

Stellungnahme

# Digitalisierungsbericht gemäß § 48 des Mess- stellenbetriebsgesetzes

Stellungnahme des Bundesverbands  
Neue Energiewirtschaft e.V. (bne) und  
der Smart-Meter-Initiative (SMI)

Berlin, 24.09.2024: Wie in § 48 Messstellenbetriebsgesetz festgelegt, hat das BMWK den Bericht „Resilienz weiter stärken, den Systemnutzen der Digitalisierung der Energiewende konsequent heben“ (kurz Digitalisierungsbericht) vorgelegt. Der Bericht soll Auskunft geben über den Stand der Digitalisierung sowie Anpassungen des Rechtsrahmens. Aus Sicht des Bundesverbands neue Energiewirtschaft e.V. (bne) und der Smart-Meter-Initiative (SMI) zeigt er vor allem, dass der Entbürokratisierungsprozess offenbar zum Stillstand gekommen ist und der eigentliche Sinn und Zweck der Digitalisierung verfehlt wird. Der Rollout intelligenter Messsysteme (iMSys) ist kein Selbstzweck. Mit der großen Menge zusätzlicher fluktuierender Erzeugung erneuerbarer Energien und den vielen neuen flexiblen Anlagen in der Niederspannung wird das Problem immer drängender, Verbrauch und Erzeugung zeitlich und räumlich zu koordinieren. Ohne zeitliche aufgelöste, rasch verfügbare abrechnungsrelevante Messwerte können erzeugende und verbrauchende Marktlokationen (MaLos) nicht auf der Basis von Werten bilanziert werden, sondern werden über standardisierte Lastprofile (SLP) abgebildet. Die einfache Erhebung und Übermittlung von Messwerten muss überragendes und vorrangiges Ziel des iMSys-Rollout sein, um auch nur ansatzweise die kurzfristigen Herausforderungen im Energiesystem angehen zu können.

## Allgemeine Kritikpunkte

**Keine Vereinfachung:** Die grundlegenden Probleme des Smart-Meter-Rollouts werden nicht adressiert, es gibt keine Perspektive für die Reduktion von Komplexität und technische Vereinfachungen, und damit eine verspielte Chance auf niedrigere Kosten im Smart Meter Rollout.

**Kein Wettbewerb:** Anstatt die Rolle des wettbewerblichen Messstellenbetreibers (wMSB) zu stärken, sollen Quoten und Jahrespläne die Marktwirtschaft ersetzen. Die Konditionen für den Einbau auf Kundenwunsch durch den grundzuständigen Messstellenbetreiber (gMSB) sollen offenbar so unattraktiv gestaltet werden, dass das Interesse an dynamischen Tarifen und das Engagement von Verbrauchern für die Energiewende insgesamt geschädigt wird.

**Keine Verhältnismäßigkeit:** Der Bericht nennt keine Lösungsvorschläge für kosteneffizientes, digitales Metering für kleinere Verbrauchsgruppen (z.B. Smart Meter *light*).

**Keine Planbarkeit:** Die Spielregeln sollen wiederholt kurz vor knapp so signifikant angepasst werden, dass die Grundlage für Geschäftsplanungen stark beeinträchtigt werden. Derartige Unplanbarkeit macht Deutschland als Innovationsstandort untragbar.

**Keine juristische Sicherheit:** Änderungen benötigen Vorlauf und Übergangsfristen. Andernfalls ergeben sich juristische Grauzonen, Schäden mit unklaren Schadensansprüchen und Verunsicherung des Marktes.

