die Messdaten regelmäßig durch den MSB ausgelesen und von diesem sodann über den VNB an den Lieferanten weitergeleitet [BNA06, S. 37ff] [BNA10, S. 63ff]. Dieser auch im stationären Bereich bestehende Unterschied zwischen der dem Schutzprofil sowie der technischen Richtlinie zugrundeliegenden sternförmigen Kommunikation und den heutigen Festlegungen, die von einer kettenförmigen Kommunikation ausgehen [RLP11], wirkt sich auch auf Anwendungsfälle an öffentlichen Ladestationen aus, so dass dieser Umstand bei näherer Betrachtung der Vorgaben des Schutzprofils und der technischen Richtlinie in die Betrachtung mit einbezogen werden muss.

[9] Dargestellt werden sollen allerdings lediglich diejenigen Anforderungen, welche sich bei einem Einsatz in öffentlichen Ladestationen als problematisch erweisen könnten (3.1 – 3.3). Insofern erhebt diese Untersuchung keinen Anspruch auf Vollständigkeit.

[10] Vgl. zu den Rollen [BSI13b, S. 13]. Das BSI nennt darüber hinaus auch noch sonstige autorisierte Dienstleister die hier allerdings außer Betracht bleiben sollen [BSI13b, S. 13].

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5

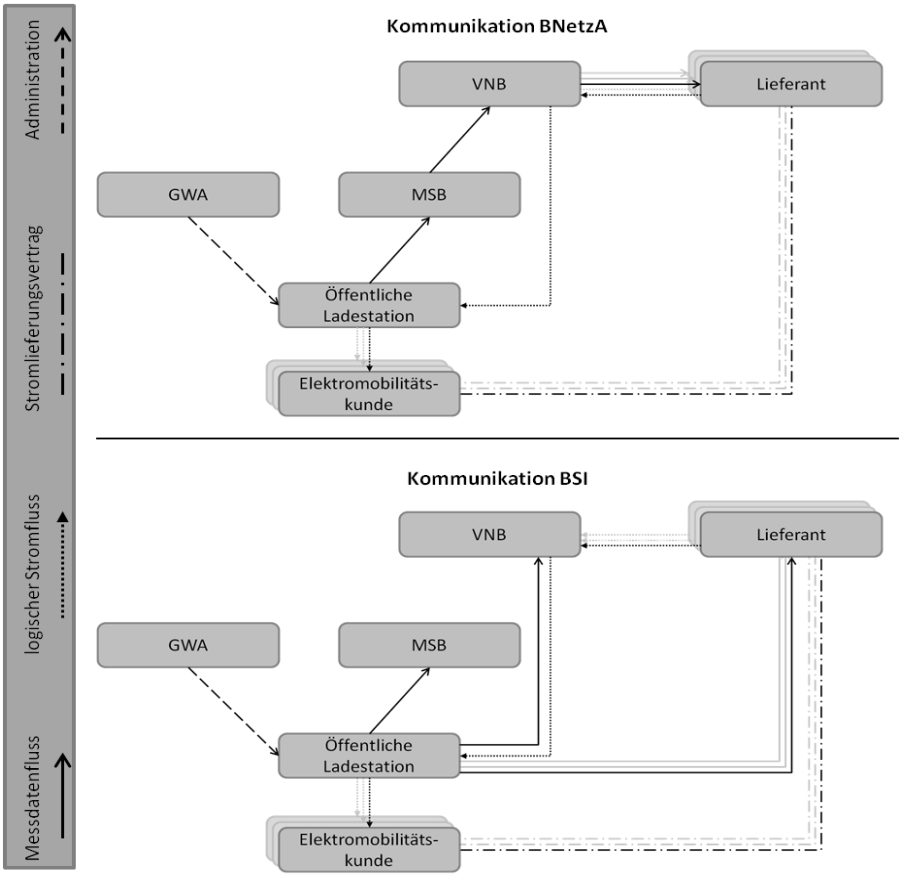

Abbildung 2: Kommunikationsmodelle BSI und BNetzA[11]

3.1.2 Die Anwendungsfälle der WAN-Kommunikation

Die Anwendungsfälle der technischen Richtlinie für die WAN-Kommunikation unterscheiden danach ob die Verbindung zum GWA oder zu einem EMT besteht. Gemein ist den WAN-Kommunikationsverbindungen, dass sie alle oberhalb der Transportschicht mittels Transport Layer Security (TLS) zu verschlüsseln sind und dass das SMGW keine von außen initiierten TLS-Verbindungen akzeptieren darf. Die TLS-Verbindung ist immer durch das SMGW aufzubauen [BSI13b, S. 37]. Diese nur einseitige Möglichkeit des Verbindungsaufbaus könnte sich für Ladevorgänge an öffentlichen Ladestationen als problematisch erweisen, da dem SMGW bekannt sein muss zu welchen Marktakteuren eine Verbindung aufzubauen ist. Bereits hier zeigen sich die wesentlichen Auswirkungen, der unterschiedlichen in Abbildung 2 dargestellten

[11] Die Administration durch den GWA erfolgt natürlich nur hinsichtlich des SMGW und nicht bezüglich den weiteren Bestandteilen der Ladestation.

