Bundesamt
für Sicherheit in der
Informationstechnik

Deutscher Bundestag
18. Wahlperiode
Ausschuss für Wirtschaft und Energie

Ausschussdrucksache 18(9)765neu
11. April 2016

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Deutscher Bundestag
Ausschuss für Wirtschaft und Energie
Platz der Republik 1

11011 Berlin

Bernd Kowalski

HAUSANSCHRIFT
Bundesamt für Sicherheit in
der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 (0) 228 9582-5700
FAX +49 (0) 228 9582-5700

Bernd.Kowalski@bsi.bund.de
https://www.bsi.bund.de

Betreff: Schriftliche Stellungnahme zur öffentlichen Anhörung „Entwurf eines Gesetzes zur Digitalisierung der Energiewende“ im Ausschuss für Wirtschaft und Energie am Mittwoch, den 13. April 2016

Bezug: Ihr Schreiben vom 1. April 2016 (Geschäftszeichen: PA 9/002)

Datum: 08. April 2016

Sehr geehrte Mitglieder des Wirtschaftsausschusses,
sehr geehrte Damen und Herren,

gerne nehme ich als Sachverständiger an der öffentlichen Anhörung „Entwurf eines Gesetzes zur Digitalisierung der Energiewende“ im Ausschuss für Wirtschaft und Energie am Mittwoch, den 13. April 2016, teil und möchte nachstehend die erbetene schriftliche Stellungnahme zu dem Gesetzesvorhaben übermitteln.

Betreff: Schriftliche Stellungnahme zur öffentlichen Anhörung „Entwurf eines Gesetzes zur Digitalisierung der Energiewende“ im Ausschuss für Wirtschaft und Energie am Mittwoch, den 13. April 2016

Stellungnahme

1. Digitale Souveränität / Intelligentes Netz

Die digitale Energiewende und das zugehörige zukünftige intelligente Netz (Smart Grid) stehen für die intelligente Vernetzung von zentralen und dezentralen Systemen, wie Energieerzeugungsanlagen, Speicher- und Verbrauchseinrichtungen und anderen digitalen Systemlösungen der Energieversorgung.

Eine solche intelligente Vernetzung des zukünftigen Energiesystems stellt Deutschland vor die **großen Herausforderungen einer sektorübergreifenden Digitalisierung verschiedener beteiligter Domänen** (Smart Grid, Smart Metering, Smart Mobility, Smart Health, Smart Home, Smart Building). Zugleich bietet sie aber auch vor dem Hintergrund der Digitalisierungs- und Standardisierungsstrategie große Chancen und Perspektiven für die beteiligten Akteure in Deutschland.

Damit der Aufbau eines intelligenten Netzes gelingt, müssen intelligente, eingebettete Produktkomponenten (Smart Embedded Devices) zu intelligenten Systemen verbunden und eine sichere, nachvollziehbare Erfassung und Austausch von Informationen zur digitalen Verarbeitung für verschiedene Anwendungsfälle ermöglicht werden. **Für den Aufbau einer zukunftssicheren, innovativen digitalen Infrastruktur der Energiewende gibt es zwei Grundvoraussetzungen: die standardisierte, sichere Infrastruktur selbst und Regelungen zum Umgang mit Daten unter Berücksichtigung von Vorgaben zum Datenschutz, zur Datensicherheit und zur Datensouveränität**.

Der **Entwurf eines Gesetzes zur Digitalisierung der Energiewende trägt diesen Kernanforderungen Rechnung** und **schafft deshalb entscheidende Voraussetzungen für den Aufbau einer intelligenten Infrastruktur für die Energiewende:** Mit seinen technischen Vorgaben, den Schutzprofilen und Technischen Richtlinien, enthält der Entwurf das Konzept für eine sichere Digitalisierung der Energiewende. Mit seinen Rolloutvorgaben (Einbauverpflichtungen) sichert der Entwurf eine breite Verwendung des neuen Standards. Die Regelungen zur zulässigen

Datenkommunikation setzen zentrale Datenschutzanforderungen um (u.a. Grundsatz der Datenhoheit und Datensparsamkeit).