## Anmerkungen zur vorgeschlagenen Weiterentwicklung des Rechtsrahmens

### Geplante Änderungen (Umfang, POG) im Kontext des Einbaus von intelligenten Messsystemen auf Kundenwunsch

Die Vorschläge im Bericht für die Einschränkung des Anspruchs des Kunden auf Einbau eines iMSys innerhalb von vier Monaten sind äußerst negativ zu bewerten: Der für jedes

Netzgebiet bestehende Anspruch der Kunden auf vorzeitigem Einbau eines iMSys zu festgelegten Kosten und innerhalb definierter Fristen ist die Grundlage für die Abwicklung von vertrieblichen Produkten, insbesondere für das Angebot von flexiblen Tarifen. Der Einbau auf Kundenwunsch wird effektiv verzögert, was zur Benachteiligung der "First Mover" führt. Es ist zu erwarten, dass die Akzeptanz dynamischer Tarife bei Verbrauchern erheblich beeinträchtigt wird. Es kann nicht mehr sichergestellt werden, dass Kunden, die dynamische Tarife nutzen wollen, innerhalb eines vorab planbaren Zeitraums und damit rechtzeitig zum avisierten Produktstart ein iMSys vom grundzuständigen MSB (gMSB) erhalten. Die Konsequenz einer Einführung von Quotenregelungen oder „Rollout-Vereinbarungen“ wird zudem dazu führen, dass in jedem Netzgebiet eine andere Rechtslage hinsichtlich eines Einbauanspruchs gegen den gMSB Anwendung finden wird. Die für einen bundesweiten Vertrieb benötigte zeitliche und kostenseitige Planbarkeit wäre damit nicht weiter gewährleistet. Gleiches gilt für die Möglichkeit der freiwilligen Rolloutvereinbarung zwischen VNB und dem gMSB. Nach derzeitigem Verständnis würde dies zu einer vollständigen Befreiung im Betrachtungszeitraum bis 31.12.2031 für einen freiwilligen Einbau auf Kundenwunsch in diesem Netzgebiet führen. Im Bericht wird fälschlicherweise eine solche Rollout-Vereinbarung mit einem Einbau auf Kundenwunsch als gleichwertige Alternative erachtet. Diese Sichtweise verkennt, dass der Kunde im Rahmen einer Rolloutvereinbarung bis zu 6 Jahre auf den Einbau eines iMSys durch den gMSB warten müsste. Neben den damit einhergehenden EU- und verbraucherrechtlichen Fragestellungen, ist aktuell vollständig unklar, wie und mit welchen Konsequenzen solche (individuellen) Vereinbarungen auf Umsetzung, Vollzug und ggf. Nichterreichung überwacht werden sollen und welche Konsequenzen sich daraus für die Beteiligten (insb. Sanktionierung der säumigen gMSB) ergeben.

Die Besteller-POG schädigt massiv die Beteiligungsdimension, indem sie Verbraucher bestraft, die sich aktiv für innovative Energiewende-Produkte entscheiden. Diese werden auf Lebenszeit des Stromzählers mit höheren, jährlich wiederkehrenden Kosten belastet, was subjektiv als ungerecht empfunden werden wird.

Wir fordern, dass mindestens 50% der Besteller-POG durch den Netzbetreiber getragen wird, da dieser davon ausgehen kann, dass viele der betroffenen Verbraucher/innen zukünftig von Netznutzen sein werden, da sie bspw. auch dynamische Netzentgelte aktiv nutzen

oder nicht “reine dynamische Tarifikunden” ohne steuerbare Verbrauchseinrichtungen bleiben. Der dynamische Tarif ist hier nur das der Startpunkt.

### Umfang und Bepreisung von Zusatzleistungen

Ein bundesweit einheitlicher Leistungskatalog mit einheitlichen Preisobergrenzen in jedem Netzgebiet ist für bundesweit tätige Anbieter zur Umsetzung ihrer Produkte unabdingbar: Unterschiedliche Rahmenbedingungen je Netzgebiet führen zu einer hohen Komplexität (je Netzgebiet unterschiedlicher Umfang der angebotenen Zusatzleistungen zu unterschiedlichen Kosten), verhindern damit ein einheitliches Produktangebot und wirken sich nachteilig auf die Wirtschaftlichkeit aus. Auch sind bundesweit einheitliche Preisobergrenzen zwingend erforderlich, die Preisstellung darf nicht allein den gMSB unterliegen: Sollten die gMSB künftig von der POG abweichen wollen, weil sie die Leistung nicht zu der festgelegten POG erbringen können, muss künftig zwingend sichergestellt werden, dass sie etwaige Abweichungen vorab gegenüber einer Behörde (BNetzA, Landesregulierungsbehörden) anzeigen und auf Angemessenheit überprüfen lassen müssen. Erst dann dürften diese Preise Anwendung finden. Es kann nicht den Bestellern von Zusatzleistungen zugemutet werden, sich bei Zweifeln an der Angemessenheit von Preisen selbst gegen diese wehren zu müssen.