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5

Kommunikationsparadigmen, die durch das BSI bzw. die BNetzA vorgegeben werden. Während der MSB konstant für eine öffentliche Ladestation zuständig sein dürfte und dementsprechend dem SMGW als EMT bekannt sein dürfte, wird das SMGW den mit dem Elektromobilisten vertraglich verbundenen Lieferanten nicht unbedingt kennen, so dass es zur Durchführung des Anwendungsfalls WAF5: Übertragung von Daten an externe Marktteilnehmer, der vorherigen Installation eines entsprechenden Kommunikationsprofils bedürfen könnte [BSI13b, S. 23]. Im Kommunikationsmodell der BNetzA könnten die Übermittlungsvorgänge der Messdaten an EMT, welche dem SMGW unbekannt sind, außerhalb dessen durch den MSB veranlasst werden. Wohingegen im Fall der Sternkommunikation zunächst ein Mechanismus etabliert werden müsste, der es ermöglicht, dass das SMGW in der Lage ist eine Kommunikationsverbindung zum Lieferanten des jeweiligen Kunden aufzubauen.

Ein solcher Mechanismus wird von der technischen Richtlinie im Rahmen des Anwendungsfalls WAF1: Administration und Konfiguration vorgesehen. Dieser Anwendungsfall beschreibt verschiedene Dienste, die das SMGW bereitzustellen hat und welche nur durch den GWA durchgeführt werden dürfen [BSI13b, S. 21]. Einer dieser Dienste ist die Profilverwaltung, wonach der GWA u.a. Kommunikationsprofile in das SMGW einbringen, aktivieren und löschen kann [BSI13b, S. 21]. Diese Kommunikationsprofile legen fest, gegenüber welchen EMT welche Kommunikation stattfinden darf. Ohne ein hinterlegtes Kommunikationsprofil wäre das SMGW nicht in der Lage einen Kommunikationskanal zu einem EMT zu öffnen.

Zunächst müsste der GWA aber überhaupt Kenntnis davon erlangen, dass sich ein Kunde an der Ladestation befindet. Auch dies könnte eventuell über den Anwendungsfall WAF2: Zugriff auf Dienste beim GWA oder über WAF3: Alarmierung und Benachrichtigung ermöglicht werden. Allerdings müsste das SMGW auch in der Lage sein über diese Anwendungsfälle dem GWA mitzuteilen, für welche EMT es Kommunikationsprofile benötigt, was wiederum voraussetzen würde, dass das Fahrzeug bzw. der Nutzer einen Kommunikationskanal zum SMGW besitzen müsste, welcher es erlaubt Daten direkt an das SMGW zu senden. Eine solche Kommunikationsverbindung ist derzeit allerdings nicht vorgesehen und würde auch das Schutzziel des SMGW konterkarieren, da mit einem solchen Kommunikationskanal die Möglichkeit für Attacken auf das System eröffnet werden würde.[12]

Aber selbst wenn der GWA z.B. auf dem Wege einer dritten Kommunikationsverbindung, in die Lage versetzt würde, für jeden die Ladestation nutzenden Kunden ein Kommunikationsprofil im SMGW der Ladesäule ad hoc einzuspielen, so würden sich noch weitere Probleme stellen. Kommunikationsprofile für die WAN-Kommunikation haben nämlich u.A. auch noch Zertifikate des EMT, sowohl für die TLS-Authentifizierung, die Signierung der Inhaltsdaten sowie für den Schlüsseltransport, zu enthalten [BSI13b, S. 116]. Daneben müssen noch Zertifikate des SMGW, Referenzen für die Verwendung eines bestimmten privaten Schlüssels des SMGW für die TLS-Authentifizierung sowie für die Signierung der Inhaltsdaten und für den Schlüsseltransport festgelegt werden [BSI13b, S. 116f]. Vor dem Hintergrund

[12] Denkbar wäre zwar die Informationen nicht über das SMGW sondern über eine dritte Kommunikations-einheit an den GWA zu senden, dies dürfte aber ebenfalls den Schutz durch das SMGW verringern.

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5
 www.informatik2013.de

wechselnder Nutzer und EMT an öffentlichen Ladestationen dürfte sich dieses Konzept als verhältnismäßig aufwändig erweisen, da die Konfiguration jedenfalls einzelner Kommunikationsprofile für jeden Ladevorgang erneut vorgenommen werden und von Seiten des GWA hierfür alle notwendigen Zertifikate beschafft werden müssten.[13]