2. Sichere Kommunikationsplattform für das intelligente Netz

Intelligente Messsysteme sind wichtige Systemlösungen der modernen Mess-, Steuerungs- und Kommunikationsinfrastruktur des intelligenten Netzes. Auf der einen Seite sorgen intelligente Messsysteme für eine aktuelle Verbrauchstransparenz, auf der anderen Seite für eine sichere Übermittlung von Mess-, Steuerungs- und Netzführungsdaten sowie Energiemanagement- und Mehrwertdienstdaten. Mit der zusätzlichen Fähigkeit, eine Plattform für die Steuerung von elektronischen Verbrauchsgeräten und Erzeugungsanlagen zu bieten, verbessern intelligente Messsysteme zukünftig das Last- und Erzeugungsmanagement im Verteilnetz, da auch diese Anwendungsfälle über die sichere und standardisierte Plattform abgewickelt werden können. **Zentrale Komponente eines intelligenten Messsystems ist das Smart Meter Gateway als Kommunikationseinheit, die Sensor-, Mess-, Aktor- und Steuerungseinheiten sicher in das intelligente Netz einbindet.**

Das Smart Meter Gateway mit integriertem Sicherheitsmodul erfüllt die energiewirtschaftlichen Anforderungen des Rechtsrahmens und stellt zudem eine Basissystemarchitektur zur Etablierung eines intelligenten Netzes mit einheitlichem Sicherheitsniveau bereit.

Da es beim Aufbau und der Nutzung eines intelligenten Netzes nicht zuletzt auch um die Verarbeitung personenbezogener Daten geht, sind die Sicherheit und der Schutz eben jener Daten eine zentrale Voraussetzung für Vertrauen und Akzeptanz in die neue Technik. **Besonders im Interesse der Bürgerinnen und Bürger sind verbindliche Vorgaben für intelligente Messsysteme, wie sie der Entwurf enthält, nötig, um für ein hohes Maß an Datenschutz und Datensicherheit sowie Interoperabilität in dieser kritischen Infrastruktur zu sorgen.**

3. Datenschutz und Datensicherheitsstandards des BSI („privacy & security by design“)

Gegenstand des neuen Stammgesetzes über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (**Messstellenbetriebsgesetz – MsbG**) in Artikel 1 ist u.a. die **Festlegung hoher technischer Standards in Form von Schutzprofilen (Protection Profiles, PP) und Technischen Richtlinien (TR) des BSI zur Gewährleistung von Datenschutz und Datensicherheit (§§ 19 bis 30**), welche die stufenweise Einführung und Betrieb von nachweislich

sicheren, intelligenten Systemkomponenten wie das Smart Meter Gateway für die Digitalisierung des Energienetzes regeln.

Im Auftrag des Bundesministeriums für Wirtschaft und Energie entwickelt das BSI seit 2010 **Anforderungen an vertrauenswürdige Produktkomponenten** (Smart Meter Gateway mit integriertem Sicherheitsmodul), an die **Informationssicherheit bei Administration und Betrieb** sowie an die **vertrauenswürdige Kommunikationsinfrastruktur** (Smart Metering - Public Key Infrastruktur).

Sicherheitsstandards können nur dann erfolgreich sein, wenn sie bereits in der Innovationsphase mitgestaltet werden (**„privacy & security by design“**) sowie auf breite Akzeptanz bei Herstellern und Anwendern stoßen. Daher hat das BSI diese von Anfang an in die Erstellung und Weiterentwicklung der Schutzprofile und der Technischen Richtlinien eingebunden. **Eingebunden in die Entwicklung wurden verschiedene Verbände aus den Bereichen Telekommunikation, Informationstechnik, Energie, Wohnungswirtschaft und Verbraucherschutz sowie die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Bundesnetzagentur sowie die Physikalisch-Technische Bundesanstalt.** Das BSI setzt die Datenschutzanforderungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) im Rahmen der BSI-Vorgaben um. Die BSI-Vorgaben berücksichtigen auch die betroffenen eichrechtlichen Anforderungen der Physikalisch-Technischen Bundesanstalt (PTB), sowie die Zuständigkeiten der BNetzA.