### Einführung einer „Haltepflicht“ bei Ersteinbau intelligenter Messsysteme

Die Einführung einer Haltepflicht hebt ohne Not das gesetzlich verbriefte Recht auf Wechsel des Messstellenbetreibers für die Kunden aus. Nach erfolgtem Ersteinbau durch den gMSB wäre der Kunde dann erst einmal viele Jahre gebunden. Rein aus Kundensicht wäre eine solche Zwangs-Haltefrist allerdings sehr nachteilig: Für den Fall, dass der Kunde für einen langen Zeitraum an den gMSB gebunden wäre, wären dem Kunden bspw. die Inanspruchnahme von marktlichen Bündelangeboten inklusive Messstellenbetrieb verwehrt. Alternativ müsste er einen nicht unerheblichen Entschädigungsbetrag leisten, sollte er innerhalb der Haltepflicht dennoch den MSB wechseln wollen. Dies käme einem Wechselentgelt und damit einer „Wechselhürde bzw. einer Markteintrittsbarriere gleich, was nach den aktuellen gesetzlichen Regelungen unzulässig wäre. Zudem stellt sich die Frage, inwieweit dem Kunden im Falle einer Preiserhöhung für den

Messstellenbetrieb innerhalb der Haltepflicht ein entsprechendes Sonderkündigungsrecht eingeräumt würde. Eine Haltefrist im Umfang von 5-8 Jahren durch den gMSB ist daher abzulehnen.

Stattdessen sollte bei einem Wechsel des Messstellenbetreibers (MSB) der neue MSB verpflichtet werden, funktionierende Smart Meter vom bisherigen MSB für einen vorher festgelegten Preis zu übernehmen. Die Übernahme sollte im Messstellenbetriebsrahmenvertrag festgehalten werden (Änderung § 9 MsbG & § 16 MsbG). Der Übernahmepreis sollte sich an Alter, Zustand und Funktionsumfang des iMSys bemessen („Lifetime Value“) und vom Gesetzgeber im Austausch mit der Branche festgelegt werden. Die bestehende Option in § 16 Abs. 2 MsbG, wonach der neue MSB den Ausbau der Messeinrichtung vom bisherigen MSB verlangen kann, muss entsprechend gestrichen werden. Analog dazu muss auch für die Übernahme der Gateway-Administration durch den neuen MSB ein festes Entgelt festgelegt werden.

### **Einführung eines BNetzA-„Rollout-Monitoring“**

Die Einführung eines regelmäßigen Monitorings über den Rollout-Fortschritt ist grundsätzlich zu begrüßen, sofern sich das Monitoring nicht nur in einer „Bestandsaufnahme“ erschöpft, sondern auch unmittelbar behördliche Maßnahmen eingeleitet werden, die zügig für eine Einhaltung der gesetzlichen Vorgaben durch den gMSB sorgen. Es muss zwingend sichergestellt sein, dass die gMSB – unabhängig von ihrer Größe - ihre gesetzlichen Pflichten, insbesondere auch die fristgerechte Umsetzung der beantragten Zusatzleistungen zuverlässig erfüllen, damit gesetzliche Ansprüche nicht ins Leere laufen. Die bisherige Erfahrung zeigt, dass Versäumnisse leider kaum Konsequenzen nach sich ziehen, daher wäre eine Verschärfung der ordnungsrechtlichen Maßnahmen sehr wünschenswert gewesen und sollte auch weiterhin konsequent eingefordert werden.