Aber auch wenn man von der allgemeinverbindlich festgelegten Kettenkommunikation ausgeht, stellt sich dieses Problem in ähnlicher Weise. Zwar müssten die Kommunikationsprofile nicht für jeden einzelnen Ladevorgang hinsichtlich des Empfängers neu konfiguriert werden, da der erste Marktteilnehmer im WAN immer der MSB bzw. gemäß § 21b Abs. 1 EnWG der VNB als Grundzuständiger MSB ist. Allerdings wäre auch hier zu berücksichtigen, dass alle versendeten Messwerte grundsätzlich einer Inhaltsdatenverschlüsselung mittels Cryptographic Message Syntax (CMS) unterliegen [BSI13b, S. 36f]. Die Inhaltsdatenverschlüsselung muss dabei „*für den Endempfänger*" erfolgen [BSI13b, S. 36]. Aus technischer Sicht bedeutet das, dass die Inhaltsdaten mittels eines symmetrischen Verfahrens verschlüsselt und mit einem Message Authentication Code (MAC) gesichert werden [BSI13b, S. 123]. Die Schlüssel hierfür, sogenannte „session keys", werden direkt zuvor vom Sicherheitsmodul zufällig erzeugt [BSI13b, S. 123]. Diese werden dem CMS Container sodann angefügt und mittels eines Schlüssels verschlüsselt, welcher mit der Methode ECKA-EG berechnet wird [BSI13c, S. 19]. Für diese Berechnung muss allerdings der öffentliche Schlüssel desjenigen vorliegen, der als Endempfänger im Sinne dieser Vorgabe gilt [BSI12, S. 26f]. Fraglich ist aber wer Endempfänger im Sinne der technischen Richtlinie ist und wessen öffentlicher Schlüssel insofern für den Schlüsseltransport des session keys verwendet werden und somit im Sicherheitsmodul bereitliegen muss. Für den Fall der Sternkommunikation und für den Fall, dass die Daten über einen Marktteilnehmer indirekt verteilt werden ist dies relativ klar zu bestimmen, da die Daten in beiden Fällen immer nur für Zwecke eines bestimmten Marktteilnehmers vorgesehen sind.

Im Fall der von der BNetzA vorgegebenen kettenähnlichen Kommunikation liegt der Fall jedoch anders. Zum Einen sind hier mehrere Instanzen vorhanden, die die Daten weiterleiten. So werden die Daten nämlich vom SMGW zunächst an den MSB, von diesem dann an den VNB und letztendlich auch an den Lieferanten bzw. zu weiteren Verwendungszwecken auch an weitere Marktteilnehmer gesendet. Zum Anderen ist es ausgehend vom von der BNetzA vorgesehenen Kommunikationsparadigma so, dass neben dem Lieferant als eigentlichem Endempfänger der Daten auch dem VNB, als an der Übermittlung der Messdaten beteiligten Akteur, bestimmte Aufgaben zugewiesen sind, die eine Einsicht in die Inhaltsdaten erfordern.[14] Insofern ist auch für stationäre Fälle bei Zugrundelegung der Kettenkommunikation unklar mit wessen Schlüsselmaterial die Inhaltsdatenverschlüsselung zu erfolgen hat, wer also der Endempfänger der Daten ist. Ausgehend davon, dass das BSI eine sternförmige Kommunikation zugrundegelegt hat und somit offensichtlich eine Ende-zu-Ende Verschlüsselung anstrebte, müsste eigentlich der Lieferant der Endempfänger im Sinne dieser Vorgabe sein. Dies würde auch im Sinne des Grundsatzes der Datensparsamkeit

[13] Denkbar wäre jedenfalls für die Zertifikate des EMT die Nutzung eines zentralen Repositories o.Ä., bei welchem diese durch den GWA abgefragt werden könnten.
[14] Der VNB muss die Messwerte auf Plausibilität prüfen und bei Bedarf auch eine Ersatzwertbildung vornehmen, vgl. [BNA06, S. 37].

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5

sein, da sowohl der VNB als auch der MSB nicht in allen Fällen die gleichen hochaufgelösten Werte benötigen, wie dies beim Lieferanten der Fall sein könnte. Allerdings muss festgestellt werden, dass jedenfalls der VNB eigene Aufgaben wahrnimmt, für welche er zwangsläufig auch die Inhaltsdaten kennen muss. Dies würde wiederum aus Praktikabilitätsgründen dafür sprechen, den VNB als Endempfänger im Sinne der Vorgabe der technischen Richtlinie zu verstehen, da er andernfalls seine gesetzlichen Aufgaben, bei Verwendung einer Marktkommunikation wie sie die BNetzA verbindlich vorschreibt, nicht wahrnehmen könnte. Wenn man insofern die Daten nicht gerade in mehrfacher Ausfertigung entlang der Prozesskette versenden will, muss die Vorgabe wohl so ausgelegt werden, als dass die Inhaltsdatenverschlüsselung mit dem Schlüssel desjenigen zu erfolgen hat, der die Daten als erstes in der Kette benötigt.

Für Einsatzzwecke in öffentlichen Ladestationen würde die Qualifikation des MSB oder VNB, die wohl beide fest einer Ladestation zugeordnet sein werden, als Endempfänger bedeuten, dass sich entsprechend der Ausführungen hinsichtlich der Transportsicherung keine Notwendigkeit ergeben würde weiteres Schlüsselmaterial des Lieferanten des Kunden in den Kommunikationsprofilen aufzunehmen. Das benötigte Schlüsselmaterial wäre bereits in den vorhandenen Kommunikationsprofilen hinterlegt. Sollte allerdings doch der Lieferant als Endempfänger anzusehen sein, so müsste das benötigte Schlüsselmaterial von diesem ad hoc in einem Kommunikationsprofil hinterlegt werden.