<u>Datenschutzkonzept des intelligenten Messsystems / Sternförmige Kommunikation</u>

Das im Gesetzentwurf verankerte **Datenschutzkonzept des intelligenten Messsystems** nach § 60 MsbG regelt, dass die **Messwerterfassung, Verarbeitung (inklusive Plausibilisierung und Ersatzwertbildung) und Speicherung vor Ort im Gateway** erfolgt (**Datenhoheit)**. Dabei werden **Messdaten anonymisiert, pseudonymisiert und aggregiert im Gateway** aufbereitet (**Datensparsamkeit**) und **sternförmig direkt an berechtigte Stellen verschlüsselt durch das Gateway** versendet (**Zweckbindung**). Letztverbraucher wie z. B. Haushalts- und Gewerbekunden haben volle **Transparenz über die im Smart Meter Gateway verarbeiteten Daten und** können **Kommunikations- und Verarbeitungsschritte** nachvollziehen („im Logbuch“). Durch die Dokumentation im Logbuch würde jeder Datenmissbrauch erkennbar und nachweisbar, was die

Durchsetzung von Verbraucherrechten erheblich erleichtert. Die gesicherte, korrekte Verarbeitung der Daten durch das Gateway wird durch die Prüfung und Zertifizierung des Gateways beim BSI nachgewiesen.

Bis zu einem Jahresverbrauch von 10.000 Kilowattstunden sieht der Gesetzentwurf nach § 60 MsbG standardmäßig **nur eine Übermittlung von jährlichen Jahresarbeitswerten an Berechtigte** vor. Der **Durchschnittshaushalt in Deutschland verbraucht ca. 3.500 Kilowattstunden Strom im Jahr.** Nur wenn der Letztverbraucher selbst einen Tarif oder einen Mehrwertdienst wählt, der eine häufigere Datenübermittlung erfordert, werden diese zweckgebunden auch an Netzbetreiber und Lieferanten oder weitere berechtigte Marktteilnehmer versendet.

Das **BSI gewährleistet die technische Umsetzung der Datenschutzanforderungen des BfDI** im Schutzprofil sowie in der Technischen Richtlinie und stellt nachweislich sicher, dass die Gesamtheit der detaillierten Verbrauchsdaten lediglich in der Obhut der Letztverbraucher ist und nur aufbereitete Daten durch das Gateway soweit dies erforderlich ist verschlüsselt an berechtigte Dritte übermittelt werden. Daher gibt es keine Argumentation für einen Opt-Out Bedarf beim Letztverbraucher.

Die **Vorschläge zu sogenannten „Datendrehscheiben“ bei Verteilnetzbetreibern**, wie sie der BDEW in seiner Stellungnahme zum Regierungsentwurf fordert, **sind mit dem Datenschutzkonzept nicht vereinbar**. Zum Grundsatz der Datensparsamkeit gehört die Maßgabe, Daten möglichst direkt an Berechtigte zu übermitteln und von gestuften Systemen und Datenaufbereitungen Dritter (wie z.B. bei Verteilnetzbetreibern) möglichst abzusehen. Hier würden ansonsten sämtliche detaillierte Verbrauchsdaten bei Verteilnetzbetreibern zunächst gespeichert und erst anschließend bereinigt, aufbereitet und weitergeleitet werden. **Die Etablierung von derartigen, zentralen Datensammlungen widerspricht den Grundsätzen der Datensparsamkeit und Datenvermeidung**. Zudem bildet das Datenschutzkonzept durch die **dezentrale Intelligenz im Smart Meter Gateway** überhaupt erst die **Basis**, zweckgebundene Daten **für zukünftige Netzsteuerungsprozesse und Mehrwertdienste sowohl im Weitverkehrsnetz als auch im lokalen Heimnetz** bereitzustellen.
In Fällen wie z. B. der korrekten Tarifierung von Haupt- und Untermessungen sowie die Bildung von Ersatzwerten bei technischen Kommunikationsstörungen wird die Ersatzwertbildung einer einfachen Regel folgen, da die zu verteilende Energiemenge aufgrund historischer Werte im Gateway bekannt ist. Die Spezifikation der Plausibilisierung und Ersatzwertbildung im Smart Meter Gateway wird in der