Auch die Einführung von speziellen Rollout-Quoten für die besonders systemdienlichen und damit vordringlichen Kundensegmente wie Kunden mit §14a-Anlagen würde dazu führen, dass diese Kunden deutlich schneller und vorrangig ausgestattet werden würden, wodurch sich auch die Notwendigkeit eines Einbauantrags auf Kundenwunsch – welcher kostenseitig ausschließlich zulasten dieser Kunden geht - deutlich verringern könnte.

Dies wäre auch die logische Konsequenz des geforderten beschleunigten Pflichtrollouts für §14a-Anlagen durch den Gesetzgeber selbst.

### **Planung weiterer sicherheitstechnischer Anforderungen an den Betrieb von Erzeugungs- und Verbrauchsanlagen**

Aufgrund der Tatsache, dass vermehrt auch kleine PV-Anlagen bis hin zu Balkon-PV-Anlagen und zudem auch §14a-Anlagen über eine gesonderte Internetverbindung außerhalb der geschützten Smart-Meter-Gateway-Struktur angebunden sind und sich nach Aussage des BMWK teilweise konkrete tatsächliche Anhaltspunkte für gravierende IT-Sicherheitslücken v.a. bei massenhaft importierten vernetzten dezentralen Anlagen für Haushaltskunden vorliegen, werden im Bericht weitergehende sicherheitstechnische Anforderungen an Erzeugungs- und Verbrauchsanlagen gefordert. Grundlage dafür könnten die im Zuge der letzten EnWG-Novelle bzw. im Rahmen des Solarpakets implementierten Rechtsverordnungen sein, die entsprechende zusätzliche Anforderungen an die kommunikative Anbindung von §14a-Anlagen und PV-Anlagen oder sogar eine Untersagung bestimmter Betriebsweisen vorsehen können. Näher Angaben, welche Sachverhalte hier adressiert werden sollen, und welche konkreten Maßnahmen ergriffen werden, lässt der Bericht bisher aber offen.

Der im Bericht angekündigte Erlass entsprechender Rechtsverordnungen für die verpflichtende Vorgabe weiterer sicherheitstechnischer Anforderungen ist sehr kritisch zu bewerten. Sie eröffnet dem Verordnungsgeber die Möglichkeit, nahezu im beliebigen Umfang nachträgliche Anforderungen an ein etabliertes Geschäftsfeld zu definieren oder sogar dessen Umsetzung vollständig zu untersagen, ungeachtet der damit verbundenen Folgen für bestehende und künftige Geschäftsmodelle und ungeachtet bereits getätigter Investitionen für Anbieter und einer Vielzahl an Kunden.

## Wie die Digitalisierung gelingen kann

### Prozesse und Vorgaben verschlanken - Administrativer Aufwand rechtfertigt nicht die Erhöhung der POG

Warum die überbordende Komplexität der Regelungen die Digitalisierung zu erliegen gebracht hat, lässt sich exemplarisch anhand der Bündelungsregelung der POG festmachen. Das BMWK schlägt vor, diese Bündelungsregelung aufzuheben und die POG pro iMSys zu erhöhen. Kernargument für diesen Vorschlag ist der im Vergleich zur ursprünglichen Abschätzung wesentliche höhere Aufwand bei der Installation und Administration eines jeden iMSys, nicht nur des ersten.

Diese Einschätzung greift zu kurz. Denn der hohe Aufwand ist selbst verschuldet. Mit der geplanten Erhöhung würden die Kosten der handwerklich schlechten Regulierung und des fehlenden Wettbewerbs auf die Stromkunden verlagert.