Ein weiteres Problem im Hinblick auf die Verwendung von BSI-konformen Messsystemen ergibt sich daraus, dass die technische Richtlinie neben den Kommunikationsprofilen auch noch sogenannte Auswertungsprofile vorsieht [BSI13b, S. 114f]. Auswertungsprofile sind Regelwerke die bestimmen, wie mit Daten die durch das SMGW empfangen werden umzugehen ist [BSI13b, S. 16]. Z.B. wird durch die Auswertungsprofile festgelegt in welcher Granularität Messwerte zu erfassen sind, um den vom Kunden gewählten Tarif umsetzen zu können [BSI13b, S. 114]. Dies bedeutet, dass die Messwerte in der Taktung zu erfassen sind, in der sich der Tarif des Kunden ändern kann. Diese Taktung ergibt sich dabei aber aus der vertraglichen Beziehung zwischen Kunde und Lieferant, so dass hierfür für jeden Kunden eine separate Konfiguration erforderlich wäre, was zu derselben Problematik führt, wie soeben für die Kommunikationsprofile dargestellt.

3.2 Anforderungen an Verbindungen in das LMN

Das LMN verbindet das SMGW mit den Zählern. Insofern besteht zunächst kein Unterschied zwischen dem LMN in stationären Fällen und bei öffentlichen Ladestationen. Als Anwendungsfälle in diesem Netzwerk schreibt die technische Richtlinie die Anwendungsfälle LAF1: LMN Zählerverwaltung und LAF2: Abruf/Empfang von Messwerten vor, welche beide zwingend durch das SMGW unterstützt werden müssen [BSI13b, S. 45ff]. Der Anwendungsfall LAF1: LMN Zählerverwaltung betrifft die Registrierung und Konfiguration der Zähler, sowie das Schlüssel- und Zertifikatsmanagement [BSI13b, S. 45f]. Während das Schlüssel- und Zertifikatsmanagement für die Kommunikation zwischen SMGW und LMN an öffentlichen Ladestationen ebenso umsetzbar wäre wie in stationären Fällen, stellt sich

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5

im Hinblick auf die Registrierung und Konfiguration die Problematik, dass die technische Richtlinie vorschreibt, dass der Zähler einem Letztverbraucher zuzuordnen ist. Aufgrund des ständigen Wechsels der Letztverbraucher an öffentlichen Ladestationen darf insofern als fraglich bewertet werden, wie sich diese Anforderung praktisch umsetzen lässt.

LAF2: Abruf/Empfang von Messwerten beschreibt den Fall, dass die durch den Zähler gemessenen Werte an das SMGW ausgeliefert bzw. von diesem abgeholt werden. Dies muss vom SMGW sowohl per Einzelabruf als auch durch eine periodische Zulieferung der Messwerte umgesetzt werden können. Für öffentliche Ladestationen ist zu bemerken, dass entweder Zähler oder SMGW in der Lage sein müssen zu registrieren, wann sich ein Kunde an die Ladestation anschließt als auch wann er diese wieder verlässt. Ein solcher Trigger wäre zwar wohl in den Anwendungsfall integrierbar, wird aber derzeit nicht vorgesehen. Er ist aber insofern zwingend notwendig, als dass vermieden werden muss, dass ein Messwert erst dann zum SMGW gelangt, wenn bereits mehrere Kunden die Ladestation frequentiert haben und sich die Messwerte somit vermischen konnten.[15]

3.3 Anforderungen an Verbindungen in das HAN

Hinsichtlich der Verbindungen in das HAN stellt sich bereits die ganz grundlegende konzeptionelle Frage, welcher Bereich an einer öffentlichen Ladestation als HAN anzusehen ist. Ausgehend von den HAN-Anwendungsfällen zeigt sich, dass es um die Bereitstellung von Daten für den Letztverbraucher (HAF1) bzw. den Service-Techniker (HAF2) geht und auch darum einen transparenten Kommunikationskanal zwischen CLS und EMT (HAF3) zu ermöglichen [BSI13b, S. 54ff]. Als Teilnehmer im HAN kommen insofern, ebenso wie in stationären Fällen, nur solche Teilnehmer in Betracht, welche sich physisch an der Ladestation befinden. Während der Anwendungsfall HAF2 auch bei SMGW in öffentlichen Ladestationen umsetzbar sein wird, ist dies bei den anderen genannten Anwendungsfällen fraglich.