entsprechenden Technischen Richtlinie (siehe 3.1.2) bis Ende 2016 / Anfang 2017 erfolgen, so dass die **Voraussetzungen zur sternförmigen Kommunikation durch das Smart Meter Gateway technisch erfüllt** sein werden. Der Gesetzentwurf sieht hier für den Bereich Strom bereits eine **sehr angemessene Übergangsregelung zur sternförmigen Kommunikation** vor. Der Bundesnetzagentur wird die Möglichkeit zur Gestaltung der technischen Übergangsphase bis zum 31. Dezember 2019 eingeräumt (Aufbereitung und Übermittlung nicht vom Smart Meter Gateway). **Perspektivisch werden mit der direkten, sternförmigen Datenkommunikation sowohl deutliche Effizienzgewinne (wie z.B. zeitnahe Informationen über Energieverbräuche) als auch gleichzeitig ein Mehr an Datenschutz und Datensicherheit einhergehen. Die geforderten Änderungsvorschläge zum Referentenentwurf in Richtung von „Datendrehscheiben" bei Verteilnetzbetreibern sind im Hinblick auf das Datenschutzkonzept kontraproduktiv und lassen die geschaffenen technischen Möglichkeiten ungenutzt.** Sie sind auch nicht verständlich vor dem Hintergrund, dass das BSI die Systemarchitektur-Grundentscheidung zugunsten der sternförmigen Kommunikation bereits 2011 in einem transparenten Verfahren nach Diskussionen mit allen Beteiligten (auch den energiewirtschaftlichen Verbänden) getroffen hat. Das gesamte entwickelte Datenschutz- und Datensicherheitskonzept baut auf das Konzept der sternförmigen Kommunikation.

3.1 Vertrauenswürdige Produktkomponenten (§§ 22, 24 MsbG)

Das **BSI entwickelt** nach § 22 MsbG sowohl **hohe sicherheitstechnische Vorgaben in Form von Schutzprofilen** als auch **funktionale Anforderungen zur Interoperabilität in Technischen Richtlinien** für das Smart Meter Gateway.

3.1.1 Nachweis der sicherheitstechnischen Vorgaben

Die **Einhaltung der sicherheitstechnischen Vorgaben (inkl. Prüfung des Sourcecodes) nach dem Schutzprofil für das Smart Meter Gateway werden** gemäß § 24 MsbG im Rahmen des Zertifizierungsverfahrens nach Common Criteria (CC) **durch das BSI überprüft**. Das BSI betreut derzeit acht CC-Zertifizierungsverfahren von Herstellern, die bereits mit der Entwicklung von Smart Meter Gateways begonnen haben:

- Dr. Neuhaus Telekommunikation GmbH (BSI-DSZ-CC-0822)
- OPENLiMiT SignCubes AG Sponsor: Power Plus Communications AG (BSI-DSZ-CC-0831)
- Landis + Gyr AG (BSI-DSZ-CC-0905)
- Theben AG (BSI-DSZ-CC-0918)
- EMH metering GmbH & Co.KG (BSI-DSZ-CC-0919)

- devolo AG (BSI-DSZ-CC-0934)
- Kiwigrid GmbH (BSI-DSZ-CC-0982)
- EFR GmbH (BSI-DSZ-CC-1000)