- Die Regelungen für die Installation eines iMSys sind überaus komplex und die resultierenden Prozesse sehr aufwändig, so dass die Installation und Inbetriebnahme eines iMSys mehr als doppelt so lange dauert wie bei einer mME (siehe [BDEW Anwendungshilfe zum Einbau eines iMSys](#)). Diese Komplexität ist nicht zwingend, sondern Folge schlechter Regelungen, komplizierter Sicherheitsanforderungen ohne tatsächlichen Zugewinn an Sicherheit, sowie fehlendem Fokus auf Nutzerfreundlichkeit und Installationseffizienz: So gab es bei der Entwicklung der Regelungen und darauf aufbauender Normen keine Anforderungen an die Ergonomie, keine kontrollierten Nutzertests, und keine Forderung nach einer Mindesteffizienz gemäß definierter Benchmarks.
- Die Administration des SMGW – z.B. Einspielen von HAN- und WAN-Profilen, Konfiguration von Tarifierungsfällen, Monitoring und Klärung von Fehlerfällen, etc. – muss ebenfalls nicht so aufwändig und kompliziert sein, wie sie in den Richtlinien des BSI, den Prozessen der BNetzA und den Anwendungshilfen des BDEW umgesetzt wurde. Es ist keinesfalls so, dass die hohen Sicherheitsanforderungen zwingend derart komplexe und nutzerunfreundliche technische

Lösungen und Prozesse bedingen (wie die alltagstauglichen Prozesse rund um die Sicherheit moderner Smartphone-Plattformen zeigen).

- Die Software-Systeme für die Gateway-Administration sowie für EMTs sind sehr aufwändig zu bedienen, bislang nicht ausreichend tauglich für das automatisierte Massengeschäft und für den Umgang mit Fehlerfällen. Dies ist zum Teil Folge der oben genannten unnötig komplizierten Regeln und Prozesse, zum Teil Folge mangelnden Wettbewerbs durch die Oligopolstruktur des Marktes (wenige Anbieter, teilweise gesellschaftsrechtlich verbunden mit Netzbetreibern), und zum Teil Folge fehlender Anreize für eine höhere Effizienz im Betrieb: Die Software-Hersteller entwickeln nur die Funktionen, die zwingend regulatorisch gefordert sind.

Die angedachte Erhöhung der POG verdeutlicht die grundlegenden, bei den Behörden verursachten Probleme beim BSI wie die ineffektiven Sicherheitsanforderungen und unnötig komplizierte Installationsprozesse; bei der BNetzA unnötig komplizierte Prozesse zur Bestellung von Konfigurationen, Messprodukten den Wechsel von Messstellen sowie Akzeptanz des Oligopols weniger Software-Anbieter und Dienstleister. Vielmehr sollte eine Erhöhung der POG nur dann in Betracht gezogen werden, wenn gleichzeitig die Rahmenbedingungen für einen effizienten Rollout und Betrieb intelligenter Messsysteme geschaffen werden. Das BMWK sollte zuerst beim BSI in seiner Aufsichtsfunktion effektive und effiziente Prozesse einfordern, sollte für mehr Wettbewerb unter den SW-Anbietern im SMGW-Umfeld sorgen durch niedrigere Marktzugangshürden und Belohnung von Prozesseffizienz bei den MSB und VNB, und sollte künstliche Kostentreiber in den uneinheitlichen Technischen Anschlussbedingungen und - Regeln reduzieren.

### **Realistische systemische Sicherheitsbetrachtung**

Die hohen Anforderungen an das iMSys dienen der Sicherheit des Energiesystems. Der Digitalisierungsbericht geht umfassend auf die Bedrohungen ein und zeigt auf, dass eine Weiterentwicklung der Sicherheitsarchitektur nötig ist. Leider bleibt der Bericht



sehr vage sowohl bezüglich der Effektivität und Effizienz der aktuell vom BSI entwickelten Sicherheitsarchitektur als auch im Hinblick auf zukünftige Entwicklungen.