3.3.1 Anwendungsfall HAF1: Bereitstellung von Daten für den Letztverbraucher

Der Anwendungsfall HAF1: Bereitstellung von Daten für den Letztverbraucher ist dafür gedacht, die sich aus der Definition des Messsystems in § 21d Abs. 1 EnWG ergebende Anforderung der Widerspiegelung von Daten für den Letztverbraucher, umzusetzen. Sinn und Zweck dieser Anforderung ist es dem Letztverbraucher seinen eigenen Energieverbrauch anzeigen zu können und dadurch zu Energieeinsparungen anzuregen. Inwieweit das Ziel der Vorschrift an öffentlichen Ladestationen überhaupt erreicht werden kann ist fraglich, da das Elektrofahrzeug zwangsläufig eine bestimmte Energiemenge laden muss und somit bis auf eventuelle Lastverschiebungen keine Reduktion der Energieentnahme zu erwarten ist. Nichtsdestotrotz setzt die technische

[15] Hierfür kommt es allerdings darauf an, welcher Teil des Messsystems die Zuordnung der einzelnen Messwerte zu dem jeweiligen Kunden vornimmt. Da die Zeitstempelung der Messwerte erst im SMGW erfolgt, vgl. [BSI13b, S. 15], wird hier davon ausgegangen, dass die Zuordnung eines Messwertes zu einer Kunden-ID, welche eichrechtlich genauso wie die Zeitstempelung notwendig ist, vgl. [PRW10, S. 407f], auch erst im SMGW oder in einer weiteren Einheit erfolgt.

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5

Richtlinie die Schnittstelle IF_GW_CON voraus über welche dem Letztverbraucher die Visualisierungsmöglichkeit geboten werden soll. An öffentlichen Ladestationen kommen nun grundsätzlich drei Möglichkeiten der Visualisierung in Betracht. So könnte das Widerspiegeln über ein in die Ladestation integriertes Display oder ein solches im Fahrzeug selbst erfolgen. Daneben wäre auch noch eine Visualisierung über eine Web Anwendung denkbar, was allerdings nicht dem HAN-Anwendungsfall HAF1 zuzuordnen wäre, sondern vielmehr eine Anwendung im WAN-Bereich darstellen dürfte. Dies sieht auch die technische Richtlinie in ihrem allerdings nur informativen Anwendungsfall TAF13: Bereitstellung von Messwertsätzen zur Visualisierung für den Letztverbraucher über die WAN-Schnittstelle vor [BSI13b, S. 105].[16]

Problematisch hieran ist in Bezug auf öffentliche Ladestationen, dass ein lesender Zugriff des Letztverbrauchers nur nach erfolgreicher Authentifizierung entweder mittels HAN-Zertifikaten oder eindeutiger Kennung und Passwort erfolgen darf [BSI13b, S. 57f]. Zudem ist der Kommunikationskanal ebenso wie bei der WAN Kommunikation mittels TLS zu sichern [BSI13b, S. 71]. Dies bedeutet, dass sogenannte HAN-Kommunikationsprofile im SMGW zuvor durch den GWA zu hinterlegen sind [BSI13b, S. 73].[17] Diese müssen zum Einen die Adresse des Kommunikationspartners im HAN und zum Anderen auch das Zertifikat des Kommunikationspartners für die TLS Authentifizierung enthalten [BSI13b, S. 74f]. Da auch diese Kommunikationsprofile ausschließlich durch den GWA eingespielt werden dürfen [BSI13b, S. 75], dürfte jedenfalls die Anforderung, dass das Zertifikat des Kommunikationspartners im HAN und somit das des ladenden Letztverbrauchers im Kommunikationsprofil enthalten sein muss, ebenso wenn nicht noch problematischer umsetzbar sein, wie dies für die Kommunikationsprofile im WAN dargestellt wurde. Auch die von Seiten der technischen Richtlinie vorgesehene Möglichkeit der Letztverbraucherauthentifikation mittel eindeutiger Kennung und Passwort führt insofern nicht weiter, da auch dieser Authentifikationsmechanismus einer Hinterlegung im Kommunikationsprofil bedarf.

3.3.2 Anwendungsfall HAF3: Transparenter Kommunikationskanal zwischen CLS und EMT

Im Rahmen des Anwendungsfalls HAF3, der die Kommunikation zwischen im HAN befindlichen CLS und EMT im WAN zum Gegenstand hat und dem SMGW insofern eine Proxy Funktionalität zukommen lässt, stellen sich dieselben Problemstellungen wie sie bereits in Bezug auf die Kommunikation ins WAN und mit dem Letztverbraucher dargestellt wurden. Kernpunkt ist erneut, dass das SMGW in diesem Fall sogenannte Proxy-Kommunikationsprofile, welche ebenfalls nur durch den GWA eingespielt werden dürfen, enthalten muss [BSI13b, S. 76ff]. Diese müssen wiederum Zertifikate des EMT und des CLS für die TLS-Authentifizierung enthalten [BSI13b, S. 77f].[18]

[16] Aufgrund des lediglich informativen Charakters des Anwendungsfalls TAF13, bedarf es aber bei Zugrundelegung der technischen Richtlinie dennoch einer Umsetzung des Anwendungsfalls HAF1.
[17] Dies geschieht ebenfalls durch Ausführung des bereits dargestellten Anwendungsfalls WAF1: Administration und Konfiguration, siehe hierzu [BSI13b, S. 21f].
[18] Nennenswert ist dieser Anwendungsfall vorliegend deswegen, da er darauf abzielt, dass CLS überhaupt gesteuert werden können und er zudem als einziger Anwendungsfall der technischen Richtlinie eine