Für die ersten Einbauverpflichtungen ab 2017 von Smart Meter Gateways steht der **Nachweis der geleisteten Sicherheitsfunktionalität für die verordneten Anwendungsbereiche im Vordergrund**. Zur Gewährleistung einer stringenten Weiterentwicklung des Produktes, um u.a. die Vorgaben des Rechtsrahmens zu ermöglichen, ist der Nachweis zum **erfolgreichen Abschluss der Zertifizierung nach Common Criteria entscheidend**.
Im Hinblick auf die Digitale Souveränität sei erwähnt, dass es sich bei den o.g. Herstellern um europäische Anbieter aus der Fachbranche handelt.

3.1.2 Funktionalen Anforderungen und Nachweis der Interoperabilität

Die funktionalen Anforderungen zur Interoperabilität (z.B. Spezifikation der Datenformate, Protokolle) sind mit der aktuell gültigen und veröffentlichten Version 1.0 der Technischen Richtlinie zum Smart Meter Gateway bereits bekannt. **Aktuell werden die Feinspezifikation (inklusive Plausibilisierung und Ersatzwertbildung), die Testspezifikation und die darauf aufbauende Testumgebung zum Nachweis der Interoperabilität entwickelt**. Die Fertigstellung der Feinspezifikation der Technischen Richtlinie ist Ende 2016 / Anfang 2017 geplant, eine modulare Veröffentlichung von (Teil-)Spezifikationen ist vorgesehen. Die Fertigstellung der Testspezifikation wird voraussichtlich Anfang / Mitte 2017 erfolgen, eine modulare Veröffentlichung ist ebenfalls vorgesehen. Mit der Entwicklung der Testumgebung wird Mitte 2016 begonnen.

Die Einhaltung der Vorgaben zur Interoperabilität werden ebenfalls nach § 24 MsbG im Rahmen eines Zertifizierungsverfahrens **durch das BSI überprüft.** Der Nachweis der Einhaltung der **sicherheitstechnischen Vorgaben im Rahmen des Zertifizierungsverfahrens nach Common Criteria (CC) beinhaltet u.a. auch die Bestätigung einer sicheren Update-Funktionalität**, so dass zukünftig weitere Funktionalitäten oder neue Datenformate/Protokolle durch ein Software-Update in der Verantwortung des Administrators nachgerüstet werden können, ohne dass Geräte ausgetauscht werden müssen. Damit ist auch ein **Nachweis zur Interoperabilität der bereits installierten Smart Meter Gateways zu einem späteren Zeitpunkt in der Markteinführungsphase** möglich.
Der **Zeitpunkt der Nachweispflicht zur Interoperabilität wird durch das BSI festgelegt** und nach § 27 MsbG im Ausschuss Gateway-Standardisierung bekannt gemacht. Nach Festlegung des Zeitpunktes der Nachweispflicht zur Interoperabilität sind Smart Meter Gateway Administrator bzw.

Hersteller verpflichtet das Zertifikat zur Konformität zur festgelegten Version der Technischer Richtlinie vorzulegen.

3.2 Informationssicherheit bei Administration und Betrieb (§ 25 MsbG)

Für den sicheren, technischen Betrieb des intelligenten Messsystems ist der Smart Meter Gateway Administrator verantwortlich. **In § 25 MsbG wird sichergestellt, dass der Betrieb beim Administrator Mindestanforderungen zur Durchsetzung der Informationssicherheit genügt.** Für alle Marktteilnehmer, die die Aufgaben des Administrators selbst wahrnehmen oder als Dienstleister für Dritte anbieten möchten, ist ein vergleichbares Maß an Informationssicherheit notwendig. Folglich sind **einheitliche organisatorische und technische Anforderungen sowie Maßnahmen für die Mindestsicherheit beim Administrator** erforderlich, die in der **Technischen Richtlinie „Smart Meter Gateway Administration“** festgelegt wurden. Der Nachweis der Umsetzung der definierten Mindestanforderungen kann zum einen durch eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz und zum anderen durch eine Zertifizierung gemäß ISO/ IEC 27001 erbracht werden. Nach Einschätzung des BSI werden ca. 20 technische Dienstleister in der Rolle des Administrators erwartet. Hiervon befinden sich bereits 11 Unternehmen beim BSI in Beratung.