Wir sehen hier dringenden Handlungsbedarf, da die aktuelle Sicherheitsarchitektur dem technischen Fortschritt und der Veränderung des Nutzerverhaltens nicht mehr gewachsen ist: Mit dem SMGW wird der Ansatz der sog. "Perimeter Security" verfolgt – also der Absicherung eines Systems an seinem Rand. Dieser wurde heute weitgehend abgelöst durch Sicherheit in der Tiefe, gestufte Sicherheitskonzepte und Resilienz. Grundlegend für diese inzwischen breit akzeptierten Ansätze sind die Erkenntnisse, dass

- bestimmend für die Sicherheit immer das schwächste Glied in der Kette ist: Bildlich gesprochen bringt es nichts, ein Glied besonders stark auszulegen, wenn die Kette als ganzes funktionieren muss; genau diesen Ansatz implementiert aber das aktuelle SMGW.
- früher oder später Perimeter-Security kompromittiert werden wird, da IT-Systeme nicht mit vertretbarem Aufwand zu 100% abgesichert und über ihre Lebensdauer sicher gehalten werden können. Mit dem aktuellen Schutzprofil (PP) ist aber dieser 100%-Ansatz umgesetzt, bezogen auf die Perimeter-Komponente SMGW und nachzuweisen durch eine aufwändige Zertifizierung gemäß Common-Criteria (CC).
- ausschließlich die skalierenden Angriffe relevant sind für die Systemsicherheit, bei denen zu sehr geringen Grenzkosten viele der "target Assets" kompromittiert werden können. Zur Verhinderung solcher Angriffe kommt es vor allem darauf an, die Grenzkosten hoch zu halten, so dass eine Skalierung für Angreifer ausreichend teuer wird.

Die aktuelle SMGW-Architektur geht davon aus, dass (a) Angriffe auf das Energiesystem über das WAN ausgeführt werden, also über die Internetverbindung des SMGW; und (b) das SMGW Ziel des Angriffs ist, z.B. um dort hinterlegte Konfigurationen zu ändern oder um über das SMGW ausgetauschte Steuerbefehle zu manipulieren. Die Situation stellt sich aber heute, zehn Jahre nach Veröffentlichung der ersten Version des Schutzprofils, komplett anders dar:

- Relevant für die Sicherheit des Energiesystems sind die Anlagen, welche tatsächlich Energie beziehen oder einspeisen. Dies sind heute Elektrofahrzeuge, Batteriespeicher, PV-Wechselrichter, Wärmepumpen etc., welche in Millionenstückzahl von Privathaushalten und Gewerben angeschafft werden. Systemkritisch ist, wenn ein Angreifer viele dieser Anlagen unter seine Kontrolle bringen kann – typischerweise, indem es ihm gelingt, eigenen Programmcode auf all diesen Anlagen auszuführen.
- Alle diese Anlagen sind heute über das Internet mit einem Backend-System verbunden – meistens dem Backend-System des jeweiligen Herstellers. Per Smartphone-App oder Web-Schnittstellen können Nutzerinnen und Nutzer über das Hersteller-Backend ihre Anlagen konfigurieren, steuern und überwachen. Der Haupt-Angriffspfad ist daher nicht die WAN-Verbindung des SMGW sondern die Internetverbindung der Anlage und die Backend-Systeme der Hersteller.

Anstatt die geänderte Bedrohungslage, Kundenerwartungen und Erkenntnisse der Sicherheitsforschung einzubeziehen, sehen wir in der aktuell konsultierten Novelle von PP und der Technischen Richtlinie (TR) wie auch im vorliegenden Digitalisierungsbericht die Fortschreibung der überholten iMSys-Sicherheitsarchitektur. Dies mag aus Sicht der wirtschaftlichen Interessen inzwischen etablierter Akteure verständlich sein, führt aber zu hohen Kosten im Betrieb, ohne jedoch die Systemsicherheit zu erhöhen. Die offensichtlich einfache Lösung ohne grundlegende Änderung der Sicherheitsarchitektur, ist das Verbot jegliche Kommunikationsverbindungen für energiesystemrelevanten Anlagen, außer über das SMGW. Dieser Weg ist in einer Verordnungsermächtigung angelegt und scheint auch im vorliegenden Digitalisierungsbericht bevorzugt zu werden. Wir halten diese Lösung nicht für zielführend, weil sie die Sicherheit in der Praxis nicht erhöht, aber der Energiewende schadet:

- Kunden erwarten heute digital integrierte Geräte, die sie per Smartphone bedienen können. Ein deutscher Sonderweg, bei dem Anlagen jede Kommunikation über das SMGW führen müssten, würde in den nächsten Jahren nicht zufriedenstellend funktionieren, die Auswahl und damit der Wettbewerb würde kleiner und Kunden würden sich gegen Energiewendeanlagen entscheiden.

- Ebenfalls nicht gangbar scheint der Weg, alle Energiewende-Anlagen einer verpflichtenden Sicherheits-Konformitätsbewertung durch eine benannte Stelle zu unterwerfen, da dies massiv den freien Warenverkehr in der EU einschränken und wiederum die Auswahl einschränken, den Wettbewerb behindern und die Preise erhöhen würde.
- Durch die hohen Anforderungen an die Backend-Systemanbindung für aktive externe Marktteilnehmer (aEMT) kommt es heute schon zu einer Konzentration auf wenige Dienstleister, so dass zentrale Angriffspunkte entstehen und die Sicherheit effektiv sinkt.

#### **Stattdessen sehen wir folgenden regulatorischen Ansatz als zielführend an:**

- Energiesystemrelevante Anlagen, welche über eine Kommunikationsschnittstelle mit einem Backend-System kommunizieren, müssen diese Schnittstelle kostenfrei offenlegen oder einen frei verfügbaren Standard implementieren. Somit soll es möglich werden, dass alternative Backend-Systeme entstehen, lock-in vermieden wird, und Kunden sich den für ihre Bedürfnisse passenden Anbieter auswählen können – z.B. wegen guter Sicherheitsbewertung oder Datenschutz.
- Hersteller sind verpflichtet, über die beworbene Lebensdauer der Anlage (10-20 Jahre) Marktbeobachtung zu betreiben und Software-Updates zu liefern.
- Sollte ein Hersteller aus dem Markt ausscheiden, so muss er den Quellcode der Anlagen-Software offenlegen, um es Dritten zu ermöglichen, weiterhin Updates für die im Feld befindlichen Anlagen bereitzustellen.
- Das SMGW sollte über eine stabile, moderne Web-API für Energiewende-Anlagen sicherheitsrelevante Funktionen anbieten (Zufallszahl-Generator, Signatur, Zeitführung, Firewall, Message-Broker für die Kommunikation mit dem jeweils zuständigen Netzbetreiber), welche Anlagen niederschwellig nutzen können.

## Bundesverband Neue Energiewirtschaft (bne)

Der bne verbindet Wettbewerb, Erneuerbare und Innovation im Energiemarkt. Seine Mitgliedsunternehmen lösen alte Grenzen auf und setzen die Kräfte der Energiewende frei.

## Smart-Meter-Initiative (SMI)

Die im Januar 2024 gegründete Smart-Meter-Initiative besteht aus den digitalen Ökostromanbietern Octopus Energy, RABOT Charge, Tibber und Ostrom. Der Initiative haben sich zahlreiche weitere innovative Energieunternehmen angeschlossen, darunter 1KOMMA5, zolar, Go-e, Kiwigrid und Lichtblick. Gemeinsam wollen die Unternehmen den Smart-Meter-Rollout in Deutschland begleiten und beschleunigen. Als Pioniere dynamischer Tarife setzen sie sich gemeinsam mit Messstellen- und Verteilnetzbetreibern für den vorzeitigen Einbau von intelligenten Stromzählern ein. Die Vision: Verbrauchenden die Möglichkeit bieten, den eigenen Stromverbrauch flexibel an das Stromangebot anzupassen und so von günstigeren Preisen zu profitieren.