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5

4 Die rechtliche Perspektive

Wie gezeigt werden konnte, bestehen bei der Verwendung von BSI-konformen Messsystemen in öffentlichen Ladestationen einige Problemstellungen, die sich primär aus der notwendigen Vorkonfiguration sowie der Zertifikatsverwaltung des SMGW ergeben. Der Gesetzgeber hat diese Problematik offensichtlich erkannt, da in § 12 MsysV eine Übergangsregelung für solche Messsysteme geschaffen wurde, „*die ausschließlich der Erfassung der zur Beladung von Elektromobilen entnommenen oder durch diese zurück gespeisten Energie dienen*“ (im Folgenden Elektromobilitätsmesssysteme). Nach dieser Übergangsregelung sollen die Elektromobilitätsmesssysteme bis zum 31.12.2020 von den Regelungen der MsysV ausgenommen sein, welche zum Ziel hat, die vom BSI entwickelten Schutzprofile für SMGW und für das Sicherheitsmodul, sowie die dazugehörigen technischen Richtlinien für allgemeinverbindlich zu erklären [Bu13, S. 2].[19] In der Rechtsfolge könnte die Nichtanwendbarkeit der MsysV für Elektromobilitätsmesssysteme also bedeuten, dass Schutzprofile und technische Richtlinien des BSI nicht eingehalten werden müssten, was vor dem Hintergrund der dargelegten Problemstellungen auch begrüßenswert wäre.

Fraglich ist jedoch in Bezug auf § 12 MsysV, was eigentlicher Regelungsgegenstand dieser Norm ist und welche Rechtsfolgen sich daraus für Elektromobilitätsmesssysteme ergeben. Aus rechtlicher Sicht kommen diesbezüglich nämlich zwei Alternativen in Betracht. Zum Einen könnte vertreten werden, dass § 12 MsysV auf Basis der Ermächtigungsgrundlage des § 21i Abs. 1 Nr. 11 EnWG erlassen wurde, wonach der Verordnungsgeber ermächtigt wird „*den Bestandsschutz nach § 21e Absatz 5 […] inhaltlich und zeitlich näher zu bestimmen und damit gegebenenfalls auch eine Differenzierung nach Gruppen und eine Verlängerung der genannten Frist vorzunehmen*“. Diese Auslegungsvariante hätte zur Folge, dass § 12 MsysV eine Konkretisierung der Ausnahmeregelung des § 21e Abs. 5 EnWG darstellen würde. Die Ausnahme von Elektromobilitätsmesssystemen könnte in diesem Zusammenhang nämlich durchaus eine Differenzierung nach Gruppen darstellen. Problematisch an dieser Ermächtigung ist aber, dass ein Bestandsschutz eigentlich schon begrifflich voraussetzt, dass etwas bereits Bestehendes geschützt wird. Der Bestandsschutz des § 21e Abs. 5 EnWG bezieht sich aber ebenfalls auf erst künftig einzubauende Messsysteme, so dass dies nicht dagegen spricht § 12 MsysV als von der Ermächtigungsgrundlage erfasst anzusehen. Ein weiteres Problem dass sich in diesem Zusammenhang stellt ist, dass § 21i Abs. 1 Nr. 11 EnWG lediglich von „*der genannten Frist*“ spricht. § 21e Abs. 5 EnWG enthält jedoch zwei Fristen und zwar eine betreffend den Einbauzeitpunkt und die andere hinsichtlich der Nutzungsdauer bereits eingebauter Geräte. Es lässt sich zwar nicht eindeutig erkennen welche Frist durch § 21i Abs. 1 Nr. 11 EnWG adressiert ist und kann vorliegend aufgrund des begrenzten

Kommunikation zwischen Geräten im HAN mit Teilnehmern im WAN ermöglicht. Gerade Elektromobile werden in § 14a EnWG als unterbrechbare Verbrauchseinrichtungen explizit benannt und können somit auch CLS im Sinne der technischen Richtlinie darstellen. Dem Anwendungsfall HAF3 könnte insofern gerade für den Bereich der Elektromobilität eine besondere Relevanz zukommen, da sich Elektromobile als steuerbare Lasten aufgrund des hohen Verschiebepotentials besonders gut eignen werden.

[19] Zentrale Norm zur Verrechtlichung der Schutzprofile und technischen Richtlinien soll dabei§ 4 MsysV sein [Bu13, S. 24].

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5

Umfangs des Beitrags auch nicht näher untersucht werden, allerdings erscheint es durchaus möglich eine Verlängerung der Einbaufrist als von der Ermächtigungsgrundlage grundsätzlich umfasst anzusehen.[20]