3.3 Vertrauenswürdige Kommunikationsinfrastruktur (§ 28 MsbG)

Um den Schutz der von den Haushalten übermittelten Messdaten zu gewährleisten, ist für die Verbindung des Smart Meter Gateways zu einem berechtigten Teilnehmer im Weitverkehrsnetz eine gegenseitige Authentisierung der Kommunikationspartner erforderlich. Die **Kommunikation erfolgt dabei stets über einen verschlüsselten, integritätsgesicherten Kommunikationskanal. Zudem werden zu sendende Daten vom Smart Meter Gateway zusätzlich auf Inhaltsebene für den Endempfänger verschlüsselt und signiert.** Für die gegenseitige Authentisierung der Teilnehmer und zur Etablierung eines verschlüsselten, integritätsgesicherten Kommunikationskanals, als auch für die Verschlüsselung und Signatur von Daten werden Zertifikate bereitgestellt.
Das gewählte Modell der PKI sieht eine **zentrale, staatliche Root (Wurzel) als Vertrauensanker** in der Infrastruktur der Smart Meter Gateways vor. Darunterliegend operieren private Unternehmen, sogenannte Sub-Cas (untergeordnete Zertifizierungsstellen), welche die Betreuung der Marktteilnehmer übernehmen. Das **BSI ist Inhaber der Wurzelzertifikate (Root) der Smart Metering Public Key Infrastruktur** (SM-PKI). Der **Wirkbetrieb der Root wird seit dem 1. März 2015 unter der Aufsicht des BSI** von einem Zertifizierungsdiensteanbieter **durchgeführt**. Des

Weiteren werden den Marktteilnehmern **zusätzlich zur Root verschiedene Testsysteme zur Ausgabe von digitalen Test-Zertifikaten** bereitgestellt.
Die zugehörige **Zertifizierungsrichtlinie nach § 28 MsbG** wird durch das BSI vorgegeben und **regelt** die Teilnahmebedingungen an der Smart Metering PKI für jeden berechtigten Teilnehmer des intelligenten Netzes. Das MsbG regelt somit alle Vorgaben für einen sicheren Datenaustausch zwischen autorisierten Teilnehmern und den intelligenten Systemkomponenten und setzt somit einen **einheitlichen Sicherheitsstandard für die sichere Kommunikation zwischen den Systemen des intelligenten Netzes** durch. Ebenso wird durch das **§ 52 Abs. 4 MsbG** festgelegt, dass der **Austausch von personenbezogenen Daten, Stammdaten und Netzzustandsdaten nur über die Smart Metering PKI gestützte Kommunikation mit den berechtigten Teilnehmern erfolgen muss**.

4. Aufrechterhaltung des Sicherheitsniveaus und Weiterentwicklung der BSI-Standards
Mit dem Ziel, Standards für die Digitalisierung der Energiewende zu schaffen und zugleich präventiv gegen Angriffe durch technische und organisatorische IT-Sicherheit zu agieren, werden neben dem eingebetteten Produkt Smart Meter Gateway auch **sicherheitstechnische Vorgaben und funktionale Anforderungen des BSI für weitere digitale Systemlösungen des intelligenten Netzes**, für z.B. intelligentes Einspeise- und Lastmanagement, umgesetzt.
Insbesondere die **Regelungen im Rahmen des MsbG (§§19 bis 30) ermöglichen** die nachhaltige Digitalisierung des intelligenten Energienetzes und schaffen den **Rahmen für die Aufrechterhaltung und Weiterentwicklung von verbindlichen Standards für Datenschutz und Datensicherheit**, um zukünftigen Angriffen wirksam begegnen zu können. Auf Basis der verbindlichen Standards ermöglicht der Rechtsrahmen den kontinuierlichen **stufenweisen Ausbau der intelligenten Messsysteme und anderer Komponenten**, um eine **sichere Vernetzung dieser Komponenten für sektorübergreifende Anwendungsfälle der Energiewende** zu gewährleisten.