Problematisch in Bezug auf die Auslegung des § 12 MsysV in der soeben dargestellten Weise ist aber, dass sich kaum Anhaltspunkte finden lassen, die für diese Auslegungsvariante sprechen. Die Art und Weise der Gestaltung von § 12 MsysV scheint vielmehr für eine andere Auslegungsvariante zu sprechen. § 12 MsysV könnte nämlich auch lediglich dazu dienen, den Anwendungsbereich der MsysV, welcher in § 1 MsysV geregelt ist, einzuschränken. Es ist nämlich festzustellen, dass der Verordnungsgeber in § 12 MsysV formuliert, dass Messsysteme „*von den Regelungen dieser Verordnung ausgenommen*“ sind. Ein Hinweis darauf, dass die oben genannte Bestandsschutzregelung des § 21e Abs. 5 EnWG verändert werden sollte findet sich im Wortlaut des § 12 MsysV nicht. Die einzige Ähnlichkeit mit § 21e Abs. 5 EnWG besteht zudem darin, dass eine zeitlich befristete Ausnahmeregelung betreffend den Einbau von Messsystemen geschaffen wird. Insofern deutet der Wortlaut eher darauf hin § 12 MsysV als Ergänzung zu § 1 MsysV, der den Anwendungsbereich der Verordnung regelt, zu verstehen. Hierfür spricht im Übrigen auch ein Blick in die Verordnungsbegründung. Auffällig ist nämlich, dass im Unterschied zu den anderen Regelungen der MsysV in der Verordnungsbegründung zu § 12 MsysV gerade keine Ermächtigungsgrundlage für den Erlass dieser Regelung genannt wird.[21]

Fraglich ist aber, welche Konsequenzen auf Rechtsfolgenseite aus diesen beiden Auslegungsalternativen folgen. Bei einer angestrebten Änderung der Bestandsschutzregelung des § 21e Abs. 5 EnWG dürften Elektromobilitätsmesssysteme, die nicht den Anforderungen des § 21e Abs. 2-4 EnWG genügen, bis 2020 eingebaut werden, sofern die Nutzung nicht mit unverhältnismäßigen Gefahren verbunden ist und der Anschlussnutzer schriftlich und in Kenntnis, dass das Messsystem nicht den genannten Anforderungen genügt, zugestimmt hat. Ob eine solche schriftliche Zustimmung gerade an öffentlichen Ladestationen praktikabel ist darf bezweifelt werden, zumal auch nicht klar ist gegenüber wem in diesen Fällen die Zustimmung zu erklären wäre. Sollte die schriftliche Zustimmung indes nicht vorliegen, so müssten doch die durch die MsysV konkretisierten Anforderungen des § 21e Abs. 2-4 EnWG befolgt und insofern durch die Hintertür nun doch die Vorgaben der Schutzprofile und technischen Richtlinien eingehalten werden.

Betrachtet man § 12 MsysV hingegen als bloße Einschränkung des Anwendungsbereichs der MsysV so ändert sich an der Regelung des § 21e EnWG zunächst nichts. Alle Messsysteme die nach dem 31.12.2014 eingebaut werden, müssen dann gemäß § 21e Abs. 1 S. 2 EnWG den Anforderungen der Absätze 2-4 genügen. Eine diese Anforderungen konkretisierende Verordnung für Elektromobilitätsmesssysteme würde insofern noch ausstehen, da der Anwendungsbereich der MsysV für diesen Fall aufgrund von § 12 MsysV gerade nicht eröffnet ist. Fraglich wäre aber, welche Konsequenzen

[20] Vorliegend müsste allerdings eine genaue Untersuchung dahingehend erfolgen, inwieweit eine solch weit ausgedehnte Ausnahmeregelung mit dem eigentlichen Schutzzweck des § 21e EnWG, das Recht auf informationelle Selbstbestimmung zu schützen, vereinbar wäre.
[21] Vgl. zur Nennung bei den weiteren Regelungen [Bu13, S. 21ff].

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5
 www.informatik2013.de

eine nicht existierende Verordnung für die Anforderungen des § 21e Abs. 2-4 EnWG hätte. In Betracht kommt, dass es sich hinsichtlich der Konkretisierung der Anforderungen nicht um eine reine Ermächtigung zum Erlass einer Verordnung handeln könnte, sondern eventuell um eine Pflicht zum Erlass. Der Wortlaut lässt nämlich bereits erkennen, dass der Gesetzgeber im Rahmen der Anforderungen des § 21e Abs. 2-4 EnWG davon ausging, dass es eine Rechtsverordnung mit konkretisierenden Regelungen geben muss. Zwar ist der Verordnungsgeber grundsätzlich frei in der Entscheidung ob er eine Verordnung erlassen will. In bestimmten Fällen, insbesondere dann wenn die gesetzliche Regelung ohne die ausgestaltende Verordnung nicht praktikabel ist, kann es aber sein, dass keine Ermächtigung, sondern eine Anordnung auf Erlass einer Rechtsverordnung vorliegt [Uh13, Art. 80, Rn. 30]. In der Konsequenz könnte dies bedeuten, dass der Verordnungsgeber unter Umständen verpflichtet werden könnte eine Rechtsverordnung, welche auch Elektromobilitätsmesssystem regelt, zu erlassen oder aber auch, dass sich aufgrund der konkreten Ausgestaltung des § 21e Abs. 2-4 EnWG die verpflichtende Anwendung der Schutzprofile und technischen Richtlinien direkt aus dieser Norm herleiten lässt. Auch diese Fragestellung wird künftig noch weiterer rechtlicher Untersuchungen bedürfen.

Im Ergebnis kann festgehalten werden, dass die Übergangsregelung des § 12 MsysV aus rechtlicher Sicht als problematisch zu bewerten ist. Fraglich ist insbesondere, ob die offensichtlich seitens des Gesetzgebers vorgesehene Freistellung von Elektromobilitätsmesssystemen hinsichtlich der Anforderungen der derzeitigen Schutzprofile und technischen Richtlinien rechtskonform auf dem gewählten Weg umsetzbar ist. Die aufgezeigten Auslegungsvarianten des § 12 MsysV führen nämlich beide zu Folgeproblemen, welche die beabsichtigte Freistellung unter Umständen wieder beseitigen könnten. Eine vorzugswürdige Lösung wäre es daher gewesen die Freistellung nicht in der Verordnung, sondern direkt im EnWG zu verankern. Diese Problematik wird aber künftig – insbesondere im Falle des unveränderten Inkrafttretens – noch weitergehende Untersuchungen erfordern.

5 Fazit und Ausblick

Aus technischer Sicht konnte gezeigt werden, dass der Verordnungsgeber mit Schaffung der Übergangsregelung des § 12 MsysV grundsätzlich auf dem richtigen Weg ist. Es konnte nachgewiesen werden, dass die Anforderungen, die durch die technische Richtlinie gestellt werden, insbesondere im Hinblick auf die Konfiguration der Kommunikations- und Auswertungsprofile und die benötigten Zertifikate und Schlüssel nur sehr umständlich an öffentlichen Ladestationen umgesetzt werden können. Insofern ist die Freistellung dieser Art von Messsystemen durch § 12 MsysV sachlich begrüßenswert. Allerdings bedarf es künftig noch einer tiefergehenden rechtlichen Prüfung ob das von § 12 MsysV gewünschte Ergebnis auch rechtskonform ist.

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5

Literaturverzeichnis

[BfD11] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: Positionspapier zu den Datenschutzanforderungen an Smart Meter. 2011. Online unter http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/39_SmartMeter.html?nn=1857092.

[BNA06] Bundesnetzagentur: Festlegung einheitlicher Geschäftsprozesse und Datenformate zur Abwicklung der Belieferung von Kunden mit Elektrizität, Anlage zum Beschluss BK6-06-009 vom 11.07.2006 (konsolidierte Lesefassung gültig ab 01.04.2012). Online unter http://www.bundesnetzagentur.de [27.03.2013].

[BNA10] Bundesnetzagentur: Wechselprozesse im Messwesen, Anlage 1 zum Beschluss BK6-09-034 / BK7-09-001 vom 09.09.2010 (konsolidierte Lesefassung gültig ab 01.04.2012). Online unter http://www.bundesnetzagentur.de [25.03.2013].

[BSI12] Bundesamt für Sicherheit in der Informationstechnik: Technical Guideline TR-03111, Elliptic Curve Cryptography,. Version 2.0 – 28. Juni 2012. Online unter https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03111/index_htm.html [08.05.13].

[BSI13a] Bundesamt für Sicherheit in der Informationstechnik: Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen. Version 1.2 - 18. März 2013 (Final Release). Online unter https://www.bsi.bund.de/DE/Themen/SmartMeter/smartmeter_node.html [27.3.2013].

[BSI13b] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109-1 1, Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems. Version 1.0 - 18.03.2013. Online unter https://www.bsi.bund.de/DE/Themen/SmartMeter/smartmeter_node.html [27.3.2013].

[BSI13c] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie TR-03116-3 eCard-Projekte der Bundesregierung, Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen. Stand 18 März 2013. Online unter https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html [08.05.13].

[Bu13] Referentenentwurf der Bundesregierung: Verordnung über technische Mindestanforderungen an den Einsatz intelligenter Messsysteme.

[Ho09] von Hoff, S.: Zugangsanspruch zu Elektromobilitätstankstellen. Zeitschrift für Neues Energierecht 2009, S. 341-345.

[PRW10] Pallas, F.; Raabe, O.; Weis, E.: Beweis- und eichrechtliche Aspekte der Elektromobilität. In: Computer und Recht 2010, S. 404-410.

[RLP11] Raabe, O.; Lorenz, M.; Pallas, F.; Weis, E.: Harmonisierung konträrer Kommunikationsmodelle im Datenschutzkonzept des EnWG – „Stern“ trifft „Kette“. In: Computer und Recht 2011, S. 831-840.

[Uh13] Uhle, A.; In: Epping, V.; Hillgruber C.: Beck'scher Online-Kommentar GG. Stand 1.1.2013.

[WPL13] Weis, E.; Pallas, F.; Lorenz, M.; Raabe, O.: Datenschutz und Elektromobilität. In: Boesche, K. V.; Fest, C.; Franz, O.; Gaul, A.: Berliner Handbuch zur Elektromobilität. München 2013.

[WPR11] Weis, E.; Pallas, F.; Raabe, O.; Lorenz, M.: Szenario 6: Elektromobilität mit untertägigem Lieferantenwechsel. In: Raabe, O.; Pallas, F.; Weis, E.; Lorenz, M.; Boesche K.V.: Datenschutz in Smart Grids – Anmerkungen und Anregungen. London/Berlin. 2011.

Erschienen im Tagungsband der INFORMATIK 2013
Lecture Notes in Informatics, Volume P-220
ISBN 978-3-88579-614-5