Für die modulare Weiterentwicklung der IT-Sicherheitsstandards für digitale Systemlösungen des intelligenten Netzes wird eine sektorübergreifende Anwendungsfallbetrachtung aus den Domänen Smart Metering/Sub Metering (weitere Sparten, flexible Tarife, Energieeffizienz, Erfassung von Netzzustandsdaten und Verbrauchsdaten), Smart Grid (Netzsteuerung mit intelligentem Einspeise-und Lastmanagement von dezentralen Erzeugern und Verbrauchern, Strommärkten und virtuellen Kraftwerken), Smart Home/Smart Building (Gebäudeautomatisierung, Energiemanagement), Smart Mobility (Integration der intelligenten Ladesäulen-Infrastruktur und

Elektrofahrzeuge) sowie Smart Health/Smart Services (Betreutes Wohnen/ Mehrwertdienste) **durch die Weiterentwicklungsprojekte des BSI umgesetzt werden.**
Mit dem Inkrafttreten des Gesetzes zur Digitalisierung der Energiewende **wird das BSI eine Roadmap zur Weiterentwicklungsstrategie der technischen Vorgaben** in Form von Schutzprofilen und Technischen Richtlinien **veröffentlichen und zur breiten Konsultation bereitstellen.** Mit dem Inkrafttreten des MsbG und der damit einhergehenden Etablierung der BSI-Vorgaben, der mit dem Markt abgestimmten Standardisierungsstrategie und der BSI-Zertifizierung kann zugleich eine innovative als auch nachweislich sichere digitale Systemarchitektur für das intelligente Energienetz aufgebaut werden.

5. Einführung und Betrieb von intelligenten Messsystemen

Der maßgebliche Start der Einführung von intelligenten Messsystemen ist neben der Festlegung, dass der Rollout ab 2017 für bestimmte Einbaugruppen beginnt, an die technische Freigabe gemäß § 30 MsbG gekoppelt. **Für die Einführung und Betrieb von** intelligenten Messsystemen und somit der Einführung und Betrieb von **zertifizierten Smart Meter Gateways wird das BSI entsprechende Feststellungen der technischen Möglichkeit** zum Einbau und Betrieb von intelligenten Messsystemen gemäß § 30 MsbG **definieren**. **Berücksichtigen wird das BSI dabei natürlich die konkrete Einsatzumgebung** und die daran anknüpfenden energiewirtschaftlichen Anforderungen (z.B. Fähigkeit zum Einspeisemanagement und zur Übertragung von Ist-Einspeisungen bei größeren EEG-Anlagen).
Zur Feststellung der technischen Möglichkeit gehören neben den Systemkomponenten des intelligenten Messsystems auch die umgesetzten Anforderungen der Informationssicherheit bei der Administration und Betrieb von intelligenten Messsystemen und Anbindung an die Smart Metering PKI bei den beteiligten Marktakteuren.

Um vollumfänglich die Anwendungsfälle des intelligenten Messsystems umsetzen zu können, müssen entsprechende Prozesse der Marktkommunikation angepasst und die Digitalisierung vorangetrieben werden. Die Bundesnetzagentur wird in Abstimmung mit dem BSI und den Marktakteuren die Prozesse zur Marktkommunikation fortentwickeln, sodass eine **stufenweise Erprobung und Einführung von intelligenten Messsystemen** möglich wird. Hierzu wird das BSI Festlegungen zum Mindestumfang der zu realisierenden Anwendungsfällen veröffentlichen, so dass eine stufenweise, **Anwendungsfall-scharfe Einführung von zertifizierten Messsystemen** umgesetzt werden kann. Administratoren, die die dafür notwendigen organisatorischen und sicherheitstechnischen

Mindestanforderungen der Technischen Richtlinie „Smart Meter Gateway Administration“ nachweislich erfüllen, werden somit die vom BSI definierte Mindestanzahl an Anwendungsfällen umsetzen müssen. Im Anschluss muss stufenweise die Mindestanzahl von Anwendungsfällen auf Basis der Feststellung der technischen Möglichkeit erweitert werden. Das mit dem BSI und den Marktakteuren abgestimmte Zielmodell der Marktkommunikation wird bis Ende 2020 durch die Bundesnetzagentur bereitgestellt. Eingebunden in die Entwicklung der Standards werden folglich verschiedene Verbände aus den Bereichen Telekommunikation, Informationstechnik, Energie, Wohnungswirtschaft und Verbraucherschutz sowie die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Bundesnetzagentur und die Physikalisch-Technische Bundesanstalt.

6. Fazit

Intelligente Messsysteme sind **wichtige Bausteine im intelligenten Netz** und **benötigen „Security & Privacy by Design“** in dieser kritischen Infrastruktur. Das Smart Meter Gateway ermöglicht als **sichere Kommunikationsplattform die digitale Sektorkopplung** und wird zum **Treiber für Innovationen der Digitalisierung**.

Die **Schutzprofile und die Technischen Richtlinien des BSI als wesentlicher Bestandteil des Gesetzentwurfs gewährleisten ein hohes Maß an Datenschutz und Datensicherheit** und sorgen für einen einheitlichen und interoperablen Sicherheitsstandard im künftigen Energieversorgungssystem. Das **Datenschutzkonzept des intelligenten Messsystems berücksichtigt** eine **zweckgebundene Datenverarbeitung und sternförmige Datenversendung des Gateways**, das sowohl für den Letztverbraucher nachvollziehbar und transparent aufgezeigt ist, als auch den **Umgang der Daten im Sinne der Datensouveränität** technisch durchsetzt. Für die Nachweise zur Einhaltung der Schutzprofile und der Technischen Richtlinien werden entsprechende **Prüfungen bei anerkannten Prüfstellen mit abschließender Zertifizierung durch das BSI** durchgeführt.

Bedenken bezüglich des Datenschutzes und der Datensicherheit sind damit unbegründet und als Grundlage für die **Argumentation einer „Opt-Out“-Möglichkeit des Letztverbrauchers nicht stichhaltig**.

Die **direkte, sternförmige Datenkommunikation durch das Smart Meter Gateway ermöglicht** sowohl **deutliche Effizienzgewinne** als auch gleichzeitig ein **Mehr an Datenschutz und**

Datensicherheit. **Änderungen** am gesetzlichen Rahmen zur Etablierung von „Datendrehscheiben“ bei Verteilnetzbetreibern **wären dagegen kontraproduktiv** und würden die technischen Möglichkeiten ungenutzt lassen.

Der Gesetzentwurf ermöglicht den ersten wichtigen Schritt zur digitalen Transformation der Infrastruktur zu einer innovativen, digitalen Infrastruktur des intelligente Netzes. Mit dem Regelungsentwurf wird zusätzlich die Grundlage geschaffen, um eine **stufenweise Fortentwicklung der Sicherheitsvorgaben des BSI sowohl für intelligente Messsysteme als auch für weitere wichtige Systemkomponenten des intelligenten Energienetzes** über eine **Roadmap zur Digitalisierung** umzusetzen.

Der derzeitige Regelungsentwurf schafft in Zusammenhang mit den technischen Standards des BSI die notwendige Rechtssicherheit und setzt das im Koalitionsvertrag verfolgte Ziel um, **verbindliche Rahmenbedingungen für den sicheren und datenschutzkonformen Einsatz von intelligenten Messsystemen für vielfältigste Anwendungsfälle im intelligenten Netz** zu regeln.

Im Auftrag
gez.

Kowalski